THE OXFORD PROCESS

Feb. 14, 2022

International Law and the Russia-Ukraine Cybercrisis

The Oxford Process on International Law Protections in Cyberspace

Cyberspace has become a critical battleground in the ongoing crisis in Ukraine. An effective global response to the crisis will demand collective ingenuity, cooperation, and coordination of many tools, including international law. Indeed, much of the normative framework to assess the legality of on- and offline conduct targeting Ukraine already exists. In the last few years, while the UN has been gathering views of states, international lawyers have identified areas of clear agreement on what the law already requires. Amid fast-changing facts, there is broad consensus on the rules of international law applicable to state behaviour in cyberspace. Simply put, some things are always protected — healthcare, elections, infrastructure critical to daily life — and some ways of misusing cyberspace — ransomware, for example — are essentially forbidden. The UN Charter clearly prohibits illegal uses of force and threats to do so, whether conducted through kinetic means or information and communications technologies. Existing international law also proscribes coercive intervention — including through cyber-means — in the domestic affairs of states and arbitrary interference with human rights.

Over the last two years, more than one hundred international lawyers from around the world have engaged in the "Oxford Process on International Law Protections in Cyberspace", which, as elaborated here, has clarified the legal rules governing three areas:
(1) prohibited cyber-targets;
(2) prohibited cyber-means and methods; and
(3) affirmative state duties. The current crisis demands urgent work on a fourth issue as well:
(4) lawful responses.

Prohibited cyber-targets:

International law prohibits a state (or those acting under its instructions, direction or control) from using cyber-means to cause harmful consequences on certain targets. For example, states may not launch cyber operations, like ransomware, "which are aimed at or result in disruption to electoral systems, healthcare, electric grids, water distribution systems, and nuclear power plants." The ongoing pandemic

has highlighted that international law also prohibits states from targeting "essential medical services" or another state's "healthcare sector and essential medical facilities" such as "vaccine research, trial, manufacture and distribution facilities". If a state of armed conflict arose, that would trigger further legal obligations under international humanitarian law: for example, states could not lawfully attack by cyber-means medical personnel and facilities, humanitarian personnel and consignments, civilians, civilian objects, or objects indispensable to the survival of the civilian population. Under certain circumstances, individuals who violate these prohibitions through cyber operations could be convicted for war crimes or crimes against humanity.

Prohibited cyber-means and methods: The Oxford Process further concluded that existing international law prohibits and restricts the means and methods by which cyber operations occur, declaring some cyber operations illegal per se while others must be limited in scope or character. For example, ransomware operations may constitute a violation of the principles of sovereignty or non-intervention in a state's internal or external affairs, amount to a prohibited threat or use of force, or violate human rights law. International law also prohibits a state, or actors whose conduct may be attributed to a state, from conducting information operations or activities that spread false or manipulated claims to incite discrimination, hostility and violence on racial, national or religious grounds, or advance propaganda for war.

Affirmative state responsibilities: States facing cyber-misconduct are not free to do nothing. The Oxford Statements have clarified that existing international obligations require states to act with "due diligence" to prevent, halt and redress a range of harms caused by cyber activity. In particular, "[s]tates must not allow their territory or infrastructure under their jurisdiction or control to be used by states or non-state actors for ransomware operations that are contrary to the rights of other states, when the former states know or should know of" them. States from which cyber operations emanate must thus take available and feasible measures, such as conducting investigations and cooperating with affected states to prevent, stop and mitigate "adverse consequences" caused, for example, to electoral processes and healthcare facilities abroad. These affirmative duties apply insofar as the state from which the cyber operations emanate should have known of such operations regardless of whether the operations are carried out by a state's organs or its proxies.

Lawful responses: A state that has committed an internationally wrongful act is under an obligation to cease such acts where they are continuing and to make full reparation. But if it refuses to do so, law-abiding states may induce

compliance with such obligations by resorting to retorsion (unfriendly but lawful acts) or, under certain conditions, countermeasures (unlawful acts that the law allows when done in response to prior illegal behaviour). As the Ukraine crisis unfolds, states and other stakeholders must give close and immediate attention to the range of lawful responses available to combat unlawful cyber operations and illegal state failures to exercise due diligence. Exactly how countermeasures apply in cyberspace remains open to discussion, and the Oxford Process intends to convene urgent dialogue about these issues in the near future.

In sum, the Ukraine crisis is not happening in a legal vacuum. As the facts on the ground evolve, state representatives and other relevant actors must assess those facts in light of the applicable rules of international law. Framing the dispute in the language of international law can depoliticize debate and open space for meaningful interstate dialogue and engagement. International lawyers – inside and outside governments – must discuss such urgent questions as: whether prohibited cyber targets encompass data associated with the provision of essential civilian services; whether prohibited cyber-means include placing of malware that threatens, but has not yet resulted in, harmful consequences; how far and to which states existing due diligence obligations extend; and whether and when countermeasures may be taken collectively by states in response to unlawful cyber operations on a single state.

By analysing the applicable legal framework, the Oxford Process sheds light on the emerging crisis' many faces. The Oxford Process involves multinational statements of what the law already is, made by leading scholars. It has clarified rules underutilized so far in discussions about potential international illegality in cyberspace.

In the weeks ahead, states, through their public statements and actions, should ground their discussions in international law and explain how they understand it applies to their conduct and others'. Every state and person involved in the Ukraine crisis should be held to these standards. Crises, like this one, offer states and other stakeholders a historic opportunity to elaborate and clarify the law governing cyberspace – and to hold each individual, institution, and government accountable for complying fully or violating it.