## REACTION

## CYBERSPACE AND INTERNATIONAL LAW: THE PENUMBRAL MIST OF UNCERTAINTY

## Michael N. Schmitt\*

It has become *de rigueur* to characterize cyberspace as a new dimension of warfare, one devoid of international law and subject to catastrophic abuse. In fact, malevolent states, cyberterrorists, or malicious hackers will likely exploit cyberspace to strike at global critical infrastructure and other essential cyberassets. The ensuing consequences of such operations could range from the disruption of government functions and economic loss to massive physical destruction and widespread death. The prominent place cyberspace occupied in the Director of National Intelligence's 2013 worldwide threat assessment was therefore neither hype nor hyperbole.

History may help place the concerns regarding cyberoperations in perspective. The appearance of new weaponry has often been accompanied by assertions that such weapons exist beyond the reach of extant principles and rules of international law. In the last century, for instance, such claims arose with respect to, inter alia, machine guns, aircraft, submarines, and nuclear weapons. And in the last few months, controversy has erupted over autonomous weapon systems, following seemingly contradictory arguments from human rights quarters that they are both unlawful per se and should be banned by treaty.

Yet, cyberspace is not a lawless firmament. As with the aforementioned weapons, the established norms of the *jus pacis*, *jus ad bellum*, and *jus in bello* govern cyberweapons and their use. Although international law sporadically addresses specific weapons through arms control treaties or express prohibitions on their use, it typically controls them through general principles and rules applicable to all weapons. In the *jus ad bellum* context, for instance, the International Court of Justice (ICJ) has confirmed in the *Nuclear Weapons* advisory opinion that the U.N. Charter's use of force provisions, all of which reflect customary law, apply "regardless of the weapons employed." And the *jus in bello's* customary and treaty law requirement of a legal review of

<sup>\*</sup> Project Director, Tallinn Manual on the International Law Applicable to Cyber Warfare; Chairman, International Law Department, United States Naval War College; Honorary Professor, Strategy and Security Institute and Law School, Exeter University (UK); Honorary Professor of International Humanitarian Law, Durham University (UK). The views expressed in this article are those of the author in his personal capacity.

new weapons makes no sense unless the weapons are subject to the preexisting rules of international humanitarian law. Accordingly, the full applicability of the existing international legal regime to cyber-space has been accepted by the U.S. government, as evidenced by former State Department Legal Adviser Harold Koh's comments at the 2012 Cyber Command Legal Conference. The International Group of Experts who prepared the 2013 *Tallinn Manual on the International Law Applicable to Cyber Warfare (Tallinn Manual)* took an identical stance.

In fact, a thick web of international law norms suffuses cyberspace. These norms both outlaw many malevolent cyberoperations and allow states to mount robust responses. States have a sovereign right to exercise control over cyberinfrastructure and activities on their territory, as well as to protect them from harmful actions. In a principle confirmed in the first ICJ case, *Corfu Channel*, international law also obligates states to ensure that cyberinfrastructure on their territory is not used for acts that unlawfully affect other states. Most importantly, international law codified in the U.N. Charter's Article 2(4) prohibits states from directly or indirectly using cyberforce against other states. This rule is the most fundamental legal prohibition governing international relations, one that is often characterized as *jus cogens*.

In terms of responses to cyberoperations, states enjoy jurisdiction ratione loci, materiae, and personae to the same extent as with non-Moreover, cyber activities. when confronting unlawful cyberoperations conducted by other states, they may, pursuant to the law of state responsibility, respond with proportionate countermeasures, including cyber-countermeasures, that would themselves otherwise be unlawful. Although the prevailing view is that countermeasures may not include "uses of force," this position has been questioned, most notably in ICJ Judge Simma's separate opinion in the Oil Plat-Should a state experience cyberoperations from an unforms case. known source that threaten "grave and imminent peril" to its "essential interest[s]," it may take protective measures based on the "plea of necessity." This right exists even if doing so affects the (nonessential) interests of other states, such as shutting down networks on which other states rely or striking back at cyberinfrastructure involved in the offending operation.

At a certain level of severity, cyberoperations cross the "armed attack" threshold, thereby allowing states to defend themselves with force, including cyberforce, pursuant to Article 51 of the U.N. Charter and customary international law. The concept of armed attacks at least includes cyberoperations causing death, injury, or significant damage. Although the ICJ seemed to suggest otherwise in its *Congo* judgment and *Wall* advisory opinion, state practice appears to extend the right of self-defense to cyberattacks launched by nonstate actors such as a transnational terrorist group. Moreover, there is no cogent

2013]

reason to narrow the right of states to engage in anticipatory selfdefense against an imminent attack with respect to cyberspace. So long as an attacker possesses the capability to conduct cyberoperations at the armed-attack level, intends to do so, and defensive operations are required immediately lest the target state lose its opportunity to defend itself, the target may resort to force in self-defense to preempt the prospective attack.

With respect to the *jus in bello*, cyberoperations mounted by, or under the overall control of, one state against another may, depending on their severity, commence an international armed conflict. In such a case, international humanitarian law and the law of neutrality would apply to the operations. Accordingly, the prohibitions on attacking civilians, civilian objects, and other protected persons and objects would govern cyberattacks. Rules requiring the minimization of collateral damage and restricting such damage based on a cyberattack's anticipated military advantage would also apply. Moreover, belligerents may not use cyberinfrastructure in neutral territory; if it is so used and the neutral fails to address the breach, the aggrieved belligerent may take measures, by cyber or kinetic means, to put an end to the offending cyberoperations.

These normative strictures enjoy relative acceptance. However, surrounding them is, in the words of Professor H.L.A. Hart, a "penumbra of uncertainty" within which choice among alternative interpretations is possible. This penumbral mist presents opportunities and poses risks for states.

In this regard, several areas of ambiguity merit particular attention. For instance, it is clear that states may not allow cyberinfrastructure on their territory to be used to another state's detriment, but unclear whether states shoulder an obligation to monitor use or take measures to prevent misuse. Additionally, since countermeasures are available only to address state actions, interpretation of the terms "grave and imminent" and "essential" in the context of the plea of necessity lies at the heart of determinations as to when and how the victim state may address cyberoperations launched by nonstate actors.

The *jus ad bellum* is likewise characterized by interpretive elasticity. "Use of force" irrefutably includes acts that cause physical damage or injury, but not traditional economic or political sanctions. However, no authoritative criteria exist to qualify acts falling in the twilight between physically harmful cyberoperations and those that are purely economic or political in nature. For instance, the ICJ's *Nicaragua* judgment characterized arming and training guerillas, but not funding them, as uses of force without setting forth criteria for delineation. Moreover, it is questionable whether the historic exclusion of economic warfare should be interpreted as extending to cyberoperations that generate dramatic economic consequences. The *Tallinn Manual* has suggested a methodology for handling this uncertainty in practice, but fails in its attempt to articulate a clear threshold.

The law of self-defense similarly presents opportunities for interpretive use and abuse. For example, the speed of cyberoperations and the difficulty of accurate attribution complicate situations in which States might act anticipatorily. More fundamentally, the term "armed attack" has not been adequately defined. The scope of the term is central to the ongoing debates over cyberoperations since an armed attack is the condition precedent for exercise of the right of self-defense. Unfortunately, whereas the ICJ distinguished between "the most grave forms of the use of force (those constituting an armed attack) from other less grave forms" in Nicaragua, Harold Koh recently reiterated that even in the cyber context "there is no threshold for a use of deadly force to qualify as an 'armed attack' that may warrant a forcible response" for the United States. This statement suggests the United States denies the existence of a gap between a use of force and an armed attack, although this position is somewhat ameliorated by the use of the term "deadly." While affording states a degree of useful discretion, the lack of an adequate definition of self-defense opens the door to interpretive manipulation.

In the jus in bello, prohibitions are often framed in terms of "attacks," defined by the 1977 Additional Protocol I as "acts of violence." There is universal agreement that the term encompasses any operation, including cyberoperations, which cause injury or physical damage. However, controversy surrounds the interpretation of "attack" with respect to other effects. For example, consensus is lacking as to whether civilian data is a "civilian object" enjoying protection from attack. Likewise, there is no agreement regarding cyberoperations directed against civilians and civilian objects that, while not physically harming them, nevertheless generate serious harmful consequences like widespread economic loss. With regard to neutrality, it is uncertain whether malware qualifies as a weapon such that its transmission through neutral territory is unlawful based on the 1907 Hague Convention V and customary law or whether it is more akin to military radio transmissions, which may lawfully transit communications towers in neutral territory.

These questions are but a sampling of the myriad issues with respect to which states may, and should, engage in normative policy choices. The opportunity to make such choices has been occasioned by the penumbra of uncertainty surrounding the international law applicable to cyberspace. It must be cautioned that the interpretive ambitions of states will inevitably be tempered by the reality of norm formation and maintenance. Indeed, interpretive endeavors seldom survive intact because international law, crafted as it is by states through treaty and practice, necessarily reflects the contemporary values of the international community. As these values evolve, so too will

2013]

[Vol. 126:176

international law's prevailing interpretations. For example, current understandings of the terms "use of force," "armed attack," and "attack," which are based in part on the nature (as distinct from the severity) of an act's consequences, are certain to prove wanting in tomorrow's wired social construct. Moreover, outdated law will inexorably fall into desuetude as new law materializes in response to shifting values. Ultimately, the normative architecture governing cyberspace a decade from now will differ markedly from that which exists today.

180