Navigating International Law in Cyberspace

berkeleyjournalofinternationallaw.com/post/navigating-international-law-in-cyberspace

August 23, 2022

About the author: Ahan Gadkari serves as a Research Assistant under Dr. Aniruddha Rajput, Member, UN International Law Commission.

On March 12, 2021, the UN Open-Ended Working Group (OEWG) adopted a final report reaffirming the widely held belief that international law (IL) encompasses cyberspace. Several countries have expressed this belief in proposals requesting that the OEWG address cybersecurity issues. (See here, here, here and here). Therefore, the academic debate surrounding cyberspace can shift towards determining the scope of IL. The Oxford Process and Tallinn Manual 2.0 are two of the most noteworthy initiatives to make headway in this space.

The OEWG report advocated for a set of "voluntary, non-binding norms" based on recommendations from member states. Critically, the report concluded that these norms would operate *in conjunction with* the states' obligations under IL. This conclusion refutes the argument that these new norms would supplant a state's responsibilities under IL. However, the OEWG stated this conclusion more explicitly in the pre-draft report before tempering it in the final report. Nonetheless, the final report challenges two

mutually reinforcing assumptions about the scope of IL's applicability in cyberspace. First, IL concepts can be applied to cyberspace only if *opinio juris* demonstrates their application, that is, states must believe they are obligated to apply IL concepts to cyberspace issues. Second, new cybersecurity norms render existing principles of IL inapplicable to cyberspace because cyberspace is a distinct area of IL.

If we accept these two assumptions, then we effectively place cyberspace issues outside the reach of existing IL. However, an analysis of International Court of Justice (ICJ) opinions, International Law Commission (ILC) draft articles, and nations' OEWG deliberations show that these assumptions are incorrect. Therefore, existing IL is the foundation for future developments in international cyberspace law, such as the new norms promulgated in the OEWG report.

The assumption requiring *Opinio Juris*:

The assumption that *opinio juris* is necessary rests on the premise that distinct spheres demand distinct state practices. Israel's Deputy Attorney General argued in support of this assumption that IL cannot be applied automatically from the physical to the cyber sphere. From a purely physical standpoint, he is correct; certain principles of IL are restricted to specific spheres. For example, the idea of freedom of navigation is restricted to ships operating on the high seas. However, he overlooked the fact that the cybersphere is not merely another physical sphere. This notion that IL will be applied differently in different areas originated in the law of armed conflict, where nations have varying commitments in various spheres.

The primary argument for doubting IL's applicability in cyberspace is the assumption that cyberspace is a new frontier. This is incorrect, as cyberspace activities do not take place in a new sphere. Rather, what we commonly refer to as cyberspace is a collection of information and communication technologies that enable users to more efficiently exchange and process information, such as the internet. Moreover, while software, code, and data are significant components of these technologies, the components themselves require hardware and individuals who create and use software, hardware, and data. Thus, while cyberspace activities span borders, they are nonetheless rooted in physical infrastructure.

In its Advisory Opinion on Nuclear Weapons, the ICJ rejected the contention that principles of IL and international humanitarian law do not apply to nuclear weapons because they are a new form of weaponry. Additionally, the ICJ noted that the principles of IL apply to all weapons, regardless of when they came into existence. Additionally, the ILC stated that every new technology is subject to existing principles of IL aimed at preventing transboundary harm. Further, the OEWG report underlined that the issue is technology misuse, not technology use, and that actions to avoid technology misuse should remain "technology-neutral." The term technology-neutral means that existing principles must apply to new forms of technology, without simply refuting their application based on the "new form of technology" argument. This is not to say that no adjustments are necessary when extending IL principles to cyberspace; they may be required in some cases. What this does mean is that the starting point for IL in cyberspace is not limbo but rather established principles of IL. This becomes increasingly critical, as the Czech Republic recognized, because cyberspace use accelerates at a rate that treaty development cannot keep up with.

The assumption that the new norms will replace the existing principles of IL:

The 2015 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE), which the United Nations General Assembly subsequently adopted, urged the establishment of new norms of responsible state behavior in cyberspace. As indicated at the outset of this piece, the GGE intended for these new standards to be voluntary and non-binding. Thus, what is the relationship between these new standards and established IL principles? One of these new standards requires states to prevent their territory from being used for cyber operations that violate IL. However, this requirement already exists as a general principle of IL: due diligence. Is this to say that a fundamental principle of IL has been reduced to non-binding advice under the new norms? The proponents of this assumption may desire to suggest that states have opted to dilute some IL principles in cyberspace. However, during the OEWG deliberations, states made clear that the new norms do not replace or alter their existing obligations, but rather complement them (See here, here, here and here). Additionally, the OEWG report noted that the new standards do not supplant existing legal concepts, but rather complement them. In the case of established norms of IL, states have maintained that the long precedent of states enforcing these norms further validates their application to cyberspace. (See here, here and here).

Conclusion:

Existing principles of IL continue to govern the sphere of cyberspace. Accepted principles remain in force until states decide to change them. Thus, while new cyberspace-related norms and treaties are undoubtedly necessary, this need does not render existing obligations inapplicable. The OEWG's final report and states' recommendations imply that the new norms complement current IL principles, whether they admit it or not.