Sovereign Discourse on Cyber Conflict Under International Law

Sean Kanuck*

I. Introduction

This Article will expand the Symposium's dialogue on law, information technology, and national security in two ways: first, by examining the intersection of those three subjects through the optic of public international law versus domestic statutes, regulations, or case law; and second, by providing broader context for the related legal and policy challenges that are simultaneously confronting many countries. A global perspective on these issues is essential because no single nation's declaratory policy or legal interpretations will be binding on the international community. Moreover, law will be but one factor in determining how nation-states ultimately manage cyber conflicts among themselves in the future.

Efforts to analyze "information warfare" under international law began in the 1990s,[1] and since then, numerous governmental, military, academic, and corporate commentators around the world have expressed their personal or organizational views.[2] However, the international community itself has yet to reach collective conclusions regarding many aspects of law in cyberspace, including what constitutes an act of aggression or use of force in cyberspace.[3] Those legal ambiguities are only exacerbated by the

---

* Harvard University, A.B., J.D.; London School of Economics, M.Sc.; University of Oslo, LL.M.; co-author of the 2009 White House Cyberspace Policy Review; member of the United States delegation to the 2009–2010 United Nations group of governmental experts on information security. The views expressed herein do not necessarily reflect the official position of the U.S. Government, the United Nations, or any of their respective subdivisions; accordingly, all statements of fact and opinion should be attributed solely to the author. The author wishes to thank Professor Robert Chesney for the invitation to participate in this Symposium and the Texas Law Review staff for its assistance in researching and editing this Article.

1. *See, e.g.*, Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885, 889 n.7 (1999) (citing several earlier publications that also explored international law and cyber warfare).

2. *See, e.g.*, NAT'L RESEARCH COUNCIL OF THE NAT'L ACADS., TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 241–82 (William A. Owens et al. eds., 2009) [hereinafter NATIONAL RESEARCH COUNCIL] (analyzing cyber warfare under various principles and sources of international law).

3. U.S. President Barack Obama recognized this fact in a White House report which stated, "The Nation also needs a strategy for cybersecurity designed to shape the international environment and bring like-minded nations together on a host of issues, such as technical standards and acceptable legal norms regarding territorial jurisdiction, sovereign responsibility, and use of force." WHITE HOUSE, CYBERSPACE POLICY REVIEW, at iv (2009), *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf. Furthermore, the United Nations group of governmental experts that met during 2004–2005 failed to reach any

technological limitations that currently preclude definitive attribution of cyber events within the timeframe that would be required for national-command-authority decisions in the face of genuine military attacks.[4] With those dual uncertainties—legal and practical—in mind, states are striving to protect their national security interests and critical information infrastructures.

The threefold objectives of this Article are to (1) elucidate how cyberspace and cyber conflicts are currently being considered by sovereign governments, (2) identify related and unresolved areas of public international law, and (3) describe the strategic dynamic of state practice as it pertains to cyberspace. This Article will not, on the other hand, review the secondary literature in detail, evaluate the legal arguments of any specific nation, or offer a comprehensive framework from the internationalist perspective. The purpose herein is to raise awareness of—rather than critique—the sovereign decisions that are being made within national governments and multilateral organizations as well as their potential impact. Accordingly, the normative discussion will be limited to a single, preambulary admonition that government and military officials in every nation should have the requisite knowledge to be fully cognizant of the international legal ramifications of the actions they take.[5] Without such circumspection, they may inadvertently set precedents that could lead to increased insecurity for their own countries and the global community at large.[6]

---

consensus on possible cooperative measures to address potential threats in the sphere of information security. *See* The Secretary-General, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, ¶ 5, *delivered to the General Assembly*, U.N. Doc. A/60/202 (Aug. 5, 2005) ("[G]iven the complexity of the issues involved, no consensus was reached on the preparation of a final report.").

4. *See* WHITE HOUSE, THE NATIONAL STRATEGY TO SECURE CYBERSPACE, at viii (2003), *available at* http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf ("The speed and anonymity of cyber attacks makes distinguishing among the actions of terrorists, criminals, and nation states difficult, a task which often occurs only after the fact, if at all."); A.A. Streltsov, *International Information Security: Description and Legal Aspects*, DISARMAMENT F., 2007 (Issue 3), at 11 (stating Russia's similar assessment that "it would be challenging to determine whether the attacker was acting in an individual capacity, or on behalf of a criminal organization, the government or armed forces").

5. In the United States, for example, few of the government and military attorneys formulating policy in this area have studied international law overseas or practiced in a foreign legal system. They are predominantly specialists in U.S. administrative law who—owing to both their exclusive training in the Anglo-American common law tradition and their professional focus on domestic legislation and regulatory policy—are unaccustomed to the particular sources, procedures, and modes of legal reasoning employed in public international law. That inexperience also limits their ability to assess how foreign governments will interpret and apply those same provisions.

6. *See infra* note 63 and accompanying text.

II. Territorial Sovereignty

A. Misnomer of a Virtual Jurisdiction

Although some futurists might argue that cyberspace constitutes a realm unto itself which exists beyond all territorial boundaries and cannot be regulated, nation-states do strive to exercise their sovereignty over cyberspace—albeit ineffectively at times.[7] The physical location of actors, victims, and the technical nodes that connect them are of central importance because governments continue to address cyber conflicts involving both state and nonstate actors as matters to be resolved by sovereign powers under their respective legal systems or through bilateral or multilateral agreements with other governments.[8] In the case of cybercrime, for instance, those events that cannot be adequately investigated by local law enforcement authorities or fully prosecuted under domestic criminal systems find recourse to transnational judicial cooperation via mutual-legal-assistance treaties and multilateral organizations, such as the International Criminal Police Organization (INTERPOL).[9] Furthermore, the nature of the international legal system affords this sovereign-centric approach primacy under the United Nations (U.N.) Charter regime.[10]

Every component of every information and telecommunications network around the world, under the sea, and in the air is subject to proprietary interests—whether that of a private company, a sovereign government, or possibly both.[11] Each copper wire, fiber-optic cable, microwave relay tower, satellite transponder, or Internet router has been produced or installed by some entity whose legal successors not only maintain ownership of that physical asset but also expect protection of the same by

---

7. *See, e.g.*, Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEXAS L. REV. 553, 556–57 (1998) (recounting a specific attempt to control pornography on the Internet and the subsequent holding by the U.S. Supreme Court that the law was unconstitutional).

8. *See, e.g.*, Anne Flanagan, *The Law and Computer Crime: Reading the Script of Reform*, 13 INT'L J.L. & INFO. TECH. 98, 109 (2005) (discussing the Council of Europe's promulgation of an international treaty addressing computing and crime as well as a law subsequently passed in the United Kingdom based on the treaty).

9. *See, e.g.*, INTERPOL, Secure Global Police Communications Services, http://www.interpol.int/Public/ICPO/corefunctions/securecom.asp ("INTERPOL developed the I-24/7 global police communications system . . . creating a global network for the exchange of police information and providing law enforcement authorities in member countries with instant access to the organization's databases and other services.").

10. *See* U.N. Charter art. 2, para. 1 ("The Organisation is based on the principle of the sovereign equality of all its Members.").

11. *See, e.g.*, T-Mobile West Corp. v. Crow, No. CV08-1337-PHX-NVW, 2009 WL 5128562, at *15–16 (D. Ariz. Dec. 17, 2009) (discussing the proprietary interest in wireless telecommunications systems); Med. Informatics Eng'g v. Orthopaedics Ne., No. 1:06-CV-173, 2008 WL 4099110, at *6 (N.D. Ind. Sept. 2, 2008) (assuming, without discussion, the existence of proprietary interets in computer software).

sovereign authorities.[12] When those infrastructure elements are emplaced within the terrestrial boundaries, territorial waters, or exclusive airspace of a nation-state, it can exert its sovereign authority over them.[13] Just as with other transnational legal matters, governments may also try to invoke extra-territorial jurisdiction in order to defend the property rights of their nationals' interests.

Even though the ether itself may not be owned per se, legal strictures can be imposed on the means by which wireless communications and media broadcasts are propagated through that medium. National regulations as well as those established under the auspices of the International Telecommunication Union (ITU) allocate electromagnetic frequencies among potential users and proscribe unauthorized interference.[14] Cuba, for example, has repeatedly argued that unauthorized foreign radio and television broadcasts into its territory violate both its national sovereignty and the explicit provisions of international conventions.[15]

In addition to defending physical assets or restricting use of the electromagnetic spectrum, multiple governments have sought to regulate their nations' information spaces by delimiting what content should or should not be made available to their populace even through approved channels. Foreign courts have ordered American Internet service providers to filter certain material from their European Web sites.[16] The member states of the

---

12. *See supra* note 11 and accompanying text.

13. *See* ANTONIO CASSESE, INTERNATIONAL LAW 81 (2d ed. 2005) ("[W]hoever had the physical means of acquiring and effectively controlling a portion of territory on land was legitimized to claim sovereign rights over it.").

14. For example, the Constitution of the ITU states,

> All stations, whatever their purpose, must be established and operated in such a manner as not to cause harmful interference to the radio services or communications of other Member States or of recognized operating agencies, or of other duly authorized operating agencies which carry on a radio service, and which operate in accordance with the provisions of the Radio Regulations.

CONSTITUTION OF THE INTERNATIONAL TELECOMMUNICATION UNION art. 45(1) [hereinafter ITU CONSTITUTION].

15. *See* The Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security*, ¶ 8, *delivered to the General Assembly*, U.N. Doc. A/64/129/Add.1 (Sept. 9, 2009) (claiming that even a U.S. General Accounting Office report from January 2009 "recognizes the violations of international norms and domestic legislation incurred by the programme of radio and television broadcasts by the United States Government against Cuba").

16. *See* Edmund L. Andrews, *German Court Overturns Pornography Ruling Against Compuserve*, N.Y. TIMES, Nov. 18, 1999, at C4 (discussing the prosecution, conviction, and subsequent acquittal on appeal of Compuserve Deutschland executive Felix Somm for failure to filter objectionable material hosted by Compuserve's parent company, a U.S.-based Internet service provider). In May 2000, a French court also sought to impose content limitations on a U.S.-based Internet service provider when it ruled, "We order the Company YAHOO! Inc. to take all necessary measures to dissuade and render impossible any access via Yahoo.com to the Nazi artifact auction service and to any other site or service that may be construed as constituting an apology for Nazism or a contesting of Nazi crimes." Yahoo!, Inc. v. La Ligue Contre le Racisme et L'antisémitisme,

Shanghai Cooperation Organization (SCO)—China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan—have also offered justifications for sovereign controls on informational content in their regional treaty.[17] China and Qatar have each maintained that "the free flow of information should be guaranteed under the premises that national sovereignty and security must be safeguarded"[18] and that "each country has the right to manage its own cyberspace in accordance with its domestic legislation."[19]

Both the infrastructure and content of cyberspace remain subject to national jurisdiction in the eyes of most sovereigns,[20] thereby making effective regulation a question of legal and technical implementation rather than one of right. Once one appreciates that governments seek to extend their sovereign authority into this new realm, it then becomes necessary to analyze how their interests may align or conflict in regard to nonexclusive resources.

B. Misnomer of a Global Commons

Cyberspace has become a critical feature of modern society that manifests the profound interdependencies of all nations. As a result, some commentators are considering whether this new realm should be considered a "global commons" and governed collectively for the common benefit of all mankind (including sovereign states, private companies, individuals, etc.). While the notion of a global commons is not always interpreted consistently, it stems from the two disciplines of international law and political

---

169 F. Supp. 2d 1181, 1185 (N.D. Cal. 2001) (quoting the translation of an order by the High Court of Paris), *rev'd*, 433 F.3d 1199 (9th Cir. 2006).

17. Among the "main threats in the field of ensuring international information security" listed in that treaty is "[d]issemination of information harmful to social and political, social and economic systems, as well as spiritual, moral and cultural spheres of other States." Agreement Between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security art. 2, June 16, 2009 [hereinafter SCO Agreement], *unofficial translation in* INTERNATIONAL INFORMATION SECURITY: THE DIPLOMACY OF PEACE: COMPILATION OF PUBLICATIONS AND DOCUMENTS 202, 203 (Moscow 2009).

18. The Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security*, 7, *delivered to the General Assembly*, U.N. Doc. A/62/98 (July 2, 2007).

19. The Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security*, 4, *delivered to the General Assembly*, U.N. Doc. A/61/161 (July 18, 2006). For Qatar's official submission to the U.N. Secretary-General, see The Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security*, 8, *delivered to the General Assembly*, U.N. Doc. A/63/139 (July 18, 2008) (repeating the relevant portions of the two earlier Chinese submissions almost verbatim).

20. *See* Stephan Wilske & Teresa Schiller, *International Jurisdiction in Cyberspace: Which States May Regulate the Internet?*, 50 FED. COMM. L.J. 117, 129–44 (1997) (applying bases of national jurisdiction, namely the territoriality, nationality, effects, protective, and universality principles, to cyberspace).

economy.[21] In order to ascertain the extent to which cyberspace should (or could effectively) be coordinated as a global commons, one must first understand both the treaty frameworks applied to other so-called commons (e.g., the high seas, outer space, and Antarctica[22]) and the logical criteria that must exist to warrant specialized institutions (such as collective agreements and cultural norms) that ensure communal access to particular resources.

Regarding international legal commons, it is noteworthy that in every case mankind came to those pre-existing regions through discovery; since people had no part in their creation or development, legacy property interests were not of concern. The resulting international agreements specified certain portions of the oceans and airspace as commons (for instance, the high seas beyond 200 nautical miles and outer space above an altitude of approximately 100 kilometers), but they also retained principles of sovereignty regarding both the "territory" within or below those limits and the vessels that ventured into the genuinely common areas of those realms for exploration, commerce, and recreation. Moreover, international law has also developed complex governance mechanisms for the allocation and use of certain key natural resources—such as fisheries, geostationary orbits, and electromagnetic frequencies—within the agreed common areas.[23]

There are two critical considerations when comparing and contrasting cyberspace to existing legal commons. First, the medium itself, while

---

21. For an introduction to the notion of commons under international law, see generally IAN BROWNLIE, PRINCIPLES OF PUBLIC INTERNATIONAL LAW 249–73 (7th ed. 2008) and CASSESE, *supra* note 13, at 81–97. For an introduction to the notion of commons under political economy, see generally ELINOR OSTROM, GOVERNING THE COMMONS: THE EVOLUTION OF INSTITUTIONS FOR COLLECTIVE ACTION (1990).

22. To understand similar agreements relating to other commons, see, for example, United Nations Convention on the Law of the Sea, pt. VII, Dec. 10, 1982, 1833 U.N.T.S. 3 [hereinafter Law of the Sea] (governing the high seas); Agreement Governing the Activities of States on the Moon and Other Celestial Bodies, *adopted* Dec. 5, 1979, 1363 U.N.T.S. 3 (covering outer space); Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, *opened for signature* Jan. 27, 1967, 18 U.S.T. 2410, 610 U.N.T.S. 205 (governing outer space); and Antarctic Treaty, Dec. 1, 1959, 12 U.S.T. 794, 402 U.N.T.S. 71 (covering Antarctica).

23. In regard to fisheries, see, for example, Agreement for the Implementation of the Provisions of the United Nations Convention on the Law of the Sea of 10 December 1982 Relating to the Conservation and Management of Straddling Fish Stocks and Highly Migratory Fish Stocks, *opened for signature* Dec. 4, 1995, S. TREATY DOC. NO. 104-24 (1996), 2167 U.N.T.S. 3 (regulating fisheries in order to promote conservation of migratory and straddling fish stocks) and Convention on Future Multilateral Co-operation in North-East Atlantic Fisheries, Nov. 18, 1980, 1285 U.N.T.S. 129. ITU regulations apply to the use of geostationary orbits and electromagnetic frequencies:

> In using frequency bands for radio services, Member States shall bear in mind that radio frequencies and any associated orbits, including the geostationary-satellite orbit, are limited natural resources and that they must be used rationally, efficiently and economically, in conformity with the provisions of the Radio Regulations, so that countries or groups of countries may have equitable access to those orbits and frequencies, taking into account the special needs of the developing countries and the geographical situation of particular countries.

ITU CONSTITUTION, *supra* note 14, art. 44(2).

subject to the natural laws of physics, has in essence been generated by mankind. Second, even the recognized commons are not treated as such in their entirety. Instead of merely choosing to establish a commons in lieu of adjudicating competing claims of discovery, any legal arbiter of cyberspace would need to override the long-established rights of sovereignty and property ownership recognized by the numerous domestic jurisdictions involved.[24] In addition, well-reasoned and equitable decisions would need to be reached regarding how much, and which specific portions, of cyberspace would be subjected to collective governance.

For example, one can imagine that most nation-states would be adverse to declaring the dedicated information and communication technology networks upon which their government and security apparatuses rely as common resources; yet many of those same nations would also oppose the refusal of any nation to permit its citizenry to enter the "high seas" of cyberspace to exchange ideas and conduct international trade. If sovereignty or property rights are to be recognized for certain portions or applications of cyberspace, then international customs and norms of behavior will have to be agreed upon for transit through or operation within those infrastructure elements rightfully owned by others.[25]

But even before one could attempt to develop cooperative rules for a newly ordained global commons of cyberspace, one would first have to determine if the logical circumstances of the situation warranted such a designation and those concomitant efforts. As decades of academic study have shown, not all resource systems either (a) experience the sort of collective action problems that require open access and communal governance for efficient, sustainable operation or (b) lend themselves to the particular solution embodied in the designation of a commons.[26] The basic principle behind governing the commons for political economists is the need to prevent the overexploitation of resources where no individual actor has the incentive structure necessary to pay the cost of providing a collective good or to constrain his actions in the ways necessary to preserve the future availability of a common resource.[27]

---

24. *See supra* notes 11–13 and accompanying text.

25. Imperfect but useful analogies exist to inform this process, including nonexclusive rights of innocent passage through territorial waters and responsibility for incidental damage to foreign satellites. *See, e.g.*, Law of the Sea, *supra* note 22, arts. 17–32 (governing the right of innocent passage in territorial seas); Convention on the International Liability for Damage Caused by Space Objects, *opened for signature* Mar. 29, 1972, 24 U.S.T. 2389, 961 U.N.T.S. 187 (setting forth liability requirements for damage caused by space objects).

26. For a summary of the required conditions to achieve a sustainable commons see OSTROM, *supra* note 21, at 90 tbl.3.1, 211. For qualitative analyses of public resources and the necessary conditions to overcome collective action problems, see generally RUSSELL HARDIN, COLLECTIVE ACTION (1982) and MANCUR OLSON JR., THE LOGIC OF COLLECTIVE ACTION (rev. ed. 1971).

27. *See* Garrett Hardin, *The Tragedy of the Commons*, 162 SCI. 1243, 1244 (1968) ("Ruin is the destination toward which all men rush, each pursuing his own best interest in a society that believes in the freedom of the commons.").

The aggregate effect of that unfortunate microeconomic reality is often referred to as the "tragedy of the commons."[28] Whether one analyzes communal grazing meadows in Alpine, Switzerland,[29] or fishing limitations under relevant conventions,[30] the same principle maintains. That principle also implies that the notion of a commons which requires collective management will not exist regarding a truly public good (i.e., a resource whose value and availability are not degraded or diminished by other individuals' use of that same resource).[31]

Additional conditions of a true commons are that the affected individuals have insufficient incentives to make investments to properly manage their resources and that a sustainable solution is only possible if reliable mechanisms are established to enforce compliance.[32] It remains uncertain if market forces, or other regulatory options, are capable of providing adequate incentives in cyberspace because technical factors limit reliable identity management, attribution, and deterrence.[33] Cooperative enforcement cannot be fully achieved in cyberspace given the current status of forensic technologies and the incomplete transnational judicial cooperation in many such investigations.[34] In marked contrast, according to the maritime

28. *Id.* at 1243.

29. OSTROM, *supra* note 21, at 62–64 (describing the controls that have prevented overgrazing in Swiss villages).

30. *See, e.g.*, Convention on Future Multilateral Co-operation in North-East Atlantic Fisheries, *supra* note 23 (establishing a commission to help regulate fisheries in the North-East Atlantic).

31. *See* HARDIN, *supra* note 26, at 17 ("Public goods are defined by two properties: *jointness of supply* and *impossibility of exclusion*."); OLSON, *supra* note 26, at 14 ("A common, collective, or public good is here defined as any good such that, if any person X_i in a group $X_1, \ldots, X_i, \ldots, X_n$ consumes it, it cannot feasibly be withheld from the others in that group.").

32. *See* Daniel Fitzpatrick, *Evolution and Chaos in Property Rights Systems: The Third World Tragedy of Contested Access*, 115 YALE L.J. 996, 1001 n.15 (2006) ("A tragedy of the commons arises when insufficient incentives exist for resource conservation and investment in productive capacity, because no user bears all the costs and consequences of his resource use."); Kevin Werbach, *Supercommons: Toward a Unified Theory of Wireless Communication*, 82 TEXAS L. REV. 863, 936–37 (2004) (explaining that every commons does not lead to a tragedy when there are rules and enforcement mechanisms to preserve public character).

33. The inherent difficulty of positively identifying actors in cyberspace and definitively attributing actions to them undermines the basic requirements of a collective action system. As one of her key design principles for successful common-pool resource (CPR) institutions, Nobel laureate Elinor Ostrom has argued that "[i]ndividuals or households who have rights to withdraw resource units from the CPR must be clearly defined, as must the boundaries of the CPR itself." OSTROM, *supra* note 21, at 91. "Furthermore, the long-term sustainability of rules devised at a focal SES [social-ecological system] level depends on monitoring and enforcement as well their not being overruled by larger government policies." Elinor Ostrom, *A Generalized Framework for Analyzing Sustainability of Social-Ecological Systems*, 325 SCI. 419, 422 (2009).

34. *See* Andrew Jacobs, *E-mail Accounts of Activists, Scholars and Journalists Hit by Hackers in China*, N.Y. TIMES, Mar. 31, 2010, at A8 ("[E]xperts point out that attacks appearing to come from a certain location can just as easily be emanating from computers infected with botnets, a virus that allows them [to] be controlled remotely by other computing systems."); John Markoff & David Barboza, *Academic Paper in China Sets Off Alarms in U.S.*, N.Y. TIMES, Mar. 21, 2010, at A10 (discussing the charged atmosphere between the United States and China concerning cybersecurity issues and how difficult it is to respond to incidents because "it is so easy to mask the true source of

model originally instituted under the traditional "law of nations" (the analogue of modern customary international law and the intellectual precursor of codified treaties such as the Law of the Sea), the navies of all sovereign states were empowered to enforce the agreed principles, and in fact, the crime of piracy on the high seas became one of the first peremptory norms subject to universal jurisdiction.[35]

From the political-economy perspective, then, cyberspace in its extant form fails to satisfy two logical criteria for successful treatment as a commons since (i) the underlying physical resources remain subject to private property rights and (ii) the positive identification of legitimate users—as well as the exclusion of illegitimate users—is not yet possible (thereby preventing enforcement of any established norms or collective solutions). One must also consider the economic implications of designating a global commons. History has shown that such systems lack adequate investment and innovation since no single entity can reap the full benefit of its own contributions.[36] They operate best where no maintenance of the medium is required (for instance, naturally occurring realms such as the ocean or outer space) or where the resource will naturally replenish itself—provided that it is not overutilized to the point of exhaustion (e.g., pastures, forests, and fisheries).[37]

Despite the uncertain applicability of either the international law or political-economy conception of a commons to cyberspace, some lessons can still be learned from existing legal frameworks and potentially applied to this new realm. Perhaps one of the most pertinent legal regimes concerns the polar archipelago of Svalbard (also known as Spitsbergen), where economic and ecological resources have been designated for the common benefit of multiple nations.[38] Although Norway bears the legal responsibility and cost

---

a computer network attack"); CYBER SEC. STRATEGY COMM., ESTONIAN MINISTRY OF DEF., CYBER SECURITY STRATEGY 17 (2008), http://www.mod.gov.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf [hereinafter ESTONIAN CYBERSECURITY STRATEGY] ("Since every country can decide for itself whether to co-operate in criminal procedures dealing with cyber attacks, legal solutions for the protection of cyberspace serve their purpose only when implemented in individual countries or when co-operation with other countries on an *ad hoc* basis is possible."); PAUL ROSENZWEIG, AM. BAR ASS'N STANDING COMM. ON LAW & NAT'L SEC., NATIONAL SECURITY THREATS IN CYBERSPACE 2 (2009), http://www.abanet.org/natsecurity/threats_%20in_cyberspace.pdf (asserting that because "the nature of cyberspace is such that we currently lack the technical capacity to attribute actions to the responsible actors with a high degree of confidence[,] . . . practical anonymity is achievable").

35. *See* Bradford R. Clark, *Federal Common Law: A Structural Reinterpretation*, 144 U. PA. L. REV. 1245, 1280 & n.168 (1996) (describing the law maritime as one of the historical branches of the "law of nations"); Kenneth C. Randall, *Universal Jurisdiction Under International Law*, 66 TEXAS L. REV. 785, 791 (1988) ("Piracy is the oldest offense that invokes universal jurisdiction.").

36. *See* Ostrom, *supra* note 33, at 420 (explaining how the increased cost of managing a large resource system undermines the incentive to self-regulate).

37. *See id.* at 419–20 (arguing that resource systems that require lower governance costs can avoid overutilization and destruction).

38. According to the international agreement regarding that archipelago,

> The nationals of all the High Contracting Parties shall have equal liberty of access and entry for any reason or object what[so]ever to the waters, fjords, and ports of

of administering most of the islands' territory, its sovereignty is incomplete and serves largely to preserve those resources in accordance with foreign interests (i.e., right of access for other nations and equal opportunity for economic and scientific activities).[39] This arrangement begins to resemble a trusteeship more than ownership and may represent a feasible alternative to current measures for Internet governance. A second legal paradigm for analogical consideration would be the system that governs international waterways (i.e., inland rivers, straits, and lakes with common rights of access). In this case, although adjacent countries maintain certain sovereign rights, their control is not absolute and must be balanced with the interests of their riparian neighbors as well as international navigation.[40]

Considering (or declaring) cyberspace to be a global commons would require the partial subordination of sovereignty and established property rights in numerous jurisdictions. Neither the sea nor airspace is treated as a commons in its entirety.[41] Likewise, any collective governance structure for cyberspace would also require careful distinction between possessory assets and the true commons. Finally, scholarship in political economy has shown that commons are often prone to collective action problems that encourage misuse while also discouraging investment and innovation. All of these factors will need to be weighed as new strategic and legal paradigms are considered for cyberspace.

III. International Norms

A. Dialogue on Cybersecurity

Thus far, international engagement and cooperation on rules in cyberspace can be divided into three categories: Internet governance, multilateral public policy, and international security.[42] As used herein, the

---

> the territories specified in Article 1; subject to the observance of local laws and regulations, they may carry on there without impediment all maritime, industrial, mining and commercial operations on a footing of absolute equality.

Treaty Concerning the Archipelago of Spitsbergen, art. 3, Feb. 9, 1920, 43 Stat. 1892, 2 L.N.T.S. 7.

39. *Id.* art. 1 ("The High Contracting parties undertake to recognise, *subject to the stipulations of the present Treaty*, the full and absolute sovereignty of Norway over the Archipelago of Spitsbergen . . . .") (emphasis added).

40. *See* BROWNLIE, *supra* note 21, at 261–63 (presenting various formulations of international law that account for riparian interests).

41. *See id.* at 115–16 (explaining that because airspace is appurtenant to territorial land and water, there are constraints on the free navigation of airspace that mirror constraints on the free navigation of international waters).

42. Each of those different subjects is being discussed in numerous forums as various governments seek venues that are most conducive to their own policy interests. According to the White House,

> More than a dozen international organizations—including the United Nations, the Group of Eight, NATO, the Council of Europe, the Asia-Pacific Economic Cooperation forum, the Organization of American States, the Organization of Economic Cooperation and Development, the International Telecommunication

term "Internet governance" refers to the organization, standardization, and technical administration of the Internet's infrastructure.[43] The second rubric of multilateral public policy is meant to describe legal issues that would ordinarily be of domestic concern, except that the interconnected nature of the global information and communication technology (ICT) infrastructure gives them a new transnational dimension.

Those topics include cross-border law enforcement cooperation against cybercrime, the harmonization of data privacy regulations, and the protection of fundamental human rights and civil liberties.[44] Among the most notable international documents to date in this area are the Council of Europe (COE) Convention on Cybercrime[45] and five U.N. General Assembly (UNGA) resolutions[46] from its Second and Third Committees regarding the "creation of a global culture of cybersecurity"[47] and "combating the criminal misuse of information technologies,"[48] respectively.

While each and every one of the topics already mentioned in this section warrants concerted international attention, the remainder of this Article will focus on the third and final category, namely sovereign discourse on international security and arms control in cyberspace.

The potential for military activities in cyberspace raises national security concerns that some states are now seeking to allay through multilateral agreements.[49] Since 1998, the UNGA First Committee—whose

---

> Union (ITU), and the International Organization for Standardization (ISO)—address issues concerning the information and communications infrastructure.

WHITE HOUSE, *supra* note 3, at 20.

43. For a detailed discussion of governmental involvement in those processes and the multiplicity of international organizations related thereto, see Harold Kwalwasser, *Internet Governance*, *in* CYBERPOWER AND NATIONAL SECURITY 491 (Franklin D. Kramer et al. eds., 2009). That chapter summarizes the roles of, *inter alia*, the Domain Name System (DNS), Internet Corporation for Assigned Names and Numbers (ICANN), Internet Assigned Numbers Authority (IANA), Internet Governance Forum (IGF), Internet Engineering Task Force (IETF), Institute of Electrical and Electronics Engineers (IEEE), International Telecommunication Union (ITU), International Organization for Standardization (ISO), and World Wide Web Consortium in the organization and administration of the Internet.

44. *See* WHITE HOUSE, *supra* note 3, at 20 ("[D]iffering national and regional laws and practices—such as those laws concerning the investigation and prosecution of cybercrime; data preservation, protection, and privacy; and approaches for network defense and response to cyber attacks—present serious challenges to achieving a safe, secure, and resilient digital environment.").

45. Council of Europe, Convention on Cybercrime, *opened for signature* Nov. 11, 2001, Europ. T.S. No. 185.

46. G.A. Res. 64/211, U.N. Doc. A/RES/64/211 (Dec. 21, 2009); G.A. Res. 58/199, U.N. Doc. A/RES/58/199 (Dec. 23, 2003); G.A. Res. 57/239, U.N. Doc. A/RES/57/239 (Dec. 20, 2002); G.A. Res. 56/121, U.N. Doc. A/RES/56/121 (Dec. 19, 2001); G.A. Res. 55/63, U.N. Doc. A/RES/55/63 (Dec. 4, 2000).

47. G.A. Res. 64/211, U.N. Doc. A/RES/64/211 (Dec. 21, 2009).

48. G.A. Res. 57/239, U.N. Doc. A/RES/57/239 (Dec. 20, 2002).

49. *See generally* SCO Agreement, *supra* note 17 (setting forth the terms of an agreement governing cooperation in international information security between China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan); MCAFEE, INC., VIRTUAL CRIMINOLOGY REPORT

mandate covers international security and disarmament affairs—has annually passed a resolution entitled "Developments in the field of information and telecommunications in the context of international security" that invites U.N. member states to provide their official views on international information security to the U.N. Secretary-General.[50] But each of the seventy-eight responses submitted by a total of forty-two countries through 2009 remains just that—the expression of a national viewpoint which carries no controlling authority beyond its own borders, although it might play a contributory role in the formation of customary international law over time.[51] Pursuant to

---

13 (2009), http://img.en25.com/Web/McAfee/VCR_2009_EN_VIRTUAL_CRIMINOLOGY_RPT_NOREG.pdf (identifying several countries that are developing cyber-warfare capabilities).

50. G.A. Res. 64/25, U.N. Doc. A/RES/64/25 (Dec. 2, 2009); G.A. Res. 63/37, U.N. Doc. A/RES/63/37 (Dec. 2, 2008); G.A. Res. 62/17, U.N. Doc. A/RES/62/17 (Dec. 5, 2007); G.A. Res. 61/54, U.N. Doc. A/RES/61/54 (Dec. 6, 2006); G.A. Res. 60/45, U.N. Doc. A/RES/60/45 (Dec. 8, 2005); G.A. Res. 59/61, U.N. Doc. A/RES/59/61 (Dec. 3, 2004); G.A. Res. 58/32, U.N. Doc. A/RES/58/32 (Dec. 8, 2003); G.A. Res. 57/53, U.N. Doc. A/RES/57/53 (Nov. 22, 2002); G.A. Res. 56/19, U.N. Doc. A/RES/56/19 (Nov. 29, 2001); G.A. Res. 55/28, U.N. Doc. A/RES/55/28 (Nov. 20, 2000); G.A. Res. 54/49, U.N. Doc. A/RES/54/49 (Dec. 1, 1999); G.A. Res. 53/70, U.N. Doc. A/RES/53/70 (Dec. 4, 1998).

51. *See* The Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security, delivered to the General Assembly*, U.N. Doc. A/64/129/Add.1 (Sept. 9, 2009) [hereinafter *Developments in the Field Add.* (Sept. 9, 2009)]; The Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security, delivered to the General Assembly*, U.N. Doc. A/64/129 (July 8, 2009) [hereinafter *Developments in the Field* (July 8, 2009)]; The Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security, delivered to the General Assembly*, U.N. Doc. A/63/139 (July 18, 2008); The Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security, delivered to the General Assembly*, U.N. Doc. A/62/98/Add.1 (Sept. 17, 2007); The Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security, delivered to the General Assembly*, U.N. Doc. A/62/98 (July 2, 2007); The Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security, delivered to the General Assembly*, U.N. Doc. A/61/161/Add.1 (Oct. 31, 2006); The Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security, delivered to the General Assembly*, U.N. Doc. A/61/161 (July 18, 2006); The Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security, delivered to the General Assembly*, U.N. Doc. A/60/95/Add.1 (Sept. 21, 2005); The Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security, delivered to the General Assembly*, U.N. Doc. A/60/95 (July 5, 2005); The Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security, delivered to the General Assembly*, U.N. Doc. A/59/116/Add.1 (Dec. 28, 2004) [hereinafter *Developments in the Field Add.* (Dec. 28, 2004)]; The Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security, delivered to the General Assembly*, U.N. Doc. A/59/116 (June 23, 2004) [hereinafter *Developments in the Field* (June 23, 2004)]; The Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security, delivered to the General Assembly*, U.N. Doc. A/58/373 (Sept. 17, 2003); The Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security, delivered to the General Assembly*, U.N. Doc. A/57/166/Add.1 (Aug. 29, 2002); The Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security, delivered to the General Assembly*, U.N. Doc. A/57/166 (July 2, 2002); The Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of*

those UNGA resolutions from 2005 through 2009, a second U.N. group of governmental experts has been convened during 2009–2010 to consider international information security.[52]

The U.N. Institute for Disarmament Research sponsored meetings in 1999 and 2008 to further explore international information security[53] and even dedicated an issue of its quarterly journal to this topic in 2007.[54] Several regional organizations—such as the SCO, the North Atlantic Treaty Organization (NATO), and the Organization for Security and Cooperation in Europe (OSCE)—have also begun dialogues on legal measures to ensure international information security and respond to cyber attacks.[55] Although many of these U.N. and regional initiatives have not yielded concrete results

---

International Security, delivered to the General Assembly, U.N. Doc. A/56/164/Add.1 (Oct. 3, 2001); The Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security, delivered to the General Assembly*, U.N. Doc. A/56/164 (July 3, 2001) [hereinafter *Developments in the Field* (July 3, 2001)]; The Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security, delivered to the General Assembly*, U.N. Doc. A/55/140/Add.1 (Oct. 3, 2000); The Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security, delivered to the General Assembly*, U.N. Doc. A/55/140 (July 10, 2000); The Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security, delivered to the General Assembly*, U.N. Doc. A/54/213 (Aug. 10, 1999) (providing various state contributions to the Secretary-General).

52. G.A. Res. 64/25, ¶ 4, U.N. Doc. A/RES/64/25 (Dec. 2, 2009); G.A. Res. 63/37, ¶ 4, U.N. Doc. A/RES/63/37 (Dec. 2, 2008); G.A. Res. 62/17, ¶ 4, U.N. Doc. A/RES/62/17 (Dec. 5, 2007); G.A. Res. 61/54, ¶ 4, U.N. Doc. A/RES/61/54 (Dec. 6, 2006); G.A. Res. 60/45, ¶ 4, U.N. Doc. A/RES/60/45 (Dec. 8, 2005). In 2009, the U.N. Secretary-General's Advisory Board on Disarmament Affairs was also tasked to study the issue of "cyber warfare and its impact on international security." Sergio Duarte, U.N. High Representative for Disarmament Affairs, Opening Remarks to the Advisory Board on Disarmament Matters (Feb. 18, 2009), *available at* http://www.pfcmc.com/disarmament/HomePage/HR/docs/2009/2009Feb18HRToABDM.pdf; *accord* Ban Ki-moon, U.N. Sec'y-Gen., Remarks to the Advisory Board on Disarmament Matters (Feb. 18, 2009), *available at* http://www.unrcpd.org.np/uploads/library/file/Statement%20cyberwarfare.pdf.

53. Conference, *Information & Communications Technologies and International Security*, U.N. INST. FOR DISARMAMENT RES. (April 24–25, 2008), *audio available at* http://www.unidir.org/audio/2008/Information_Security/en.htm; Private Discussion Meeting, *Developments in the Field of Information and Telecommunications in the Context of International Security*, DEP'T OF DISARMAMENT AFF. & U.N. INST. FOR DISARMAMENT RES. (Aug. 25–26, 1999).

54. Colloquy, *ICTs and International Security*, DISARMAMENT F., 2007 (Issue 3).

55. *See* SCO Agreement, *supra* note 17 (memorializing the terms of the agreement regarding cooperation in international information security between members of the SCO); Vladislav Sherstyuk, Deputy Dir., Sec. Council of the Russian Fed'n, Keynote Presentation at Working Session I of the OSCE Workshop on a Comprehensive OSCE Approach to Enhancing Cyber Security (Mar. 18, 2009) (translated transcript on file with Texas Law Review) (advocating new legal measures to combat hostile uses of information and communications technology); James Stavridis, NATO Supreme Allied Commander Eur., SACEUR Address to the Armed Forces Communications and Electronics Association (Feb. 2, 2010), *available at* http://www.aco.nato.int/page27750625.aspx?print=y (proposing that NATO's reciprocal protection for members be extended to include cyber attacks). The NATO-accredited Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia, has also organized professional conferences on this topic. *See, e.g.*, Press Release, Coop. Cyber Def. Ctr. of Excellence, President of Estonia opened International Cyber Conflict Legal and Policy Conference (Sept. 9, 2009), http://www.ccdcoe.org/149.html ("[W]e are making our way to tackle the bottlenecks in cyber conflict legal and policy areas.").

yet (with the SCO being a notable exception[56]), it is clear that the international community sees cyber conflict between sovereign nations as a growing concern worthy of increased legal attention.

B. Sources of Customary International Law

Public international law represents an amalgam of different legal systems that also contains its own unique elements. The Statute of the International Court of Justice (ICJ)—a treaty to which all U.N. members are party *ipso facto* by its incorporation into the U.N. Charter[57]—lists the appropriate sources of international law that the ICJ may rely upon in rendering its decisions.[58] Notable among those sources are "international custom, as evidence of a general practice accepted as law" and "the general principles of law recognized by civilized nations," which together form the basis of customary international law.[59] The Statute of the International Law Commission (ILC)—the U.N. organ tasked with codifying and promulgating international law—provides further guidance on the sources of customary international law.[60] Article 19 of that Statute directs the ILC to obtain "texts of laws, decrees, judicial decisions, treaties, diplomatic correspondence and other documents relevant to the topic being studied" from the governments of U.N. member states.[61] Similarly, Article 20 calls for "[a]dequate presentation of precedents and other relevant data, including treaties, judicial

---

56. *See* Pan Guang, *The SCO's Success in Security Architecture* (highlighting confidence building, cooperation against destabilizing transborder elements, and the maintenance of regional security and stability as general successes of the SCO), *in* THE ARCHITECTURE OF SECURITY IN THE ASIA-PACIFIC 33, 33–34 (Ron Huisken ed., 2009).

57. U.N. Charter arts. 92–93.

58. Statute of the International Court of Justice art. 38(1), June 26, 1945, 59 Stat. 1055, 1060, T.S. No. 993 [hereinafter ICJ Statute]. According to the ICJ Statute,

> The Court, whose function is to decide in accordance with international law such disputes as are submitted to it, shall apply:
>
> (a) international conventions, whether general or particular, establishing rules expressly recognized by the contesting states;
>
> (b) international custom, as evidence of a general practice accepted as law;
>
> (c) the general principles of law recognized by civilized nations;
>
> (d) subject to the provisions of Article 59, judicial decisions and the teachings of the most highly qualified publicists of the various nations, as subsidiary means for the determination of rules of law.

Id.

59. *Id.*

60. Pursuant to its authorities under the U.N. Charter, the UNGA has resolved that "[t]he International Law Commission shall have for its object the promotion of the progressive development of international law and its codification." G.A. Res. 174 (II), art. 1(1), U.N. Doc. A/519 (Nov. 21, 1947) [hereinafter ILC Statute]. "[T]he expression 'codification of international law' is used for convenience as meaning the more precise formulation and systematization of rules of international law in fields where there already has been extensive state practice, precedent and doctrine." *Id.* art. 15.

61. *Id.* art. 19(2).

decisions and doctrine."[62] Since both the ICJ and ILC Statutes clearly indicate state practice to be a legitimate—and guiding—source of customary international law, they confirm that what sovereign governments do and say directly affects the law itself.[63]

Nothing could be more critical in the context of cyberspace; for in the absence of historical precedents and codified rules, new international norms are being created by those government officials who are rendering legal opinions, declaring national security policies, formulating military doctrines, establishing rules of engagement, and otherwise providing evidence of state practice. Moreover, state actors seeking national advantage through cyber conflict have the opportunity to resist multilateral constraints by both rejecting treaty mechanisms and also taking certain military actions that would set precedents for the future. Conversely, multilateral efforts—such as the impending report from the current U.N. group of governmental experts—could serve to establish some norms of behavior in cyberspace that would delineate what is not acceptable to the international legal community. Perhaps there will be an international cyber-arms-control instrument in the future, but that seems unlikely in the near term. Until then, state practice remains the primary source of customary international law on this topic.

C. State Practice in Cyberspace

The modern rules of *jus ad bellum*, or the principles of just war, are derived from the U.N. Charter. Although one can easily locate references to "acts of aggression,"[64] "the threat or use of force,"[65] and "armed attack,"[66] those terms all remain undefined in the Charter itself. "The difficulties are exacerbated by the absence of any generally accepted interpretations of [those] concepts . . . in relation to information security."[67] Even though other nonbinding sources of "soft law" have attempted to clarify those terms,[68]

---

62. *Id.* art. 20(a).

63. As a "means for making the evidence of customary international law more readily available," the ILC is explicitly tasked to collect and publish "documents concerning State practice and of the decisions of national and international courts on questions of international law." *Id.* art. 24. For additional discussion of state practice and related sources of customary international law, see Ways and Means for Making the Evidence of Customary International Law More Readily Available, *in* Report of the International Law Commission Covering Its Second Session ¶¶ 24–94, U.N. GAOR, 5th Sess., Supp. No. 12, at 4–10, U.N. Doc. A/1316 (1950).

64. U.N. Charter art. 1, para. 1.

65. *Id.* art. 2, para. 4.

66. *Id.* art. 51.

67. *Developments in the Field Add.* (Sept. 9, 2009), *supra* note 51, at 7; *see also* Streltsov, *supra* note 4, at 9 (providing a nearly verbatim assessment of the definitional and interpretative problems); ESTONIAN CYBER SECURITY STRATEGY, *supra* note 34, at 17 ("Several terms, such as *cyber warfare*, *cyber attack*, *cyber terrorism*, or *critical information infrastructure*, have not been defined clearly. Everywhere they are used, but their precise and intended meaning will vary depending on the context.").

68. *See, e.g.*, G.A. Res. 3314 (XXIX), Annex art. 1, U.N. Doc. A/9631 (Dec. 14, 1974) ("Aggression is the use of armed force by a State against the sovereignty, territorial integrity or

sovereign governments actively seek to influence the legal interpretations of those provisions when they formulate national security strategies and issue declaratory policy statements. Mali, for instance, has claimed,

> The use of an information weapon could be interpreted as an act of aggression if the victim State has reasons to believe that the attack was carried out by the armed forces of another State and was aimed at disrupting the operation of military facilities, destroying defensive and economic capacity, or violating the State's sovereignty over a particular territory.[69]

The United States and Russia have both made pronouncements that cyber conflicts could have significant impacts on national security and that they will take necessary measures to protect their information infrastructures.[70] Each of those countries plays a leading role in world affairs—*inter alia* as permanent members of the U.N. Security Council—so how they decide to "deter, prevent, detect, and defend against" cyber attacks and "recover quickly from any disruptions or damage" will set a precedent for the rest of the world.[71] Their state practice in developing military capabilities for cyberspace[72] will also serve as a model for others. As one

---

political independence of another State, or in any other manner inconsistent with the Charter of the United Nations . . . .").

69. *Developments in the Field Add.* (Sept. 9, 2009), *supra* note 51, at 8.

70. President Barack Obama declared, "From now on, our digital infrastructure—the networks and computers we depend on every day—will be treated as they should be: as a strategic national asset. Protecting this infrastructure will be a national security priority." Barack Obama, U.S. President, Remarks on Securing Our Nation's Cyber Infrastructure (May 29, 2009), http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure. Similarly, Russia has stated, "The information weapon is particularly dangerous when used against military and civilian buildings and State systems and institutions, the disruption of the normal functioning of which constitutes a direct threat to national security." The Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security*, 2, *delivered to the General Assembly*, U.N. Doc. A/56/164/Add.1 (Oct. 3, 2009); *see also* Doctrine of the Information Security of the Russian Federation art. 1, *approved* June 23, 2000 [hereinafter Russian Information Security Doctrine] ("The national security of the Russian Federation depends to a substantial degree on ensuring the information security, a dependence that will increase with technological progress."), *reprinted in* RUSSIAN MEDIA LAW AND POLICY IN THE YELTSIN DECADE 492 (Monroe E. Price et al. eds., 2002).

71. Obama, *supra* note 70.

72. According to one U.S. military leader,

> In this emerging war-fighting domain, USSTRATCOM, through the Joint Task Force for Global Network Operations (JTF-GNO) and the Joint Functional Component Command for Network Warfare (JFCC-NW), in partnership with the Joint Staff is leading the planning and execution of the National Military Strategy for Cyberspace Operations. In this role, we coordinate and execute operations to defend the Global Information Grid (GIG) and project power in support of national interests.

United States Strategic Command: Hearing Before the Strategic Forces Subcomm. of the H. Armed Servs. Comm., 110th Cong. (2008) (statement of Gen. Kevin P. Chilton, Commander, U.S. Strategic Command), *available at* http://armedservices.house.gov/pdfs/STRAT022708/Chilton_Testimony022708.pdf; *see also* Military Doctrine of the Russian Federation ¶ 41(c), Feb. 5, 2010, *unofficial translation available at* http://merln.ndu.edu/whitepapers/Russia2010_English.pdf

member of the Russian delegation to the U.N. group of governmental experts on international information security has written, "There is no doubt that information weapons can be used in practice. Some armed forces are already preparing special units for military operations using ICTs."[73]

A similar process of state practice informing customary international law is also underway regarding the rules of *jus in bello* that comprise international humanitarian law (IHL), also known as the law of armed conflict. Although the Geneva Conventions and other treaty instruments have endeavored to codify general principles for the conduct of armed conflicts (including necessity, proportionality, distinction, discrimination, and humanity),[74] the development of new technologies always presents

(stating the Russian armed forces' requirement to develop forces and resources for information confrontation); Memorandum from Sec'y of Def. on Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations (June 23, 2009), *available at* http://www.defense.gov/home/features/2010/0410_cybersec/docs/cyber_command_gates_memo%5B1%5D.pdf (establishing a subordinate unified U.S. Cyber Command under U.S. Strategic Command for military cyberspace operations).

73. Streltsov, *supra* note 4, at 8; *see also* AUSTL. MINISTRY OF DEF., DEFENDING AUSTRALIA IN THE ASIA PACIFIC CENTURY: FORCE 2030, at 83 (2009), *available at* http://www.defence.gov.au/whitepaper/docs/defence_white_paper_2009.pdf ("The [Australian] Government has decided to invest in a major enhancement of Defence's cyber warfare capability."); REPUBLIC OF FR., THE FRENCH WHITE PAPER ON DEFENCE AND NATIONAL SECURITY 12 (2008), *translated summary available at* http://www.ambafrance-ca.org/IMG/pdf/Livre_blanc_Press_kit_english_version.pdf (prescribing France's "establishment of an offensive cyber-war capability, part of which will come under the Joint Staff and the other part will be developed within specialised services"); U.K. CABINET OFFICE, CYBER SECURITY STRATEGY OF THE UNITED KINGDOM 14 (2009) [hereinafter UK CYBERSECURITY STRATEGY], *available at* http://www.cabinetoffice.gov.uk/media/216620/css0906.pdf ("We recognise the need to develop military capabilities . . . to ensure we can defend against attack, and take steps against adversaries where necessary.").

74. *See, e.g.*, Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects, Oct. 10, 1980, S. TREATY DOC. NO. 103-25 (1994), 1342 U.N.T.S. 137; Protocol I on Non-Detectable Fragments, Oct. 10, 1980, S. TREATY DOC. NO. 103-25 (1994), 1342 U.N.T.S. 168; Protocol II on Prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices, Oct. 10, 1980, S. TREATY DOC. NO. 105-1(A) (1997), 1342 U.N.T.S. 168; Protocol III on Prohibitions or Restrictions on the Use of Incendiary Weapons, Oct. 10, 1980, S. TREATY DOC. NO. 105-1(B) (1997), 1342 U.N.T.S. 171; Protocol IV on Blinding Laser Weapons, Oct. 13, 1995, S. TREATY DOC. NO. 105-1(C) (1997), 35 I.L.M. 1218; Geneva 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 [hereinafter Geneva Convention I]; Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of the Armed Forces at Sea, Aug. 12, 1949, 6 U.S.T. 3217, 75 U.N.T.S. 85 [hereinafter Geneva Convention II]; Geneva Convention Relative to the Treatment of Prisoners of War, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135 [hereinafter Geneva Convention III]; Geneva Convention Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287 [hereinafter Geneva Convention IV]; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) art. 58, *opened for signature* Dec. 12, 1977, 1125 U.N.T.S. 3 [hereinafter Geneva Protocol I]; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), *opened for signature* Dec. 12, 1977, 1125 U.N.T.S. 609 [hereinafter Geneva Protocol II]. As used herein, "Geneva Conventions" collectively refers to Geneva Convention I, Geneva Convention II, Geneva Convention III, Geneva Convention IV, Geneva Protocol I, and Geneva Protocol II.

difficulties for imposing limitations on the means and methods of warfare.[75] Sovereign nations not only negotiate such agreements cognizant of their own military strengths and weaknesses but also base their military doctrines and rules of engagement on their own interpretations of the relevant treaties and customary international law.[76] Without any controlling legal authorities for cyber conflicts today, there remains broad room for maneuver—both diplomatically and militarily.

Two of the key debates within the international community are (i) the extent to which the existing rules and norms of IHL are sufficiently applicable to cyber conflicts[77] and (ii) whether there is a need for *lex specialis* disarmament measures regarding information weapons.[78] Speaking on behalf of the European Union (EU) in 2001, Sweden made a submission to the U.N. Secretary-General:

> EU is not of the view that, within the context of the General Assembly, the First Committee should be the main forum for discussing the issue of information security. Since the question mainly encompasses subjects other than disarmament and international security, EU believes there are other committees better suited for discussion of at least some of the aspects of the issue.[79]

Then in 2004, both the United States and the United Kingdom officially specified that they opposed an international treaty limiting the military use of ICTs. Moreover, they each declared that current IHL provisions adequately "govern the use of such technologies."[80]

---

75. *See* CASSESE, *supra* note 13, at 402–03 (arguing that one of the major factors rendering the traditional international law of armed conflict "defective or inadequate in many respects" and thereby leading to the development of a new international body of law governing armed conflict was the development of "new agencies of destruction" such as the airplane and the atomic bomb (emphasis omitted)); Sean Watts, *Combatant Status and Computer Network Attack*, 50 VA. J. INT'L L. 391, 392 (2010) ("Military legal history has demonstrated that the law of war's efficacy is a function of the law's ability to keep pace with, as well as to address, how war is waged."); *cf.* Kelly A. Gable, *Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent*, 43 VAND. J. TRANSNAT'L L. 57, 88 (2010) (arguing that despite the number of governmental efforts utilized to encourage international cooperation in combating the "seemingly endless array" of cyber terrorist methods, "[n]one . . . is capable of completely securing the Internet").

76. *Cf.* CASSESE, *supra* note 13, at 399 (highlighting the self-serving nature of nation-states and how that nature affects international law's ability to constrain state actions).

77. *See* Watts, *supra* note 75, at 393 (remarking on the myriad legal issues—from "'victims' right to resort to force and the lawful use of preemptive or defensive [computer network attacks (CNAs)] (so-called *jus ad bellum* issues), to analyses of how the law regulating the conduct of hostilities (the *jus in bello*) applies to CNAs"—being debated regarding the adequacy of the law of war in the face of emerging uses of offensive CNAs).

78. *See id.* at 394 ("While assessments range from conclusions that existing law is largely adequate, to arguments to abandon the extant law entirely, to calls to draft a new *lex specialis*, broad consensus exists that CNAs producing destructive effects fully implicate law-of-war restraints and authorizations, both codified and customary.").

79. *Developments in the Field* (July 3, 2001), *supra* note 51, at 5.

80. The relevant portion of the U.K. submission reads,

On the other hand, the parties to the SCO agreement, including Russia and China, have recognized a need to elaborate "collective measures regarding development of norms of international law to curb proliferation and use of information weapons that endangers the defensive capability, national and public security."[81] Although not a member of the SCO, Brazil forwarded a very similar position in its 2009 submission to the U.N. Secretary-General, asserting that "[t]he United Nations should also play a leading role in the discussions on the use of information and telecommunications as cyberwarfare in interstate conflict situations, paying special attention to the following aspects: . . . Establishment of a code of conduct for the use of information weapons."[82]

The net observation of state practice regarding the need for a *lex specialis* concerning the military use of ICTs is profound disagreement. Not only are there no generally accepted views at this time but the permanent members of the U.N. Security Council are themselves divided with the United States, United Kingdom, and France (presuming its concurrence with the 2001 EU submission) opposing new binding rules, while Russia and China would ostensibly favor them.[83] It is worth noting, however, that some of those official statements are several years old, and national policy positions may have changed. For example, President Obama's speech on May 29, 2009, and the related White House Cyberspace Policy Review may have signaled a new willingness to discuss cyber conflicts as a matter of international security (and possibly arms control)—even though the United States is not yet prepared to negotiate any formally binding instruments.[84]

What nations do of their own accord and how they respond to others' actions will serve as precedents for future cyber conflicts. State practice creates a dual-track, recursive process by which sovereign governments individually or collectively interpret the rules of *jus ad bellum* and *jus in bello*; produce their own national strategies, declaratory policies, military doctrines, and rules of engagement; and then conduct activities that in turn influence

---

> The United Kingdom does not, however, believe that there is a need for a multilateral instrument that would restrict the development or use of certain civil and/or military technologies. With respect to military applications of information technologies, such an instrument is unnecessary. The law of armed conflict, in particular the principles of necessity and proportionality, governs the use of such technologies.

Developments in the Field (June 23, 2004), *supra* note 51, at 11. The U.S. submission was equally clear in its determination: "With respect to military applications of information technology, an international convention is completely unnecessary. The law of armed conflict and its principles of necessity, proportionality, and limitation of collateral damage already govern the use of such technologies." *Developments in the Field Add.* (Dec. 28, 2004), *supra* note 51, at 4.

81. SCO Agreement, *supra* note 17, art. 3.

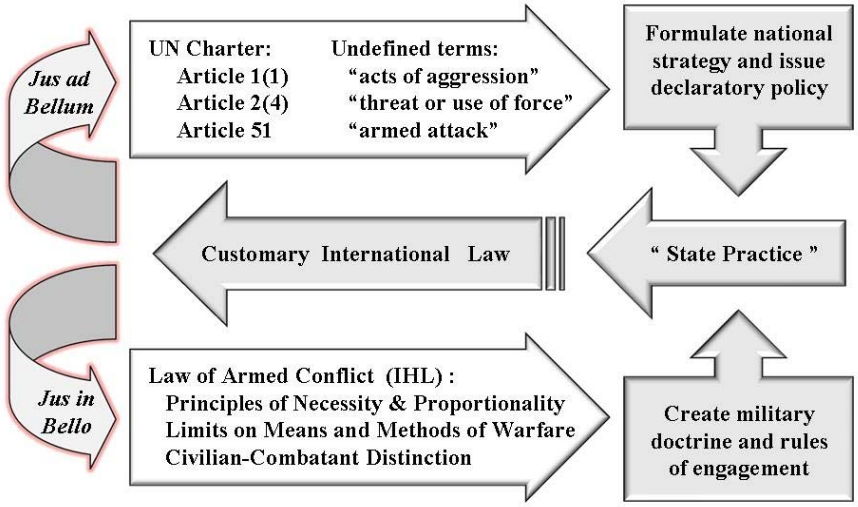
82. *Developments in the Field* (July 8, 2009), *supra* note 51, at 3–4.

83. *See supra* notes 78–82 and accompanying text.

84. *See* WHITE HOUSE, *supra* note 3 (providing a framework for engaging in international discussions about cybersecurity); Obama, *supra* note 70 (framing the problem of cybersecurity as an international problem).

customary international law and the future application of the U.N. Charter, Geneva Conventions, and other IHL provisions.

Development Cycle of International Norms for State Actors in Cyberspace



IV. Strategic Considerations

A. State Responsibility

Besides playing an active role in the formation of customary international law through statecraft, sovereign nations also seek to pursue and protect their national interests while complying with accepted legal obligations. Having already examined the notion of sovereignty as it is being projected onto cyberspace and the importance of state practice, it is necessary to consider several substantive principles of public international law that have practical import when considering cyber conflicts. The inability to attribute deleterious events in a timely fashion was already acknowledged above, and one must now recognize that any sovereign efforts to regulate or monitor their national cyberspace not only require substantial resources but may also conflict with other public-policy interests, such as privacy and free speech. Even if sovereign control were desirable, publicly available technology has simply outpaced the ability of governments to perform fully effective law enforcement and national security procedures.[85]

85. Interestingly, this is true of both developing nations whose state organs do not have the technical competence, requisite hardware and software, or judicial capacity to enforce laws as well as highly developed nations like the United States—whose legal culture currently precludes the level of systematic authentication and monitoring that would be necessary to completely quash

So, despite the pervasive will to exert sovereign authority over cyberspace, no state is currently able to completely deter, prevent, or even detect unwanted activity on or emanating from its ICT networks.[86] This limitation is a critical obstacle to applying the principle of state responsibility to the effects of state and nonstate actors alike. During the deliberations of the U.N. group of governmental experts in January 2010, for example, China proposed that sovereign states "have the responsibilities and rights to take necessary management measures to keep their domestic cyberspace and related infrastructure free from threats, disturbance, attack and sabotage."[87] India was even more explicit in its discussion of that same topic:

> By creating a networked society and being a part of [a] global networked economy, it is necessary for nation states to realise that they not only have a requirement to protect their own ICT infrastructure but at the same time have a responsibility to ensure that their ICT is not abused, either covertly or overtly, by others to target or attack the ICT infrastructure of another nation state.[88]

Although this represents the same theory of imputed accountability for failure of a sovereign to mitigate nonstate actor threats to international peace and security that has been relied upon to impose liability in other circumstances—such as the refusal or inability of the de facto government of Afghanistan to prevent the Taliban and al Qaeda from planning and conducting terrorist operations from Afghan territory[89]—it is unclear that any state is prepared (politically or technologically) to take full responsibility for all harm emanating from gateway routers, very small aperture terminals

---

cyber threats. *See* WHITE HOUSE, *supra* note 3 (stating that reform of U.S. legal structures is necessary to meet the changing needs of modern cybersecurity). In addition, many sovereign governments do not own or directly administer the critical information infrastructures in their countries—including the networks on which their own government and military entities rely. Finally, one cannot overlook the simple economic trade-off between the security and functionality of ICT networks. Thus far, no nation has made the necessary investment to develop a fully secure and functionally operative information infrastructure.

86. *See generally* ROSENZWEIG, *supra* note 34, at 14 ("The doctrine of 'State responsibility' has long been an established international law concept, but it has become particularly relevant in terms of assessing responsibility for cyber attacks.").

87. China's Contribution to the Report of the U.N. Group of Governmental Experts on Information Security 3 (January 2010) (on file with Texas Law Review).

88. India's Contribution to the Report of the U.N. Group of Governmental Experts on Information Security 3 (January 2010) (on file with Texas Law Review). Russia alluded to the same principle when it asserted, "States and other subjects of international law should refrain of such actions against each other and should bear responsibility at international level for such actions in information space, carried out directly, under their jurisdiction or in the framework of international organizations of their membership." Russia's Contribution to the Report of the U.N. Group of Governmental Experts on Information Security 5 (January 2010) (on file with Texas Law Review).

89. *See, e.g.*, Elisabeth Bumiller, *Bars Talks, Saying Hosts Will Share the Terrorists' Fate*, N.Y. TIMES, Sept. 21, 2001, at A1 ("President Bush demanded tonight that Afghanistan's leaders immediately deliver Osama bin Laden and his network and close down every terrorist camp in the country or face military attack by the United States.").

(VSATs), wireless mobile devices, and other devices within its territory or jurisdiction.[90] Any sovereign's decision to support an international norm of state responsibility in cyberspace would need to be as much a practical consideration as one of legal principle.

According to two distinguished international-law scholars, Antonio Cassese and Ian Brownlie, the appropriate legal analysis for attributing responsibility for the actions of nonstate actors to host states themselves would necessarily rest upon the degree of due diligence or negligence exhibited by the sovereign.[91] In other words, the state would not be held responsible for the act itself but would rather be held accountable for failing to fulfill a legal obligation that would have prevented the attendant harm. Outside the cyber context, the ILC has proposed that "[t]he State of origin shall take all appropriate measures to prevent significant transboundary harm or at any event to minimize the risk thereof."[92] In the absence of any international consensus on the norms for cyberspace, it would be very difficult to determine whether a state had performed adequate due diligence or taken the appropriate measures to avert harm in cyberspace.

B. International Humanitarian Law

The potential for cyber conflicts also poses several other legal and strategic difficulties concerning the notions of neutrality, perfidy, distinction, and humanity under existing IHL. While that list of topics is not exhaustive and none of them will be fully addressed or resolved here, they are all worth

---

90. This topic raises numerous legal and technical issues—including common-carrier provisions under U.S. telecommunications law and the requisite level of effective territorial control for legitimate sovereignty under public international law—that will not be addressed in any detail here due to space limitations.

91. Antonio Cassese states,

> In the case of unlawful acts committed by *individuals not acting as de facto State officials*, for instance against foreigners or foreign authorities, the State on whose territory the acts were committed incurs international responsibility only if it did not act with due diligence: if it omitted to take the necessary measures to prevent attacks on foreigners or foreign assets, or, after perpetration of the unlawful acts, failed to search for and duly punish the authors of those acts, as well as pay compensation to the victims.

CASSESE, *supra* note 13, at 250. Ian Brownlie has similarly concluded,

> There is general agreement among writers that the rule of non-responsibility cannot apply where the government concerned has failed to show due diligence. However, the decisions of tribunals and the other sources offer no definition of 'due diligence.' Obviously no very dogmatic definition would be appropriate, since what is involved is a standard which will vary according to the circumstances. And yet, if 'due diligence' be taken to denote a fairly high standard of conduct the exception would overwhelm the rule.

BROWNLIE, *supra* note 21, at 455.

92. Draft Articles on Prevention of Transboundary Harm from Hazardous Activities art. 1, *in* Report of the International Law Commission on the Work of Its Fifty-Third Session, U.N. GAOR, 56th Sess., Supp. No. 10, at 372, U.N. Doc. A/56/10 (Apr. 23, 2001–Aug. 10, 2001).

examining briefly because they collectively illustrate just how problematic certain aspects of cyber conflicts could be for the law.

If states cannot effectively monitor or control the data packets transiting their ICT networks or the electromagnetic waves permeating their airspace, then the traditional concept of neutrality may have to be revisited before it can be applied to cyber conflicts. Normally, belligerents are prohibited from using a neutral state's territory to deploy armaments or mount an armed attack.[93] Furthermore, a state can only maintain its neutrality by remaining impartial vis-à-vis opposing belligerents.[94] But, what if a neutral party did not know when its sovereignty was breached to conduct an attack or was technically incapable of restricting belligerents' use of its ICT networks without irreparably harming its own governmental functions or economy? What if the tools required to conduct or defend against a cyber attack needed to be pre-positioned in global networks to be most efficacious? What if a sovereign did not exercise due diligence in preventing its own subjects from criminally compromising foreign computer systems and later using them to attack a third sovereign nation?

The question of neutrality becomes even more complicated due to the uncertain legal status of cyberspace. If it is considered sovereign territory, then "[b]elligerents are forbidden to move troops or convoys of either munitions of war or supplies across the territory of a neutral Power."[95] If, however, it is deemed a partial or complete commons, then perhaps "[t]he neutrality of a Power is not affected by the mere passage through its territorial waters of war-ships or prizes belonging to belligerents."[96] The analogy to information weapons (and the potential "prizes" of cyber conflict) transiting foreign ICT nodes is evident, but the appropriate legal norm is far from clear because the traditional notion of neutrality depends on both observable actions and the agreed legal status of the relevant medium where they take place.[97]

Another long-standing principle of IHL is the prohibition on perfidy, which precludes "[a]cts inviting the confidence of an adversary to lead him

---

93. Convention Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land arts. 1–4, Oct. 18, 1907, 36 Stat. 2310, 1 Bevans 654 [hereinafter Hague Convention V].

94. While "[a] neutral Power is not called upon to forbid or restrict the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraphy apparatus belonging to it or to companies or private individuals . . . . Every measure of restriction or prohibition taken by a neutral Power . . . must be impartially applied by it to both belligerents." *Id.* arts. 8–9.

95. *Id.* art. 2.

96. Convention Concerning the Rights and Duties of Neutral Powers in Naval War art. 10, Oct. 18, 1907, 36 Stat. 2415, 1 Bevans 723 [hereinafter Hague Convention XIII].

97. *See id.* art. 1 ("Belligerents are bound to respect the sovereign rights of neutral Powers and to abstain, in neutral territory or neutral waters, from any act which would, if knowingly permitted by any Power, constitute a violation of neutrality."). Not only is it unclear what would constitute a violation of neutrality in cyberspace, but it is equally questionable that a sovereign would even know when its rights had been violated in order to defend and preserve its neutrality.

to believe that he is entitled to, or is obliged to accord, protection under the rules of international law applicable in armed conflict, with intent to betray that confidence."[98] Combatants are required to have distinctive signs or emblems and carry their arms openly;[99] accordingly, they are forbidden from feigning civilian, noncombatant status or using the insignia of enemy combatants during an attack.[100] The problematic nature of attribution in cyberspace, however, makes it nearly impossible to distinguish between the actions of lawful combatants (whether friend or adversary) and those of civilians. Without the equivalent of military emblems on information weapons, it becomes incredibly difficult to adhere to the principle of distinction and honor the prohibition against perfidy.[101]

From a strategic perspective, the IHL principles regarding perfidy, treachery, and chivalry are intended to ensure that certain humanitarian actions remain possible even during violent conflicts. Without them, quarter and succor would not be given, surrender would not be credible, and armistice would be meaningless. In a virtual realm where one could not identify the adversary, maintain the integrity of established symbols, or even trust the authenticity of directives allegedly issued by one's own chain of command, uncertainty would reign and the human suffering of combatants and civilians alike could increase. Even those military strategists who compare cyber conflict to aerial warfare will know that IHL historically sought to apply these same principles to that medium.[102]

The principles of distinction and discrimination also require that sovereigns take precautions to protect civilian entities from the dangers of war.[103] "[T]o the maximum extent feasible," they are required to "remove the civilian population, individual civilians and civilian objects under their control from the vicinity of military objectives" as well as to "avoid locating military objectives within or near densely populated areas."[104] Furthermore, they are prohibited from using civilians to "render certain points or areas immune from military operations."[105] Those legal obligations to physically

98. Geneva Protocol I, *supra* note 74, art. 37(1).

99. Geneva Convention III, *supra* note 74, art. 4(A)(2); Geneva Protocol I, *supra* note 74, art. 44(3); Convention Respecting the Laws and Customs of War on Land, Annex of Regulations art. 1(2)–(3), Oct. 18, 1907, 36 Stat. 2277, 1 Bevans 631 [hereinafter Hague Convention IV Annex]. As used herein, "Hague Conventions" collectively refers to Hague Convention IV Annex, Hague Convention V, and Hague Convention XIII.

100. Geneva Protocol I, *supra* note 74, arts. 37(1), 39; Hague Convention IV Annex, *supra* note 99, art. 23(f).

101. For additional discussion of perfidy in cyberspace, see Streltsov, *supra* note 4, at 11–12.

102. *See* Draft Rules of Aerial Warfare arts. 3, 13, 15–16, *in* 17 AM. J. INT'L L. SUPP. 245, 246–48 (1923) (limiting the exercise of belligerent rights and the conduct of hostilities to military aircraft and personnel exhibiting distinctive emblems).

103. Geneva Protocol I, *supra* note 74, art. 58.

104. *Id.* art. 58(a)–(b).

105. Geneva Convention IV, *supra* note 74, art. 28; Geneva Protocol I, *supra* note 74, art. 51(7).

separate military and civilian objects become almost meaningless in the context of modern ICT networks. Today, the military often relies on the same communications nodes, navigation satellites, public utility grids, hardware and software, and technical personnel as the civilian populace.[106] Unless IHL is interpreted to require that government and military organizations build and utilize their own distinct information infrastructure—which is simply not feasible on either technical or economic grounds at this juncture—the collocation of key military targets with invaluable civilian assets is inevitable. In the end, military commanders will be left to judge what level of collateral damage is permissible under the principles of necessity and proportionality.

Another strategic consideration for cyber conflict under IHL is the extent to which the principle of humanity might actually require nation-states to use nonlethal information weapons in lieu of kinetic weapons if they would achieve the same military objective while producing fewer casualties (civilian or combatant) or shorter disruptions to the affected targets.[107] Perhaps temporarily disabling a radar system at an airport or rendering a power plant inoperable is more "humane" than permanently destroying those targets with ordnance, especially when civilian lives are dependent on them. The several examples offered in this section are certainly not the only difficulties for IHL in cyberspace, but they are illustrative of new technological concerns not previously envisioned by either the Hague Conventions or the Geneva Conventions.

C. Preventing Escalation

The strategic realities of geopolitics dictate that no command decisions regarding future cyber conflicts will be made in complete isolation and that governments will not be interpreting or applying the provisions of public international law in an abstract manner. Rather, their determinations will be driven by actual events and made out of necessity. Taken in that context, the unresolved *jus ad bellum* and *jus in bello* issues concerning cyberspace raise several major concerns. Most importantly, it will be the victim state—not the original "aggressor"—who will ultimately decide if specific actions constitute an "armed attack" or "use of force." In other words, the victim state's legal interpretations will govern for practical purposes as opposed to those of

106. *See, e.g.*, WHITE HOUSE, *supra* note 3, at 17 ("The private sector, however, designs, builds, owns, and operates most of the network infrastructures that support government and private users alike."); ROBERT H. ANDERSON & RICHARD O. HUNDLEY, RAND CORP., THE IMPLICATIONS OF COTS VULNERABILITIES FOR THE DOD AND CRITICAL U.S. INFRASTRUCTURES: WHAT CAN/SHOULD THE DOD DO? 1 (1998), http://www.rand.org/pubs/papers/2009/P8031.pdf ("Critical systems on which the security and safety of the United States depend are increasingly based on commercial off-the-shelf (COTS) software systems.").

107. *See, e.g.*, DAVID A. KOPLOW, DEATH BY MODERATION: THE U.S. MILITARY'S QUEST FOR USEABLE WEAPONS 232 (2010) (discussing how cyber weapons "may offer the most humane, barrier-free mechanisms imaginable for warfare").

any foreign legal advisors who authorized such actions under their respective legal systems and military regulations. Moreover, information weapons have occasionally been compared to other weapons of mass destruction that threaten catastrophic consequences, suggesting the legal right to respond to cyber attacks—or imminent threats thereof—in any manner one sees fit.[108] Such a situation poses real concerns of escalation, where one state could view its own actions as permissible sanctions or reprisals but others would consider them impermissible acts of war.

Further compounding such tensions is the fact that current ICTs offer few solutions for mitigating such problems. Without positive attribution, there is no ability to monitor, verify, or signal in the traditional Cold War sense.[109] This in turn raises the question of whether or not cyber deterrence is even possible at this juncture.[110] One final strategic consideration is the degree to which third parties, including nonstate actors, might be able to precipitate or escalate otherwise manageable conflicts between states. Once again, the improbability of real-time attribution poses a very significant obstacle to international peace and security in cyberspace, and that technical difficulty would only be exacerbated in cases where sovereigns employed nonstate actors—such as criminal or political groups—as proxies to commit cyber attacks on their behalf in order to avoid state responsibility.[111]

Unfortunately, the same technological limitations, fears, and uncertainties that make tactical escalation a possibility would also complicate any strategic disarmament efforts. Clearly defined rules of state responsibility and demonstrable (or at least verifiable) national command-authority structures are two prerequisites for successful arms-control regimes. In the absence of either, international legal instruments proscribing the development, proliferation, or use of information weapons will be destined for failure.

---

108. *See* NATIONAL RESEARCH COUNCIL, *supra* note 2, at 296 ("U.S. declaratory policy regarding nuclear weapons suggests that the United States could respond to certain kinds of cyberattacks against it with nuclear weapons."); David Talbot, *Russia's Cyber Security Plans*, TECH. REV. EDITORS' BLOG, April 16, 2010, http://www.technologyreview.com/blog/editors/25050/ (quoting Russian Security Council member Vladislav Sherstuyuk's statement that "there is much in common between nuclear and cyberweapons, because [cyberweapons] can affect a huge amount of people").

109. *See* JAMES DENARDO, THE AMATEUR STRATEGIST: INTUITIVE DETERRENCE THEORIES AND THE POLITICS OF THE NUCLEAR ARMS RACE 48 (1995) (describing Cold War Era nuclear deterrence in terms of each nation reading the signals of other nations and striving to decrease uncertainty); THOMAS C. SCHELLING, THE STRATEGY OF CONFLICT 79–80 (1979) (recognizing the value of signals between parties in shaping a socially optimal outcome).

110. For a detailed discussion of the possibilities for deterrence in cyberspace, see Richard L. Kugler, *Deterrence of Cyber Attacks*, *in* CYBERPOWER AND NATIONAL SECURITY 309 (Franklin D. Kramer et al. eds., 2009).

111. *See* UK CYBERSECURITY STRATEGY, *supra* note 73, at 13 ("The use of proxies provides state actors with an extra level of deniability.").

V. Conclusion

Today, the international community lacks consensus regarding the generally accepted principles of law applicable to cyber conflicts.[112] While all may agree that certain principles of IHL need to be respected, sovereign nations remain in vocal disagreement regarding the sufficiency of those provisions to regulate sovereign conduct in cyberspace. However, two things are certain. First, experience indicates that cyber threats will be propagated from those jurisdictions that criminals, terrorists, or other malicious actors find most favorable, i.e., those with the least stringent domestic regulations and the greatest inability to monitor or curtail malevolent Internet traffic. In legal terminology, that means the adversary will always have the "choice of venue," which directly implies the second truism. Namely, the ultimate solution to the systemic insecurity that is engendered by a globally connected infrastructure will not be found in the reinterpretation or reform of any particular state's legal authorities and enforcement capabilities. Similarly, unilateral declarations or actions are unlikely to resolve the common problems faced by all sovereigns. Cybersecurity has become a worldwide concern which requires the establishment of collective norms and cannot be adequately addressed by any nation in isolation.

Those sovereigns wishing to adequately protect their critical information infrastructures will also need to reconsider many of their competing domestic policy objectives. Only by marshaling all of their societal resources will they be able to truly safeguard the economic and political backbone of a modern nation. At least one historical analogy is haunting:

> In most accounts, France in the late 1930s lacked a coherent national strategy to deal with the German threat. Such a strategy would have linked diplomatic schemes to military strategy, and industrial policy to military doctrine; in principle, it would have orchestrated every national strategic asset from labor power to health policy.[113]

Only through comprehensive national initiatives and the conclusion of a genuine international legal consensus will the devastating impacts of cyber conflicts that so many sovereigns now fear be averted, or at least mitigated.

---

112. *See* ESTONIAN CYBERSECURITY STRATEGY, *supra* note 34, at 17 ("So far, no binding international law on cyber security exists which expresses the common will of countries and which can serve as the basis for shaping national laws.").

113. EUGENIA C. KIESLING, ARMING AGAINST HITLER: FRANCE AND THE LIMITS OF MILITARY PLANNING 6 (1996).