Operations in Cyberspace from the Perspective of International Law

Yaël Ronen

International law is applicable to cyberspace. There is international consensus that the UN Charter, which prohibits the use of force, applies to cyberspace. There is, nonetheless, some disagreement on what would constitute an armed attack in cyberspace, and consequently, what response would be permitted. Actions that do not amount to attack may still be prohibited by international law, for example if they constitute interference in the domestic affairs of states.

Keywords: Armed attack, international law, cyberspace, self defense

The debate on the regulation of cyberspace emphasizes the defense of this sphere. Discourse in international law regarding cyber activities differs from this debate in a number of respects: First, international law deals primarily with inter-state relationships rather than with domestic ones. Second, regulation is an act of organization, surveillance, and enforcement, which is intended to enforce binding rules of behavior. The basic assumption of regulation is that rules of behavior do exist; in contrast, international law is still at the stage of clarifying what rules exist or would be desirable with regard to cyberspace; or in other words, which acts are permissible and which are forbidden in this sphere. Third, whereas domestic regulation

Yaël Ronen is a professor of international law at the Academic Center for Science and Law in Hod Hasharon; and a research fellow at the Minerva Center for Human Rights at the Hebrew University in Jerusalem.
This article is based on a presentation given on October 24, 2018 at the Institute for National Security Studies, in collaboration with the Academic Center for Science and Law, marking the launch of the publication of *Cyber Regulation* by Colonel (res.) Dr. Gabi Siboni and Ido Sivan-Sevilla.

ordinarily focuses on **defending** cyberspace, international law focuses with the implications of the use of cyberspace for **attacks**.

Cyberspace activity poses a challenge for international law. First, international law in almost all its branches, regulates relationships involving tangible objects, whereas cyberspace is intangible. As a result, the question arises whether existing norms of international law are applicable to cyberspace, or rather it is necessary to draft new norms. Second, international law is based specifically on territorial divisions: The global arena is split into territorial units, namely states, and great emphasis is placed on the division of powers and privileges as embodied in the concept of sovereignty. In contrast, cyber activity inherently crosses borders. Third, international law is traditionally based on the primacy of states as actors: Those have rights, and they bear responsibilities. It seems that with respect to cyber activities, states are not the central actors.

These differences raise a basic question: Does international law apply to cyberspace? This question has been addressed primarily within academia. The First Tallinn Manual, a document drafted by a team of scholars and published in 2013, focused on the question of how international law can be applied to cyberspace, first and foremost in relation to the prohibition on the use of force and to the right of self-defense, as well as to actions that occur within the context of an armed conflict. The Second Tallinn Manual of 2017 expanded the debate to the applicability of international law to activities that do not involve the use force or do not amount to armed conflict. The formal involvement of states in this debates remains limited, in part because technology allows penetration into sensitive areas on which governments are reluctant to speak out; nonetheless, a consensus exists today that international law also applies in cyberspace. One of the notable developments in this context is the consensus reached in 2015 by an inter-governmental group of experts, which reached agreement that the UN Charter applies in its entirety also to cyberspace. This group included, among others, experts from the United States, Britain, Russia, and China, states which constitute the major players in the international arena. The consensus reached has several implications, some of which will be discussed below.

The UN Charter enshrines the prohibition on the use of force and on threats to use force against the independence or the territorial integrity of states and declares that use of force would only be legal when carried out in

self-defense or by authorization by the Security Council, and in exceptional circumstances. The question, of course, is what is considered "use of force" in the context of cyber activity. In this regard, cyber activity refers to actions against computer systems intended to gather, infiltrate, alter, or disrupt information through various means, or to manipulate network operations. It is widely agreed that a cyber activity may be considered "use of force" or an "armed attack" if its expected consequences are comparable to those of a kinetic attack or, in other words, can cause death or injury to people and damage to property. For example, cyber activity that results in a train derailment or the breach of a water main in a populated area would be considered an armed attack, just as if the train tracks had been subject to an aerial bombardment.

An example of this type of attack was the Stuxnet incident. In 2010 a malicious computer worm ("Stuxnet") infiltrated the systems that formed the basis for the centrifuges at one of the nuclear facilities in Iran, and caused the centrifuges to spin out of control and self-destruct. This was one of the first times that a cyber operation led to the physical destruction of an object. The action demonstrated the potential destruction and harm that cyber activities can cause, just like attacks through conventional means.

Classifying an act as an "armed attack" is significant because under certain circumstances, an armed attack entitles the victim state to use force in self-defense. If cyber activities may be considered armed attacks, then a forcible response is also conceivable. From this perspective, the Stuxnet worm attack on Iran might have given rise to a right of self-defense. An important question would then have arisen: Against whom is the injured party entitled to defend itself? Stakeholders in Iran and other states have accused the United States and Israel of being behind the Stuxnet attack, although there has been no real evidence indicating the involvement of any specific state in developing and spreading the worm. Another question is which measures would meet the standards of necessity and proportionality required in order for the response to be considered legitimate within the framework of the right of self-defense.

The most complex problem, over which there is still considerable disagreement, relates to situations in which cyber activities cause severe and substantial non-tangible damage. The conventional interpretation is that acts of collecting, stealing, or even destroying or altering information are not

considered armed attacks in and of themselves. Accordingly, armed response is not permissible. Nonetheless, the negative effects of such acts might be quite substantial. An example would be a cyberattack on economic or financial institutions, such as the New York Stock Exchange, which might cause the stock exchange to crash when the trustworthiness of its data and computer infrastructure is compromised. The question that arises in this context is whether the damage is purely economic, or whether the catastrophic results of the cyberattack justify categorizing it as an "armed attack."

This kind of cyber act was actually the trigger for interest in the applicability of international law to cyberspace: In April 2007 the government of Estonia declared its intention to move a World War II memorial from the center of its capital Tallinn to a military cemetery in the suburbs. Estonian citizens of Russian ethnicity reacted to this plan by violent protest. Subsequently, for about a month, internet infrastructure in Estonia was subject to attacks. The internet is a tool of preeminent usefulness in Estonia; 95 percent of banking transactions are digitized, and 98 percent of Estonian territory is connected to the internet, to the point that it is said that in Estonia the internet is almost as important as running water. The attacks on Estonia's internet infrastructure targeted the websites of the president, prime minister, parliament, political parties, banks, public media, and more. As a result, two major domestic banks were shut down for several days, and some of the central news agencies were damaged; emergency lines were disconnected for an hour; private and public communications were harmed; and most of all, faith in the national economy faltered. The attacks have been commonly linked to Russia, and some of them indeed were produced by computers controlled by Russian government institutions. However, the sources of the attacks were traced to 177 other countries, and most attacks originated from privately owned computers.

Estonian politicians compared the attacks to an invasion and to use of conventional military operations, but the actual damage incurred was limited and primarily economic: No harm was caused to property or lives; soldiers were not sent to the frontline; and there was no use of conventional weaponry. The basic economic infrastructure of the state, however, was damaged, crippling its ability to function.

The assertion that a state that falls victim to a substantial cyberattack may not respond through military means is very problematic. Disregarding

technological developments is likely to lead to absurd results and it is unlikely that states will abide by a rule that is inconsistent with realistic needs. Therefore, academics today widely agree that it is justifiable to categorize cyber activities that may cause severe consequences as "armed attacks." The question is what criteria are used to evaluate severity. Several elements may be taken into consideration, such as the repercussions to vital national interests, the immediacy of the outcome and the degree of its directness, the level of intrusion, and the level of state involvement.

Another principle anchored in the UN Charter is the prohibition on interfering in domestic issues of other states. This prohibition does not refer to specific methods and therefore also applies to interference by cyber means. The prohibition on interfering in domestic affairs is usually not prominent in international discussions, because when a conventional attack is waged on a state, the element of "interference" becomes a relatively minor issue. It is precisely when there is no recourse to violence, but rather to social or economic manipulations, that the prohibition on interference becomes a central issue.

As a rule, an act is considered to be "interference" when there is coercion or pressure, overt or otherwise. For example, espionage and data collection from computers in foreign countries are not considered interference, because even though there is an element of infiltration into a foreign computer network, these acts do not constitute coercion or the exertion of pressure on that country. The situation is different in the case of manipulating election results or public opinion via computers on the eve of elections. In some areas, the disagreement over classification is even greater: For example, what is the law regarding damage inflicted upon a political campaign of a specific party via content sites or the creation of fictional activities intended to sway public opinion? Arguably such actions constitute interference in the core of the state's sovereignty, albeit through political and social action rather than military; regardless, the effect may be quite severe. There is no doubt that these types of acts are illegal; what is an open question is how the injured state is allowed to respond.

Activity in cyberspace creates additional challenges for international law, such as the limitations on the use of cyber due to humanitarian legal principles and the risks that the use of cyberspace poses for the protection of human rights. International law has only just begun to engage with

these issues. The need to cultivate and hammer out norms in response to technological developments is not unique to international law; moreover, there is no doubt that basic legal principles of international law are present and exist also within cyberspace.