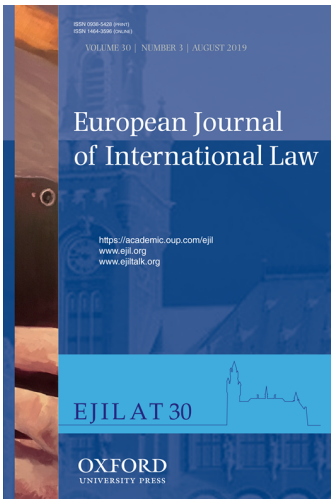
Israel's perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations

ejiltalk.org/israels-perspective-on-key-legal-and-practical-issues-concerning-the-application-of-international-law-to-cyber-operations/

By Roy Schondorf December 9, 2020

> *Transcript of the keynote speech delivered by Israeli Deputy Attorney General (International Law), Dr. Roy Schöndorf, on 8 December, 2020 at the US Naval War College's event on "Disruptive Technologies and International Law".**



I would like to present, here today, Israel's perspective on key aspects of the application of international law in connection with cyber operations, with a particular emphasis on issues related to the use of force and armed conflicts.

The question of how international law adapts to emerging technologies is one of the most challenging faced by legal advisers. These challenges compel us to revisit notions that have been with us for decades, and sometimes centuries. We can see this in the fields of artificial intelligence, blockchain, and, of course, in the context of cyber operations.

Israel considers that international law is applicable to cyberspace, and this is a view that has become almost axiomatic for a vast majority of States. However, when seeking to apply particular legal rules to this domain, we are mindful of its unique features.

These unique features shape policy and affect the legal framework applicable to the cyber domain. I wish to shortly address some of them. First, cyber operations are conducted through a global network, passing through infrastructure located in multiple jurisdictions, and lack, in and of themselves, any meaningful physical manifestation. Second, much of the cyber infrastructure is held and controlled by the private sector and civilian components are a major part of the picture. Thus, regulation of the cyber domain may have various social and economic implications as well. Third, the cyber domain is highly dynamic, given the fast pace of technological developments and innovation. The development of international legal rules, on the other hand, is a more gradual process. This is understandable since these rules are designed to stand the test of time and are not easily amended.

All these factors taken together suggest that an extra layer of caution must be exercised in determining how exactly international legal rules apply to cyber operations, and in evaluating whether and how additional rules should be developed. We, as government and military legal

advisers, are tasked with the role of identifying the relevant rules, including those set by the law of armed conflict, and determining how they apply to a particular set of facts. In some cases, it will be possible to apply a certain rule as it is; while in other cases, the situation may be conceptually different, such that it might not be possible, feasible, or even desirable to draw from existing legal rules. This process obviously has to consider the behaviour of States in the cyber domain, as international law is State-made.

When dealing with a treaty provision, we look to the regular rules of treaty interpretation to ascertain the relevance and applicability of the provisions at hand in the cyber context. As for customary law, it is necessary to examine whether there is general State practice accepted as law, substantiating the existence of a rule in the cyber domain. It cannot be automatically presumed that a customary rule applicable in any of the physical domains is also applicable to the cyber domain. The key question in identifying State practice is whether the practice which arose in other domains is closely related to the activity envisaged in the cyber domain. Additionally, it must be ascertained that the *opinio juris* which gave rise to the customary rules applicable in other domains was not domain-specific. Given the unique characteristics of the cyber domain, such an analysis is to be made with particular prudence, as it is very often the case that relevant differences exist.

Since this is the Naval War College's conference, it is only fitting that I will give an example from the law of maritime warfare. As you all know, the rules regulating maritime blockade evolved long ago. Over the years these rules have crystalized into customary law. Nonetheless, this custom was formed specifically in the maritime context. Putting aside the question of whether the concept of blockade is relevant to cyberspace, the maritime practice is not closely related to any type of activity in the cyber domain, while the *opinio juris* in this regard is domain-specific. It is therefore quite clear that the rules of maritime blockade are not applicable in the circumstances of activities in the cyber domain.

The law of neutrality also illustrates the challenges of applying rules that evolved in the context of traditional warfare to the contemporary environment of cyberspace, as many of its rules were tailored specifically to the land, sea and air domains. For example, in relation to one of the basic overarching rules of neutrality – the inviolability of a neutral State's territory – while in the land domain it is forbidden to transfer troops or convoys of munition; at sea – the passage of warships in territorial waters is possible; and in the air such passage is subject to discretion or limitations of each neutral State. Given these differences, it remains unclear if and how this rule would be applicable in cyberspace.

These are just examples that show why it is not always easy to move from the general statement that international law applies to the cyber domain, to concrete legal rules that bind States and non-State actors in their actual behavior.

Accordingly, the State of Israel has largely refrained thus far from making specific statements on whether and how particular rules apply. That is not to say that we take no position – indeed, we have consistently affirmed the application of international law to cyberspace in

forums like the UN GGE and the Open Ended Working Group. In parallel, over the last few years, we have been gradually formulating and developing our views on some contemporary issues relating to cyber operations. This is a meticulous and delicate process, impelled by the need for thorough legal and practical research and careful consideration of a multitude of views, together with an assessment of potential implications.

Bearing in mind all these challenges, in my presentation today I would like to share with you some of the insights that we have reached thus far regarding international law applicable to cyber operations, particularly in connection with armed conflicts. My hope is that this will contribute to the current legal discourse in this field.

Jus ad bellum

I will start by addressing a few key issues concerning the *jus ad bellum*. First – and this has already been acknowledged by many others – the customary prohibition set out in Article 2(4) of the Charter of the United Nations, on "the threat or use of force" in international relations, is clearly applicable in the cyber domain.

We share the support among States for the view that a cyber operation can amount to use of force if it is expected to cause physical damage, injury or death, which would establish the use of force if caused by kinetic means. For example, hacking into the computers of the railroad network of another State and programming the controls in a manner that is expected to cause a collision between trains can amount to use of force. As with any legal assessment relating to the cyber domain, as practice in this field continues to evolve, there may be room to further examine whether operations not causing physical damage could also amount to use of force.

Second, when the use of force in the cyber domain, by either a State or non-State actor, can be considered as an actual or imminent armed attack, the State under attack may act in accordance with its inherent right to self-defense, as enshrined in Article 51 of the UN Charter. Of course, the exercise of this right is subject to the customary principles of necessity and proportionality.

Finally, the use of force in accordance with the right of self-defense, against an armed attack conducted through cyber means, may be carried out by either cyber or kinetic means; just as use of force in self-defense against a kinetic armed attack may be conducted by kinetic or cyber means.

Jus in bello

I would like to move on and address some key issues concerning the applicability of the Law of Armed Conflict (LOAC) to the cyber domain.

I'll start by stating the obvious: the law of armed conflict and its fundamental principles generally apply to cyber operations conducted in the context of an armed conflict. Indeed, "the right of belligerents to adopt means of injuring the enemy is not unlimited," even in the cyber domain.

Israel is a party to the Four Geneva Conventions and other treaties[1] governing particular aspects of conduct in armed conflict and is also bound by applicable customary law. Israel – like the United States and others – is not a party to the Additional Protocols and is not bound by them as a matter of treaty law. However, we see the following as consistent with the relevant customary law and the Additional Protocols.

One of the key issues, in the conduct of hostilities in particular, is how to define "attacks", and in which circumstances cyber operations amount to attacks under LOAC. The concept of attack is central to targeting operations and only acts amounting to attacks are subject to the "targeting rules" relating to distinction, precautions and proportionality.

The definition of attack in LOAC requires several elements, but I will focus on those aspects carrying special relevance in the cyber context. Specifically, I will address the element requiring that an act will constitute an attack only if it is expected to cause death or injury to persons or physical damage to objects, beyond *de minimis*.

One aspect of this element concerns the reasonably expected consequences of the act in question. Reasonably expected consequences are those that are anticipated with some likelihood of occurrence, and entail adequate causal proximity to the act.

A second aspect in this element is the type of required damage. The requirement for physical damage has been accepted law since the introduction of the legal term of art attack into the LOAC discourse. For this reason, practices such as certain types of electronic warfare, psychological warfare, economic sanctions, seizure of property and detention have never been considered to be attacks as such, and accordingly, were not considered as subject to LOAC targeting rules.

Only when a cyber operation is expected to cause physical damage, will it satisfy this element of an attack under LOAC. In the same vein, the mere loss or impairment of functionality to infrastructure would be insufficient in this regard, and no other specific rule to the contrary has evolved in the cyber domain.

However, if an impediment to functionality is caused by physical damage, or when an act causing the loss of functionality is a link in a chain of the expected physical damage, that act may amount to an attack. For example, if a cyber operation is intended to shut down electricity in a military airfield, and as a result is expected to cause the crash of a military aircraft – that operation may constitute an attack (subject, of course, to the additional elements for attacks under LOAC).

The existence of physical damage is assessed purely on objective and technical grounds. It is a factual question and as such does not depend on the subjective perception or the manner in which the other side chooses to address the loss or impairment of functionality.

Finally, the fact that a cyber operation is not an attack does not mean that no legal limitations apply thereto. Indeed, there are general obligations in LOAC that apply to all military operations regardless of being attacks or not. Central among those is the requirement to consider the danger posed to the civilian population in the conduct of military operations. It is widely accepted today that parties to conflicts cannot blatantly disregard such harmful effects to the civilian population in their military operations. But there are also more specific protections that may apply to actions other than attacks. For example, cyber operations affecting medical units are regulated and limited, *inter alia,* by the LOAC obligation to respect and protect medical units, which applies regardless of whether the act constitutes an attack or not.

Moving on from the issue of attack, another question which is especially relevant to the cyber domain is whether the term “object”, as it is understood in LOAC, encompasses computer data. This bears implications with regard to the implementation of the LOAC rules relating to distinction, precautions and proportionality.

Objects for the purposes of LOAC have always been understood to be tangible things and this understanding is not domain-specific. It is therefore our position that, under the law of armed conflict, as it currently stands, only tangible things can constitute objects.

Here, again, this does not mean that cyber operations adversely affecting computer data are unregulated. In particular, when an operation involving the deletion or alteration of computer data is still reasonably expected to cause physical damage to objects or persons and fulfills the other elements required to constitute an attack, the operation would be subject to LOAC targeting rules. Likewise, one must have regard to rules, which are not dependent on the concept of objects, such as the obligation to respect and protect medical units.

Observations on other legal issues pertinent to cyber operations

Now, in addition to the *jus ad bellum* and LOAC, there are other legal frameworks pertinent to cyber operations that do not center on armed conflicts. Given their importance, I believe it is valuable to address them shortly, and perhaps leave some room for further thought.

I will start by addressing perhaps the broadest topic, which continues to be a subject of vibrant discussion: sovereignty. To begin with, there are diverging views regarding whether sovereignty is merely a principle, from which legal rules are derived, or a binding rule of international law in itself, the violation of which could be considered an internationally wrongful act. This issue has many facets, and while I will not offer any definitive position for the time being, I would like to stress a number of important point.

The first is that sovereignty is a cornerstone of international law and international relations. Of course, we need to distinguish, in this regard, between sovereignty, which is typically used as a general concept that connotes independence, and “territorial sovereignty”, which is an international legal rule. States will sometimes point to the need to protect their sovereignty, referring broadly to their political will and autonomy, without necessarily referring to a legal rule. The two meanings are sometimes conflated, and we need to be very careful when drawing legal conclusions.

A second, and related point, is that States undoubtedly have sovereign interests in protecting cyber infrastructure and data located in their territory. However, States may also have legitimate sovereign interests with respect to data outside their territory. For example, as governments store more and more of their data by using cloud services provided by third parties, whose servers are located abroad, how do we describe the interest that they have in relation to that data? Would the interest in protecting the data not be a sovereign interest in this case as well? Or, alternatively, when a State conducts a criminal investigation and needs to access data located abroad from its own territory, under what circumstances does it need to request the consent of the territorial State? Of course, there are no easy answers to these questions, and some of them are currently being discussed, such as in the context of the protocol to the Budapest Cybercrime Convention currently being negotiated to address this very topic.

These questions reflect an inherent tension between States’ legitimate interest and the concept of territorial sovereignty, as we understand it in the physical world. In practice, States occasionally do conduct cyber activities that transit through, and target, networks and computers located in other States, for example for national defense, cyber-security, or law enforcement purposes. Under existing international law, it is not clear whether these types of actions are violations of the rule of territorial sovereignty, or perhaps that our understanding of territorial sovereignty in cyberspace is substantively different from its meaning in the physical world.

Another matter closely related to the issue of sovereignty is that of non-intervention. Traditionally, this concept has been understood as having a high threshold. It has been taken to mean that State A cannot take actions to “coerce” State B in pursuing a course of action, or refraining from a course of action, in matters pertaining to State B’s core internal affairs, such as its economic or foreign policy choices. Its traditional application has focused on military intervention and support to armed groups seeking the overthrow of the regime in another State. This could presumably also relate to support given to armed groups in the cyber domain, such as providing information regarding cyber vulnerabilities of the State.

A more recent issue that has come to the fore relates to interference in national elections. We concur with the various positions expressed in this regard, such as that which was presented by former U.S. State Department Legal Adviser Brian J. Egan, and more recently

reiterated by U.S. DOD General Counsel Paul C. Ney, Jr. that a “cyber operation by a State that interferes with another country’s ability to hold an election or that manipulates another country’s election results would be a clear violation of the rule of non-intervention.”

I will now turn into addressing three somewhat related topics: due diligence, attribution and countermeasures.

The concept of due diligence means that States should take reasonable measures to avoid or minimize harm to other States, and seems to be useful in fields such as international environmental law. In the 2015 UN GGE Report the concept was addressed as the basis for a voluntary, non-binding norm of responsible State behavior, providing that States should not allow their territory to be used for the commission of international wrongful acts. There was wisdom in mentioning it in the chapter covering norms of responsible State behavior, as it does not, at this point in time, translate into a binding rule of international law in the cyber context. This was the position expressed by other States as well.

As I mentioned regarding the examples of maritime blockade and neutrality, we have to be careful in applying to the cyber domain rules that emerged in a different, distinct context. For instance, in the field of environmental law, where much of the focus and application of due diligence obligations has been in recent years, the acting State typically has control, or at least oversight, over the harmful activity (for example, regulating a polluting power plant). However, cyberspace is mostly private and decentralized.

The inherent different features of cyberspace – its decentralization and private characteristics – incentivize cooperation between States on a voluntary basis, such as with the case of national Computer Emergency Response Teams (CERTs). CERTs are already doing what could arguably fall into that category: exchanging information with one another, as well as cooperating with each other in mitigating incidents. However, we have not seen widespread State practice beyond this type of voluntary cooperation, and certainly not practice grounded in some overarching *opinio juris*, which would be indispensable for a customary rule of due diligence, or something similar to that, to form.

The issue of attribution is also widely debated with respect to cyber operations. Some have suggested that there needs to be more legal certainty with respect to attribution, in order to avoid mistaken attribution, which can lead to conflict escalation. This is increasingly becoming more of a theoretical issue. Over time, the attribution capabilities of States have improved, and even States with lesser capabilities have been able to rely on solid information provided by other States and by the private sector. In any event, this is a technical matter – a factual one – and I would advise against over-regulating the issue.

That being said, there is also the question of public perceptions – because sometimes, when an offensive cyber operation is public and the attribution is public, the government needs to communicate with its citizens, and with the international community at large, in order for its positions and actions to be understood. But there will be cases when a State will prefer not to

disclose the attack, the attribution, or any ensuing actions taken – for diverse reasons such as national security and foreign relations. Either way, as a matter of international law, the choice whether or not to disclose the attribution information remains at the exclusive discretion of the State.

With respect to the issue of countermeasures, I would like to echo the positions taken by the UK, the US and other States, to the effect that there is no absolute duty under international law to notify the responsible State in advance of a cyber-countermeasure. Prior notification is perhaps more realistic and practical in fields such as international trade, allowing the responsible State to reconsider its actions without frustrating the ability of the injured State to take the intended countermeasures. However, in the cyber domain, where the pace of events can be extremely fast and the other side may thwart the action if it anticipates it, announcing a cyber-countermeasure in advance would often negate its utility and effectiveness, and in some instances undermine the interests of the injured State, as well as render the countermeasure obsolete.

Concluding Remarks

One last point: I have focused thus far on cyber operations, but it is important to keep in mind that the application of international law to cyberspace is much broader than the issues I touched upon. Questions relating to cybersecurity, cybercrime, digital trade, and human rights in the cyber domain, are just a few examples. I think that international law has a crucial role to play in addressing these topics. By focusing on these topics, international law can contribute to enhancing global stability in a concrete way. We hope to share our views on these and other topics as well in due course.

I wish to conclude my remarks by taking a step back. In the discussions that we are having on the application of international law in dealing with emerging technologies, I think that the challenges lie not in identifying the basic rules of international law – the prohibition on the use of force, self-defense, non-intervention, territorial sovereignty, etc. – but in determining when and how they apply in new circumstances. Picture the land, air, and sea domains of international law as independent trees, each with its own branches and leaves, each yielding its own fruit. Each of these trees is sustained by common ingredients – soil, water, sunlight – yet each tree grows differently, depending on the external conditions, the type of seeds sown and how the roots grow. We now have a new tree whose roots are just beginning to take shape – international law of cyber operations is a nascent field. It is emerging from the same grounds of international law, the same core principles at the heart of the international system, and its leaves and fruits will bear some similarities to the other fields of law – but we do not expect that it will be identical, once fully grown. So, while the vast majority of States agree on the starting point of the application of international law to cyber operations, the international community is still very much at the beginning of the journey and the applicability of each existing rule of international law to the cyber domain requires careful assessment and review.

Thanks again for inviting me to speak here today. I look forward to your questions.

> **This speech will be published in the upcoming volume (97) of the International Law Studies (ILS) journal (expected January 2021).*

[1] For example, Israel is a party to the 1954 Hague Convention for the Protection of Cultural Property in the Event of Armed Conflict, and the 1980 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 (with Protocols I, II and IV).