CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

JUNE 2021

A BRIEF PRIMER ON INTERNATIONAL LAW AND CYBERSPACE

DUNCAN B. HOLLIS

International law structures relations among states and other international stakeholders (most notably international organizations) through various prohibitions, requirements, and permissions. As such, it has provided a path for regulating global governance issues from arms control to trade to the environment. As states give increased attention to the governance *of* cyberspace (the technical architecture that allows the global internet to function) and governance *in* cyberspace (how states, industry, and users may use this technology), the role of international law in the cyber context has gained increasing prominence.

This brief primer surveys the application of international law to cyberspace, the players involved, the main issues in its application, and potential future pathways international law may take in governing cyberspace.

INTERNATIONAL LAW APPLIES TO (AND IN) CYBERSPACE

With few exceptions (most notably, the Budapest Convention on Cybercrime and the not-yet-in-force African Union Convention on Cyber Security and Personal Data Protection), international law does not have tailor-made rules for regulating cyberspace. Moreover, the technology is both novel and dynamic. Thus, for several years, there were open questions about whether existing international law applied to cyberspace at all. Today, most states and several international organizations, including the UN General Assembly's First Committee on Disarmament and International Security, the G20, the European Union, ASEAN, and the OAS have affirmed that existing international law applies to the use of information and communication technologies (ICTs) by states. As such, the current discourse centers not on whether international law applies, but rather how it does so.

THE PLAYERS

Unlike many other international issues, the governance of cyberspace did not originate with states, but with the academic institutions and private actors who constructed the internet (albeit with government funding). With the internet's commercialization, ICT companies emerged; today, their platforms serve as the environment for the vast majority of cyber behavior, including state and state-sponsored cyber operations. States' interest in cyberspace, particularly as a zone for geopolitical rivalries, followed. Thus, cyberspace governance involves key stakeholders that include, but are by no means limited to, states.

International law, however, is primarily a legal order for states (and their creations, like international organizations). As such, international law does not hold a monopoly on the regulation of cyberspace . Given industry and civil society players, other regulatory regimes (for example, industry self-regulation) offer alternative vehicles. Multistakeholder governance, for example, has become the main avenue for governance of the internet's architecture. At the same time, nonstate actors have expressed an interest in questions of how international law applies to governance *in* cyberspace. For example, the International Committee of the Red Cross and the Independent Groups of Experts who authored the two Tallinn manuals (with plans for a third in the works) have explored how existing international law rules and principles translate into the cyber context. Microsoft's President Brad Smith even called on states to conclude a new "Digital Geneva Convention" to regulate state behavior in cyberspace.

THE MAIN ISSUES

Issues surrounding international law's application to cyberspace may be broken into five discrete categories: (i) silence; (ii) existential disagreements; (iii) interpretative challenges; (iv) attribution; and (v) accountability.

Silence: Without tailored-made treaties on cyber issues, the application of international law depends on identifying customary international law rules—that is, state practice accepted as law. For many years, figuring what states were doing in cyberspace—let alone what they thought international law had to say about it—was complicated by state silence.

Over the last decade, however, several states have begun to speak out. Beginning in 2012, the United States started to offer its views in a series of speeches and statements. In 2018, the United Kingdom's Attorney General made an important statement of UK views. In the ensuing years, other (mostly European) states began to offer their own detailed perspectives, including Australia, Estonia, Finland, France, Germany, and the Netherlands. Ongoing efforts at the UN and in regional contexts like the OAS are now seeking to expand the list of states with opinions on international law in cyberspace. As yet, however, the vast majority of states remain silent.

Why these states remain silent is often unclear. Some may wish to avoid becoming entangled in international disputes among those states who have spoken out. For others, however,

the issue may be a matter of legal capacity. Many states lack the personnel or resources to understand the issues involved in applying international law to cyberspace. Thus, a threshold issue for international law's application is building up sufficient legal capacity for all states to have a voice in shaping what international law says on cyber issues.

Existential Disagreements: Among those states that have taken positions on international law's application to cyberspace, there are a number of "existential" disagreements—competing claims that a particular international legal rule or regime is entirely included or excluded from cyberspace. In the UN context, for example, a few states have challenged the availability of international humanitarian law, the right of self-defense, the duty of due diligence, and the right to take countermeasures with respect to online activity. The existence (or absence) of one or more of these legal frameworks from cyberspace has significant implications for international law's application, impacting how states conduct their cyber operations in armed conflicts, their ability to respond to malicious cyber activity conducted by other states, and what actions they must take to protect the rights of third states from harms originating in their own territories.

Interpretative Questions: Even where states accept that a particular international legal rule or regime applies in cyberspace, substantial interpretative questions often remain open to debate. International legal regimes like nonintervention, sovereignty, and human rights encounter much ambiguity in their applications to cyberspace. The duty of nonintervention, for example, protects a states' international and external affairs from "coercive" intervention by other states. Yet, there's no consensus on which "affairs" the duty protects, let alone what differentiates coercive from noncoercive cyber activity. Similarly, sovereignty is undoubtedly one of the core architectural features of the international legal order. States appear to diverge, however, on whether sovereignty merely is a foundational principle on which other international legal rules (like non-intervention) rest, or if it is an independent rule that can be breached by certain foreign state cyber operations directly.

Attribution: International law only regulates its subjects of international law (for example, states). It does not usually direct the behavior of ICT companies or individuals (who are usually subject to one or more domestic legal orders). To apply international law in cyberspace, therefore, it is necessary to know the identity of whoever is responsible for the activity in question: is it a state or state-sponsored actor subject to international law or is it an individual(s) engaged in behavior outside international law's ambit? Such identifications are, however, difficult in cyberspace given well-known challenges in technical attribution—identifying the origins of malicious cyber behavior is often difficult and time-consuming. Moreover, where states employ proxies, attribution is further complicated by the need to show evidence of state "control" over the proxy actor (international law has yet to fully resolve how much control is required or what evidence must be shown to demonstrate it).

Accountability: Although attributions of state and state-sponsored cyber operations may be on the rise, accountability has proved challenging. States that accuse other states of malicious cyber behavior rarely invoke international law in doing so. The absence of international legal rhetoric may imply that the behavior may be lawful, even if unwanted. Nor has the

naming and shaming that has occurred done much to change the accused's behavior (it may, however, help clarify the existence and meaning of international law in cyberspace). Some states have been working to create coalitions that can cooperate on improving accountability through collective accusations or even sanctions. So far, however, such efforts have not focused on using international law's benchmarks for measuring malicious cyber behavior nor its tools (for example, countermeasures) for addressing its violation.

FUTURE POSSIBILITIES (AND PROBLEMS)

Going forward, there are two dominant questions about the application of international law to cyberspace: (a) what form should any resolution of the main issues take; and (b) in what fora should this occur?

The future form(s) of international law? Even as international law lacks tailor-made rules, various states and stakeholders suggest that existing international law is sufficient to regulate behavior of states: For these actors, the future must address how to operationalize and improve accountability under the current law.

In contrast, other states and stakeholders have suggested that there are gaps or inefficiencies in the existing law that require the formulation of new rules. This could occur via a new treaty or the evolution of customary international law. The proponents of new rules are not, however, aligned on the desired end-state. Some states are focused on a treaty that would protect states from people (for example, those who would engage in subversive speech or otherwise threaten the security of the state through online activity). Others seek a treaty that would protect people from states (for example, prohibiting states from engaging in malicious cyber operations against critical cyber infrastructure and requiring positive efforts from states to cooperate and forestall such operations by others).

The future forum for applying international law? To date, the most robust fora for addressing international law's application are non-state-oriented. Governance of the internet involves a multistakeholder process. And nonstate actors like the Independent Groups of Experts who crafted the Tallinn manuals have dominated the discourse on how international law regulates state cyber operations. Such efforts may continue to hold sway, as witnessed by the three recent Oxford statements produced by international lawyers on the law's prohibitions and protections vis-à-vis the healthcare sector and vaccine research amid the COVID-19 pandemic as well as foreign election interference prior to the 2020 U.S. presidential election. At the same time, UN member states' efforts to address international law as it applies to cyber/ICT-related issues have multiplied. Moving beyond the original UN Group of Governmental Experts forum, UN processes now also encompass an Open-Ended Working Group in the UN General Assembly's First Committee, as well as a Third Committee process on a UN cyber crime convention. It is not, however, a foregone conclusion that the United Nations will be the only landing place for shaping discussions on how international law applies. Regional organizations (such as the European Union) may offer an alternative that in some cases can avoid certain aspects of geopolitics that dominate the UN discourse. Other existing or future multistakeholder processes might also take up the mantle.

In short, even as states move past their initial reticence to address international law's application in (and to) the behaviors of different actors in cyberspace, the consequences of new voices in various forms and fora warrants heightened attention. States and other stakeholders should carefully track various issues and players involved with an eye on the big picture—seeing if international law can do more than simply apply in cyber contexts. The real question remains—can it do so in ways that are effective at regulating the behavior of states and other actors of international concern?

ABOUT THE AUTHOR

Duncan B. Hollis is a nonresident scholar at the Carnegie Endowment for International Peace and the James E. Beasley professor of law at Temple Law School, where he also serves as the associate dean for academic affairs. He has been active on several of the issues and processes described in this primer, including (i) serving as the rapporteur for the Organization of American States' Juridical Committee on its project to improve transparency around the application of international law to cyberspace; (ii) the Oxford process that has generated two statements on international law's application to cyber threats targeting healthcare-related topics; and (iii) various Microsoft Corporation initiatives as part of its Digital Peace agenda. The views expressed in this primer are, however, written entirely in a personal capacity.