Naval War College Review

Volume 68
Number 2 *Spring*

Article 3

2015

The Law of Cyber Targeting

Michael N. Schmitt

THE LAW OF CYBER TARGETING

Michael N. Schmitt

The 2008 war between Georgia and Russia was predictably short, as Russian military might quickly trumped Georgian nationalist enthusiasm. Beyond its momentous geopolitical implications, it was the first war in which cyber activities loomed large; the conflict marked the public birth of "cyber war," or at least cyber *in* war.[1]

Cyber operations were not a completely new phenomenon. Most notably, they had played a significant geopolitical role in the previous year, when "hacktivists" around the world directed malicious cyber operations at NATO member Estonia following its transfer of a Soviet-era statue commemorating the Great Patriotic War from central Tallinn to the outskirts of the capital.[2] But this was not "war" in the traditional sense of two or more states engaged in armed hostilities against each other. In the Georgian case, by contrast, the cyber activities took place on belligerent territory during an armed conflict that involved classic kinetic military operations. Although civilians launched most of the attacks, and while they caused no physical damage or injury, there is no question that, unlike the events in Estonia, international humanitarian law (IHL, also known as the law of war, law of armed conflict, and *jus in bello*) applied.

Cyber activities have become an indelible facet of contemporary warfare, not just for cyber-empowered militaries such as that of the United States, but also for low-tech forces. Terrorist and insurgent groups benefit from the use of the Internet to recruit fighters and to finance operations. Social media are exploited for purposes that range from passing targeting information to directing the deployment of forces (the insurgent "flash mob"). Mobile phones are as much part of the twenty-first-century kit bag as weapons, and e-mail and texting have become

pervasive means of military communication. The Arab Spring was a watershed in this regard, and cyber operations are ongoing in the conflicts in Ukraine and Syria. It is quite simply unimaginable that a contemporary conflict would not involve some manner of cyber operations, whether as simple as passing intelligence information using smartphones or as complicated as bringing down the enemy's integrated air-defense system.

In light of the role that cyber operations are playing in contemporary conflicts, attention must be paid to the law that governs these activities—to borrow a sports analogy, a team that takes the field without knowing the rules is usually going to lose, even if it is the better team. International law, and particularly IHL, exerts a powerful influence on tactics, operational planning, and strategic decision making in modern warfare. The fight can be won on the battlefield but lost in the court of public and international opinion when one side appears to have acted outside the law. Given the novelty of cyber operations as a method of warfare during an armed conflict, any alleged misuse, even at the tactical level, has the potential for strategic consequences.

The NATO Cooperative Cyber Defence Centre of Excellence, based in Tallinn, Estonia, has taken the global lead in addressing this issue. In 2009 it launched a three-year project to examine the application of international law, especially that governing the use of force, to cyber operations. Over twenty distinguished legal scholars and government legal advisers came together to produce the *Tallinn Manual on the International Law Applicable to Cyber Warfare,* a resource currently being expanded in the Centre's "Tallinn 2.0" project.[3]

Informed by the *Tallinn Manual* process, in which the author served as director, this article examines IHL's core norms—those governing targeting—as applied to cyber operations. It does so by following the legal logic applicable to virtually every targeting operation, from naval gunfire and air attack to special-forces operations and space attacks.[4] In each such case, those who plan, approve, and execute targeting missions have to ask the following questions:

- What law applies to my operation?
- May I engage the intended target?
- Is the weapon I want to use legal?
- What precautions must I take to avoid collateral damage?
- Do the scope and degree of likely collateral damage prohibit me from engaging the target?

There is now widespread agreement that international humanitarian law applies in its entirety to cyber operations conducted during an armed conflict.[5] Thus, the questions set out above apply fully to targeting in the cyber context,

albeit with a degree of interpretive creativity at times. This article will explain how each is resolved with respect to cyber operations. The explanation is designed for policy makers and operators who conduct, rely on, approve, or are targeted by cyber operations. In the contemporary strategic environment, knowledge of the law applicable to cyber warfare is quite simply indispensable.

THE APPLICABLE LAW (PART I)

The threshold question in every targeting operation is whether the international humanitarian law rules even apply. IHL comes into play only when there is a war—an "armed conflict," in technical legal parlance. There are two forms of armed conflict, international and noninternational.[6] The former exists when hostilities break out between two or more countries, whereas the latter involves hostilities at a fairly high level between an organized armed group and a state or between two or more organized armed groups. For example, the use of force against Ukraine by Russia clearly created an international armed conflict, whereas the hostilities between Bashar al-Assad's forces and those opposing his regime in Syria are noninternational in character. Unless one of these two forms of armed conflict exists, IHL is inapplicable, in which case human rights norms and domestic law serve as the core constraints on the targeting operation in question.

Whenever there is an armed conflict of either sort, IHL governs those cyber operations having a nexus with the conflict.[7] To take a simple example, it is no less a violation of IHL, and no less a war crime, to conduct cyber operations intended to kill members of the civilian population than it is to bomb or shell them; the same law prohibiting direct attacks on civilians is breached.[8] How that IHL rule applies is discussed below, but it is incontestable that it applies in its entirety to conflict-related cyber operations.

The somewhat more challenging legal question is whether cyber operations alone may qualify as armed conflicts to which IHL applies. In other words, if there is no armed conflict in the first place, can one begin as a result of cyber operations? The question is essential, because once an armed conflict breaks out, it becomes lawful to direct cyber and kinetic strikes against the armed forces and military objectives. This is so irrespective of blame for starting the conflict. To address this issue, it is necessary to distinguish between international and noninternational armed conflict.

If there are two or more states involved, the first criterion for an international armed conflict is met. The second, that "hostilities" have taken place, is somewhat ambiguous.[9] Two questions present themselves in this regard—one qualitative, the other quantitative. First, can cyber exchanges qualify as hostilities, or are they of such a unique nature that it is inappropriate to deem them such? It would seem logical that cyber operations that are qualitatively "attacks," as the term is used in

Naval War College Review, Vol. 68 [2015], No. 2, Art. 3

IHL, qualify as hostilities in the same way as kinetic attacks. Attacks, as explained further below, are operations causing damage or injury. There is no normative or practical logic for distinguishing between a cyber operation that damages objects or injures people and a kinetic operation with precisely the same effects.

However, whether cyber operations not qualifying as attacks under IHL may initiate an armed conflict remains unsettled. For instance, would cyber operations that result in a major loss of confidence in the stock market—a consequence far more serious than minor property damage or injury—qualify? As noted by the International Committee of the Red Cross (ICRC), "it would appear that the answer to these questions will probably be determined in a definite manner only through future State practice."[10]

The harsh reality of . . . military cyber activity is that the heavy reliance on civilian products and infrastructure dramatically expands the universe of targetable objects.

Second, is there any minimum severity below which an attack, whether kinetic or cyber, cannot be considered as having started an international armed conflict? The quantitative threshold is unclear in law. It is sometimes argued that, for instance, minor exchanges of fire between the forces of two states do not rise to the level of armed conflict. However, a better view is that which has been asserted by the ICRC for many years: "It makes no difference how long the conflict lasts, how much slaughter takes place, or how numerous are the participating forces."[11] This approach is, as lawyers say, more consistent with the "object and purpose" of IHL, since a state will want its civilians and civilian objects protected, and at the same time it will wish to be able to use lethal or destructive force against the other side if hostilities break out.

Accordingly, an international armed conflict could begin solely on the basis of cyber exchanges if two or more states were involved and the nature of the operations qualified them as attacks. To cite a well-known example, consider the 2010 Stuxnet operation against Iran. Assuming, solely for the sake of illustration, that it was states that conducted the operation, the damage arguably meant that the states involved were in an international armed conflict, at least for the period during which the damaging acts were under way.[12]

Cyber exchanges alone are far less likely to meet the two criteria for noninternational armed conflict.[13] First, the state must be facing an "organized armed group." Although the legal preconditions for qualification as such are rather complicated, in the cyber context the pressing question is whether they are met by a group organized entirely online. Organized armed groups have to be in some way "commanded," and some degree of structure must exist that allows their members to operate as a unit.[14] It is also often suggested that "organization" requires a

means to enforce IHL within the group.[15] It is difficult to see how a virtual group whose members may not even know each other's names or physical locations could meet this condition.

Additionally, the group in question must be armed. The logic underlying the discussion of international *armed* conflict would appear useful by analogy. "Armed" can be interpreted as a requirement for "hostilities," which are acts that qualify as "attacks." In this context, therefore, an organized armed group is one that conducts kinetic or cyber attacks. Thus, a group that merely conducted nondestructive denial-of-service operations, for example, would not qualify. This is one reason why the operations against Estonia did not rise to the level of a noninternational armed conflict. Those involved were acting in concert, but they were not organized into one or more particular armed groups.

Second, and unlike international armed conflict, the violence associated with a noninternational armed conflict must be protracted and must reach a high level of severity. It does not include "situations of internal disturbances and tensions, such as riots, isolated and sporadic acts of violence and other acts of a similar nature."[16] Even cyber operations causing death or destruction will sometimes not suffice. Neither would a single dramatic cyber operation, such as a cyber terrorist attack, qualify, even if causing harm far above the level just characterized, because that harm would not be protracted. In the simplest terms, the cyber conflict must start looking like a war. To turn again to the Estonian case, the hacktivist operations did not rise to this level because, despite widespread disruption of societal functions, there was no physical damage or injury.

Nonstate-actor cyber operations meeting these demanding criteria are currently unlikely. A more probable scenario is one in which cyber operations accompany kinetic ones and are governed by IHL on that basis. Therefore, when nonstate-actor cyber operations occur in isolation from kinetic attacks, they will typically be governed by the domestic law of states exercising jurisdiction over the persons and particular subject matter involved, as well as by human rights law, but not by the IHL norms described below.

THE APPLICABLE LAW (PART II)

Once it is determined that an armed conflict to which IHL applies is under way, the next step is to determine whether the law of targeting applies to the cyber operation in question.[17] Doing so is more difficult than might appear at first glance. Indeed, the *Tallinn Manual* experts struggled with the subject for three years without reaching full consensus.

Any discussion of targeting begins with the principle of "distinction," which is codified in Article 48 of the 1977 Additional Protocol I to the four 1949 Geneva Conventions: "The Parties to the conflict shall at all times distinguish between

the civilian population and combatants and between civilian objects and military objectives and accordingly direct their operations only against military objectives."[18] The United States, though not a party to that instrument, recognizes Article 48 as reflective of customary international law, which binds all states.[19] Indeed, the principle is arguably the most important in IHL, one that the International Court of Justice has labeled as one of the two "cardinal" principles of IHL.[20] In international law circles, a major debate with particular resonance in the cyber context is ongoing regarding whether the principle of distinction rules out all operations against objects and persons that do not qualify as military objectives, especially civilians and civilian objects. Textually, the article certainly appears to say as much, but such a conclusion would be both counterintuitive and ahistorical. After all, military operations, such as psychological operations, have been directed against civilian populations for centuries.

A closer look into Additional Protocol I reveals a series of prohibitions and restrictions on "attack" that operationalize the principle: *attacks* against civilians and civilian objects are prohibited, indiscriminate *attacks* are forbidden, parties to a conflict must take precautions to minimize civilian harm when planning and conducting *attacks,* a defender must take precautions to protect the civilian population against the effects of *attacks,* and so forth.[21] Helpfully, "attacks" are defined in the protocol as "acts of violence against the enemy, whether in offence or defence."[22] The characterization of an attack as a violent act is repeated throughout the treaty and in ICRC and other commentaries thereon.[23]

It would seem, however, that the protocol is inaptly worded. Violent *acts* are of less concern in IHL than are violent *consequences*. This has been obvious for decades, the paradigmatic examples being the prohibitions on chemical, biological, and radiological attacks, which are not violent in the sense of releasing kinetic force but have violent consequences, notably death. By the same logic, a cyber operation causing injury to persons or damage to objects is an attack subject to all the relevant IHL rules on attacks.[24]

But controversy surrounds the issue of whether the notion of attacks should be interpreted more broadly. A cyber operation targeting civilian cyber infrastructure ("communications, storage, and computing resources upon which information systems operate") without physical effects could be far more detrimental than one causing limited damage.[25] Consider an attack during an armed conflict on the enemy's banking, taxation, government pension, or airline reservations systems. Critics of a restrictive interpretation argue that it seems incongruent to prohibit only operations having physical effects.

Two methods have surfaced that take account of this reality without the necessity of either successfully negotiating new treaty terms (an unlikely eventuality) or interpreting the current law in a fashion that renders it unrecognizable. First,

there are those who would interpret data as an object, such that an operation that manipulated, altered, or deleted civilian data would be prohibited.[26] The conceptual problem is that the ICRC commentary to Additional Protocol I describes an object as something "tangible," and data certainly is not that.[27] Goal-oriented legal academics have proposed creative interpretation as a means of hurdling this particular obstacle but fail to offer a viable practical alternative. If data is treated as an object, any operation that manipulates civilian data would qualify as "damage" to (alteration of data) or "destruction" of (deletion of data) a "civilian object" and would thus be unlawful. As an example, deletion of a civilian's forum or blog post would be a violation of IHL, as would nondestructive psychological cyber operations directed at the civilian population. Moreover, such an interpretation would dramatically affect application of the rule of proportionality and the requirement to take precautions in attack. Both, as discussed below, extend further protection to civilian objects, the former by prohibiting attacks likely to cause "excessive" collateral damage to civilian objects, the latter by requiring an attacker to take feasible measures to limit damage to civilian objects.[28] International humanitarian law is a careful balancing of humanitarian concerns with military necessity; simply styling data as an object would throw this balance out of kilter, by barring operations that today are considered lawful in both their cyber and traditional guises.

The second approach, and the one adopted by a majority of the experts involved in the *Tallinn Manual* project, is to include "loss of functionality" in the concept of damage.[29] On this view, a cyber operation that affects the functionality of cyber infrastructure (from a laptop computer to a SCADA system*) in a manner that necessitates repair qualifies as an attack even if no physical damage results. This approach makes sense, for it is fair to describe an item as damaged when it does not work; it is broken, even though it may not be physically damaged. Among the experts taking this position during the *Tallinn Manual* project there were various shades of opinion. Some were of the view that necessity to reload an operating system satisfied the damage criterion. Others went so far as to say that cyber operations affecting data stored on the computer's drives would suffice, although this was a minority view.

The implications of the majority positions set out above are significant. Unless a cyber operation has consequences that at least affect the functionality of an object, it is not damaged in the IHL sense and the operation does not qualify as an attack. Therefore, the operation is not subject to the prohibition on conducting

* Supervisory control and data acquisition—referring to "computer systems and instrumentation that provide for monitoring and controlling industrial, infrastructure, and facility-based processes, such as the operation of power plants, water treatment facilities, electrical distribution systems, oil and gas pipelines, airports, and factories" (*Tallinn Manual,* p. 262).

attacks against civilian objects. As a result, it is generally legal during an armed conflict to conduct cyber operations directed against civilian objects, so long as these objects are not physically damaged or do not lose functionality (or somehow result in injury to civilians). To illustrate, it would be lawful to conduct denial-of-service attacks that blocked civilian e-services such as tax collection or the payment of pension benefits but did not harm or affect the functionality of the associated cyber infrastructure, at least until the economic consequences became so severe that they began to have physical effects, such as starvation or illness. Similarly, by the majority approach it would be lawful to alter or destroy data so long as no consequences amounting to injury, physical damage, or loss of functionality are manifest; examples could include government archives, birth or citizenship records, business records, and market returns. Although such operations might raise serious moral, political, and social issues, they appear lawful today.

THE TARGET

Assuming that a cyber operation occurs during an armed conflict and qualifies as an attack, the next hurdle is determining whether the target is a lawful one. Cyber operations most frequently implicate the prohibition on attacking civilian objects. In IHL, civilian objects are defined negatively as "all objects which are not military objectives."[30] Military objectives are "objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage."[31]

The equipment and facilities of the armed forces are military objectives by nature; a command-and-control facility and cyber infrastructure developed for specific military tasks both qualify, for example, on this basis. A particular location can also be a military objective, as when cyber means are used to open a dam's gates to flood an area and deny its use to the enemy. Aside from military equipment, the most likely military objective in the cyber context is an object that qualifies by the "use" criterion—that is, one that was formerly or is still being used for civilian purposes but is now being employed, at least in part, for military ends. It should be cautioned that a rule of reason holds when applying this criterion to cyber activities. For instance, the mere fact that the military sends e-mail over the Internet does not render the entire Internet a lawful target. Finally, a civilian object can become a military objective through "purpose," which refers to the intended future use of an object. For example, if there is reliable intelligence that a civilian server farm will soon begin to store military data, the farm is a military objective that may be attacked even before data storage begins.

These definitions do not present any particular problems in the cyber setting. However, it must be acknowledged that the pervasive use of civilian cyber infrastructure for military purposes has transformed much of it into the character of valid military objectives. When an object is used for both civilian and military purposes, it is labeled "dual use." In targeting terms, the term applies whether something is exclusively used for military purposes, is shared by civilian and military users, or is only used to a limited degree by the military—it qualifies as a targetable military objective. The civilian aspects of the target are relevant to the requirements for proportionality and precautions in attack as described below, but civilian use does not diminish its qualification as a military objective.

There is now widespread agreement that international humanitarian law applies in its entirety to cyber operations conducted during an armed conflict.

To take a simple example, many air-traffic-control and airspace-management systems serve both civilian and military aircraft. When this is the case, they are military objectives irrespective of the extent of civilian reliance on them. The communications lines to which the systems are connected are also dual-use and so too qualify as military objectives, as do any routers involved and any servers on which their data is stored. The harsh reality of twenty-first-century military cyber activity is that the heavy reliance on civilian products and infrastructure dramatically expands the universe of targetable objects, including systems on which important civilian functions rely.

The introduction of cyber capabilities into contemporary combat has also exacerbated a long-standing debate over the very notion of military objectives. All states and legal commentators agree that the term encompasses "war fighting" and "war supporting" objects. The former are those used to conduct military operations, whereas the latter include objects on which military operations rely in some relatively direct sense, such as factories that make munitions, weapons, or equipment (including computer equipment) used by the military, even when they also produce civilian products. They may not necessarily be attacked, because of the rule of proportionality and the requirement to take precautions, but they unquestionably qualify as military objectives. What is especially significant with regard to the war-supporting category in the cyber context is the extent to which the dependence of the armed forces on civilian products and infrastructure makes not only the objects in question legally targetable but also the facilities that produce them.

However, a third category, "war sustaining" objects, has generated widespread controversy. The U.S. Navy's *Commander's Handbook on the Law of Naval*

Operations, the most current U.S. manual addressing international humanitarian law, labels enemy war-sustaining objects as military objectives susceptible to lawful attack.[32] An annotated version of the previous edition of the handbook offers the example of cotton during the American Civil War.[33] But for the export of cotton, the Confederacy would have been unable to finance its war effort. Cotton exports, then, sustained the war; therefore, according to this approach, that industry was lawfully targetable. The contemporary analogue would be those aspects of an economy or governmental financial system on which the enemy relies to fund participation in the conflict. Obvious examples are the oil industries of countries that depend heavily on oil exports for funds; although the United States has never developed the concept with any granularity, other examples might also include the tax systems, financial systems, transport networks, and the like.

The significance of this approach in its application to the cyber environment cannot be overstated. Many war-sustaining targets cannot be struck kinetically in a fashion that would generate the same effects as cyber attacks. Consider the banking system. While kinetic attacks against banks would be highly disruptive, they would be unlikely, given the limitations of kinetic weaponry and the number of potential targets falling into this category, to create strategic effects on the order of undermining the sustainability of the war effort. However, cyber attacks that would, for instance, render dysfunctional the cyber infrastructure on which the banking system relies could bring the entire system down. The war-sustaining debate once loomed large; the ability of cyber operations to make war-sustaining attacks possible and effective at the operational and strategic levels will probably reinvigorate it. This is especially so in light of the fact that very few states have openly embraced the U.S. approach, thereby rendering the world's most cyber-empowered military an outlier on the matter. Ironically, the United States is itself highly vulnerable to attacks on its own "war sustaining" infrastructure, thereby raising the question whether its interpretation is ill-advised when applied to the cyber context.

In addition to objects, "persons" may qualify as lawful targets. It is, of course, possible to attack people by cyber means—for instance, by starting fires in facilities in which they are located, interfering with air-traffic control relied on by the aircraft transporting them, causing train collisions, and so forth. Additionally, individuals involved in cyber operations may be targeted kinetically once they have been identified and located. The issues are which people are targetable, as a matter of law, and when they may be targeted.

Obviously, members of the armed forces who conduct cyber operations are always targetable (unless hors de combat); they are combatants.[34] The rules regarding when civilians may be targeted are far more complex. To address this, the International Committee of the Red Cross sponsored a five-year (between

2003 and 2008) research study involving a group of forty international experts.[35] The experts agreed that members of an organized armed group, as defined above, are targetable while they are members of the group.[36] They disagreed, however, over precisely which members of the group were targetable. The ICRC was of the position that only those with a "continuous combat function" could be attacked. Such functions encompass roles in the group that involve activities likely to affect the enemy adversely.[37] Some individual participants in the project, including the author, countered that all members of a group formed to conduct hostilities (or the members of the armed wing of a group that includes other functions, such as Hamas) could be attacked, a position that appears to be favored by the United States, Israel, and other countries with significant combat experience.[38]

Applied to cyber, the approaches taken to direct participation lead in different directions. Take an organized armed group that conducts kinetic hostilities but also has "cyber operators." All those who conduct cyber operations against the enemy or who defend against the enemy's operations have continuous combat functions and therefore would be targetable by either approach. Other members may have such cyber-related duties as maintaining propaganda websites or recruiting members. By the ICRC approach, they do not have continuous combat functions and therefore would not be targetable unless they assumed such functions within the group. By the alternative approach, they could be attacked at any time, on the basis of their membership in the group.

Individuals unaffiliated with organized armed groups or, in the ICRC approach, who do not have continuous combat functions in such groups are targetable only "for such time" as they "take a direct part in hostilities."[39] An act amounts to direct participation when it meets three criteria.[40] First, it must either adversely affect the military operations or military capability of one of the parties to the conflict or injure or damage persons or objects protected by IHL, such as civilians and civilian objects.[41] It is important to understand that this criterion does not require that the activity qualify as an attack. As an example, gathering and disseminating tactical- and operational-level intelligence by cyber means suffices, as would probing enemy systems to identify vulnerabilities.

Second, the qualifying activity must directly cause the harm or be an integral component of the operation that does so.[42] There has been some controversy over this requirement with respect to the production of improvised explosive devices and services as voluntary human shields. Although both activities are sometimes characterized as indirect, the better position is that causal nexus between such activities and harm to the enemy is sufficiently direct.[43] The cyber analogue would be developing software specific to an attack on the enemy system or allowing cyber operations to be launched from one's home or business by others. One thing on which all parties agree is that factory workers do not qualify as

Naval War College Review, Vol. 68 [2015], No. 2, Art. 3

direct participants in hostilities. This being so, individuals involved in the general production of cyber infrastructure and equipment or in its general (as distinct from operational) maintenance are not targetable direct participants, although the *facilities* in which they operate qualify as military targets by virtue of their use.

The third requirement is that there be a nexus between the activity and the conflict.[44] In other words, the activity must be related to the ongoing conflict, as distinct from being an act of criminality or mere maliciousness. Although the facts of particular cases are sometimes difficult to discern, experts are in accord on this criterion.

It is difficult to overstate the importance of the direct-participation rules in the cyber context. The Georgia-Russia armed conflict, as well as subsequent ones, demonstrates that the civilian population is highly likely to become involved in the cyber aspects of the conflict. For instance, in the Georgia case a website (StopGeorgia.ru) containing cyber targets and downloadable "malware" (malicious software) necessary to conduct cyber operations appeared online soon after the launch of kinetic operations.[45] The site proved effective in enabling cyber operations by civilians against Georgian military and civilian cyber targets. As this example illustrates, it is far easier to "cyber arm" a civilian population than to arm it with traditional weaponry. Additionally, many individuals have the know-how to conduct harmful cyber operations; all they require to begin participating in the hostilities is connectivity.

To borrow a sports analogy, a team that takes the field without knowing the rules is usually going to lose, even if it is the better team.

To compound matters, the scope of activities constituting direct participation in hostilities is broad. Conducting a simple denial-of-service operation, building a botnet* for use against the enemy, or texting to report visual sightings of enemy forces would all qualify as direct participation that justifies lethally attacking the civilian involved. As should be apparent, the direct-participation rule could make the pool of targetable individuals extremely large in future conflicts, far more than is the case in classic conflict.

That said, one possible obstacle to far-reaching application of the rule is that a direct participant is targetable only "for such time" as he or she is so participating.[46] The ICRC has suggested that this period includes measures preparatory to specific acts of direct participation, as well as deployment to and return from the activity concerned.[47] This is a rather impractical standard in the cyber context. Except for close-access operations (those involving in-person manipulation of cyber infrastructure), there is usually no deployment to and from cyber

* "A network of compromised computers, the 'bots,' remotely controlled by the intruder, 'the botherder,' used to conduct coordinated [malicious] cyber operations" (*Tallinn Manual,* p. 257).

operations; they are conducted remotely. Thus, by the ICRC approach, the direct participant would have to be caught in the act, a standard that dramatically narrows the window of targetability. Further rendering this position impracticable is the fact that cyber operations can be very brief, sometimes so brief that an attacker cannot be identified to a level of reasonable confidence before the operation is over. Therefore, the better approach is to characterize an individual who engages in multiple cyber operations that are part of an ongoing cyber campaign as a direct participant targetable throughout the period of activity. Once individuals definitively withdraw from participation, they regain their protection from attack, but not before.[48]

THE WEAPON

While certain uses of cyber weapons (destructive or injurious malware), such as "attacking" civilians, violate IHL, cyber weapons may also be unlawful per se—that is, irrespective of actual use. The prohibition most relevant in this regard is that on indiscriminate means (weapons).[49] Weapons are prohibited when they either cannot be directed at a specific military objective or generate uncontrollable effects. In both cases, the weapons are indiscriminate in the sense that they are incapable of distinguishing between combatants and civilians or between civilian objects and military objectives. The paradigmatic example of the former is the V-2 rocket used during World War II, which had a guidance system so rudimentary that the rocket could not be reliably aimed at individual military objectives. Biological contagions illustrate the latter, because an attacker employing them cannot control their spread from human to human.

Cyber weapons may at times run afoul of these prohibitions. For example, consider malware intended for use against military cyber infrastructure linked to civilian networks. If the malware is designed to spread randomly throughout the system into which it is introduced, it is indiscriminate by nature and prohibited per se. Similarly, malware developed for placement on a website that is open to civilians and combatants alike would qualify as indiscriminate irrespective of any desire on the part of its user to affect only military systems. Perhaps the best-known indiscriminate cyber weapon is a malicious but seemingly innocuous e-mail attachment sent to a combatant's private e-mail account. Since the attacker has no control over to whom it might be forwarded, the e-mail, depending on its apparent nature (e.g., a humorous e-mail likely to be forwarded), would be indiscriminate.

It must be cautioned that the restrictions on indiscriminate weapons apply only when the cyber weapon in question is designed to conduct attacks. They do not bear on malware that does not cause injury, damage, or loss of system functionality. For instance, an e-mail attachment that when opened simply enables

future access by the sender would not be unlawful under IHL, even though the sender might not be able to control its further spread into civilian systems.

Because of this, as well as the fact that advanced cyber weapons likely to be used by states in armed conflict are by their nature designed to exploit particular vulnerabilities in specific systems, few cyber weapons violate the prohibition on indiscriminate weapons. For example, bespoke cyber weapons can be employed against closed military systems in which the risk of bleed-over into civilian networks is low. Of course, there is always some risk of unintentional or unanticipated migration into civilian systems, as illustrated by the Stuxnet malware, which, contrary to the intent of its designers, escaped the nuclear enrichment plant that had been targeted. Yet the risk of malfunction or unanticipated effects is a pervasive feature of weaponry writ large; only when the weapon is *incapable* of being aimed or controlled is it prohibited as indiscriminate.

PRECAUTIONS TO AVOID CIVILIAN HARM

Even when employing a lawful cyber weapon against a lawful target, an attacker must take "constant care" to "spare the civilian population, civilians and civilian objects."[50] To this end the law specifies a number of precautionary measures. The attacker must do everything feasible to verify that the target is not protected by IHL;[51] must select the weapon, tactic, and target that will minimize civilian harm without forfeiting military advantage;[52] must cancel or suspend an attack when reason to believe that the attack may be unlawful comes to light;[53] and must warn the civilian population of any attack that may affect it, unless doing so would not be feasible in the circumstances.[54]

Cyber capabilities raise a number of issues in this regard. They can, for example, be used to gather target information. If doing so would improve knowledge of the target's legal status (and if it is militarily feasible in the circumstances, given such factors as attack timing and competing demands on the cyber asset), the attacker must undertake the effort. Cyber operations may also provide a means of issuing warnings to the civilian population of both cyber and kinetic attack. For instance, general warnings of attack could be transmitted through civilian systems networked to military cyber infrastructure urging measures to be taken to safeguard them from the effects of attack on the military objectives.

However, the most significant impact of the precautions-in-attack rules lies in the requirement to consider alternative weapons, tactics, and targets to minimize civilian incidental harm. To illustrate, it may be possible to neutralize an integrated air-defense system by cyber means instead of by conducting kinetic attacks against its assorted components. Since cyber operations would in most cases be less likely to cause collateral damage, they would be required by law in lieu of kinetic alternatives, if their employment is feasible and militarily sensible. Cyber

operations may also open the possibility of striking different targets to achieve a desired effect. As an example, to disrupt enemy operations it may be possible to use cyber assets against communications infrastructure serving a command-and-control facility located near civilians, rather than attacking the facility itself, and achieve precisely the desired effect. Indeed, it could prove useful to preserve the facility to exploit it subsequently by using cyber means to transmit false instructions and other information to the enemy forces.

It must be emphasized that the precautions-in-attack rule regarding selection of weapons, tactics, and targets is obligatory. If cyber means are reasonably available, their use makes military sense in the circumstances, and their employment would not diminish the likelihood of operational success, the attacking force must use them. Failure to do so will violate the law. It is accordingly prudent for those who plan, approve, and execute military operations to have ready access to cyber expertise that can apprise them of cyber options. Ignorance is not an excuse for failure to comply with the rule in situations where the individual concerned should have known that a cyber operation was feasible in the circumstances and would likely have resulted in less collateral damage.

COLLATERAL DAMAGE

Once the attacker has surveyed the range of possible operations to achieve the desired effects and selected that viable alternative that best minimizes collateral damage, the operation is assessed against the rule of proportionality. This rule provides that "an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated" is prohibited.[55]

Two mistakes have proved common in application of the rule of proportionality. First, the rule is often mischaracterized as a balancing test in which military advantage and collateral damage are somehow accorded values that presumably can be compared. Not only is it difficult to imagine how this could be done in practice, but portraying proportionality as a balancing test runs counter to the plain text of the rule, which precludes an attack only when the collateral damage is "excessive." "Excessive" refers to a "significant imbalance," one in which it is reasonably clear that causing the expected degree of collateral damage is not justified by the military advantage the attacker hopes to attain.[56] Since cyber operations can generate effects that are not typically present in warfare and are therefore somewhat unfamiliar, fidelity to the "excessive" standard is essential, as it affords the attacker the correct degree of discretion.

Second, the rule is unfortunately often applied *post factum*. However, as is clear from its text, the proportionality assessment is made *ex ante* (i.e., at the

Naval War College Review, Vol. 68 [2015], No. 2, Art. 3

outset). Expected collateral damage is assessed against the *anticipated* military advantage. The actual collateral damage caused and the military advantage that actually results are relevant to evaluating the reasonableness of the attacker's pre-attack proportionality assessment but are not dispositive of whether the attacker has satisfied the rule of proportionality. This is again an important point in the cyber context, because of the widespread linkage of civilian and military systems and the difficulty an attacker may face in evaluating potential effects at the time the cyber mission is planned, approved, or executed.

Cyber activities have become an indelible facet of contemporary warfare, not just for cyber-empowered militaries such as that of the United States, but also for low-tech forces.

With respect to the substantive aspects of proportionality, cyber operations can serve to minimize collateral damage and therefore make compliance with the rule more likely. The networked nature of cyber infrastructure, however, heightens the risk of indirect effects on civilian systems. This is particularly true in light of the wide-ranging reliance of some militaries on dual-use cyber systems. To the extent to which indirect effects are foreseeable, they must be considered when making proportionality calculations. That said, the proportionality rule, like the prohibition on weapons generating uncontrollable effects, requires the consideration only of "loss of civilian life, injury to civilians," and "damage to civilian objects." Other, indirect effects of a cyber operation on civilians, civilian objects, and other persons and objects protected by IHL are not factored into the equation.

Cyber operations appeared on the battlefield in a dangerous interpretive void. As so often happens, technology has outpaced the law, or at least in this case full understanding of how extant law governs emerging cyber capabilities. Such a state of affairs is always strategically perilous. On the one hand, options that are in fact lawful are sometimes needlessly taken off the table out of misguided concern about their legality. On the other, unlawful options are at times seriously considered, thereby risking public and international condemnation should they be selected.

The normative fog of cyber war is beginning to clear, albeit slowly. This article has surveyed those aspects of international humanitarian law relevant to targeting, the activity during an armed conflict that poses the greatest risk to the defender and the civilian population. But targeting equally poses the greatest risk to the attacker, not only from an operational perspective, but also in terms of mission accomplishment. Characterization of a cyber operation as unlawful can quickly wipe away any gains that the operation has attained. It is accordingly essential that those occupying roles having responsibility for overseeing and

executing cyber operations develop a degree of understanding of their normative boundaries.

NOTES

The views expressed are those of the author in his personal capacity.

1. On the Georgian case, see Eneken Tikk, Kadri Kaska, and Liis Vihul, *International Cyber Incidents: Legal Considerations* (Tallinn, Est.: NATO Cooperative Cyber Defence Centre of Excellence [hereafter NATO CCD COE], 2010), pp. 66–90.
2. Ibid., pp. 14–34.
3. See Michael N. Schmitt, gen. ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge, U.K.: Cambridge Univ. Press, 2013) [hereafter *Tallinn Manual*]. For the Tallinn 2.0 project, see "Tallinn Manual," *CCDCOE: NATO Cooperative Cyber Defence Centre of Excellence,* ccdcoe.org/.
4. For a discussion of the law of targeting in general, see Michael N. Schmitt and Eric Widmar, "'On Target': Precision and Balance in the Contemporary Law of Targeting," *Journal of National Security Law and Policy* 7 (2014).
5. *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,* UN Doc. A/68/98 (New York: 24 June 2013), para. 19, undocs.org/A/68/98 (regarding international law generally). This is the U.S. position; Harold Honju Koh (Legal Adviser, U.S. State Dept., remarks to USCYBERCOM Inter-Agency Legal Conference, 18 September 2012), available at www.state.gov/. The International Committee of the Red Cross has endorsed the same view; International Committee of the Red Cross [hereafter ICRC], *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts,* ICRC Doc. 31IC/11/5.1.2 (Geneva: 31 October 2011), p. 37.
6. Article 2 of the four 1949 Geneva Conventions addresses international armed conflict, while Article 3 deals with noninternational armed conflict. Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, 12 August 1949, 6 UST 3114, 75 UNTS 31; Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, 12 August 1949, 6 UST 3217, 75 UNTS 85; Convention (III) Relative to the Treatment of Prisoners of War, 12 August 1949, 6 UST 3316, 75 UNTS 135; Convention (IV) Relative to the Protection of Civilian Persons in Time of War, 12 August 1949, 6 UST 3516, 75 UNTS 287.
7. On the topic generally, see Michael N. Schmitt, "Classification of Cyber Conflict," *International Law Studies* 89 (2013), p. 233.
8. For each of the norms, this article will cite the relevant treaty provision, although the United States is not a party to that most often cited, Additional Protocol I to the 1949 Geneva Conventions; the ICRC's Customary IHL study rule indicating that the norm is customary in nature, i.e., binding on all states; the relevant paragraph from the U.S. Navy's *Commander's Handbook on the Law of Naval Operations;* and the applicable *Tallinn Manual* rule reflecting its application in the cyber context. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, art. 2, 8 June 1977, 1125 UNTS 3 [hereafter Additional Protocol I]; Jean-Marie Henckaerts and Louise Doswald-Beck, eds., *Customary International Humanitarian Law* (Cambridge, U.K.: Cambridge Univ. Press for the ICRC, 2005), rule 1; U.S. Navy Dept. and U.S. Homeland Security Dept., *The Commander's Handbook on the Law of Naval Operations,* NWP 1-14M/MCWP 5-12.1/COMDTPUB P5800.7A (Washington, D.C.: 2007) [hereafter *Commander's Handbook*], para. 8.3; *Tallinn Manual,* rule 32.
9. *Tallinn Manual,* p. 82.
10. ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts,* p. 37.

11. Jean Pictet, ed., *Commentary: Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field* (Geneva: ICRC, 1952), p. 20.
12. But see discussion in Cordula Droege, "Get off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians," *International Review of the Red Cross* 94, no. 886 (2012), p. 548.
13. Prosecutor v. Tadić, Case No. IT-94-1-l, Decision on Defence Motion for Interlocutory Appeal on Jurisdiction, p. 70 (International Criminal Tribunal for the former Yugoslavia, 2 October 1995).
14. Prosecutor v. Limaj, Case No. IT-03-66-T, Judgment, para. 89 (International Criminal Tribunal for the former Yugoslavia, 30 November 2005).
15. See, e.g., Yves Sandoz, Christophe Swinarski, and Bruno Zimmermann, eds., *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Geneva: ICRC, 1987) [hereafter *Additional Protocol Commentary*], p. 62; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-international Armed Conflicts, art. 1(1), 8 June 1977, 1125 UNTS 609 [hereafter Additional Protocol II].
16. Additional Protocol II, art. 1(2) (the provision is generally characterized as reflecting customary law regarding qualification as a noninternational armed conflict). See also Rome Statute of the International Criminal Court, art. 8.2(d), 17 July 1998, 2187 UNTS 90.
17. On the subject generally, see Michael N. Schmitt "'Attack' as a Term of Art in International Law: The Cyber Operations Context," in *Proceedings of the 4th International Conference on Cyber Conflict,* ed. Christian Czosseck, Rain Ottis, and Katharina Ziolkowski (Tallinn, Est.: NATO CCD CCOE, 2012), p. 283, available at ccdcoe.org/.
18. Additional Protocol I, art. 48. See also Henckaerts and Doswald-Beck, *Customary International Humanitarian Law,* rules 1 & 7; *Tallinn Manual,* rule 31.
19. *Commander's Handbook,* para. 8.2. Customary international law is a form of law unique to international law. It "crystallizes" into a norm binding on all states once widespread state practice that is engaged in out of a sense of legal obligation *(opinio juris)* exists. Although unwritten, it is of equal legal force to treaty law; Statute of the International Court of Justice, art. 38, 26 June 1945, 59 Stat. 1055, 33 UNTS 993.
20. Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 ICJ 226, para. 78 (July 8).
21. Additional Protocol I, arts. 51(2), 52(1), 57, 58 [emphasis added].
22. Ibid., art. 49.
23. *Additional Protocol Commentary,* para. 1875; Michael Bothe et al., *New Rules for Victims of Armed Conflicts* (Leiden, Neth.: Martinus Nijhoff, 1982), p. 289. For attack as a violent act, see, e.g., Additional Protocol I, arts. 35, 51(1), 51(2), 55, 56(1).
24. *Tallinn Manual,* rule 30.
25. Quote in ibid., p. 258.
26. Ibid., p. 126.
27. For "tangible," *Additional Protocol Commentary,* paras. 2007–2008.
28. See discussion of this issue in Michael N. Schmitt, "The Notion of 'Objects' during Cyber Operations: A Riposte in Defence of Interpretive Precision," *Israel Law Review* 48 (forthcoming 2015).
29. *Tallinn Manual,* pp. 108–109.
30. Additional Protocol I, art. 52(1). See also Henckaerts and Doswald-Beck, *Customary International Humanitarian Law,* rule 9; *Commander's Handbook,* para. 8.3; and *Tallinn Manual,* rule 38.
31. Additional Protocol I, art. 52(1). See also Henckaerts and Doswald-Beck, *Customary International Humanitarian Law,* rule 8; *Commander's Handbook,* para. 8.2; and *Tallinn Manual,* rule 38.
32. *Commander's Handbook,* para. 8.2.
33. A. R. Thomas and James C. Duncan, eds., *Annotated Supplement to the Commander's Handbook on the Law of Naval Operations* (Newport, R.I.: Naval War College, 1999), p. 403.
34. Additional Protocol I, arts. 50(1), 51(2); Henckaerts and Doswald-Beck, *Customary International Humanitarian Law,* rule 1;

Commander's Handbook, para. 8.2.1; *Tallinn Manual,* rule 34.

35. Nils Melzer, ed., *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law* (Geneva: ICRC, 2009).
36. Ibid., p. 71. The author served as one of the experts. On the issue, see Kenneth Watkin, "Opportunity Lost: Organized Armed Groups and the ICRC 'Direct Participation in Hostilities Interpretive Guidance,'" *New York Journal of International Law and Politics* 42 (2010), p. 641.
37. Melzer, *Interpretive Guidance,* p. 71.
38. See discussion in Michael N. Schmitt, "The Interpretive Guidance on the Notion of Direct Participation in Hostilities: A Critical Analysis," *Harvard National Security Journal* 1, no. 5 (2010), pp. 21–24.
39. Additional Protocol I, art. 51(3); Additional Protocol II, art. 13(3); Henckaerts and Doswald-Beck, *Customary International Humanitarian Law,* rule 6; *Commander's Handbook,* para. 8.2.2; *Tallinn Manual,* rule 35.
40. See generally Michael N. Schmitt, "Deconstructing Direct Participation in Hostilities: The Constitutive Elements," *New York Journal of International Law and Politics* 42 (2010), p. 698.
41. Melzer, *Interpretive Guidance,* p. 47.
42. Ibid., p. 51.
43. See ibid., pp. 53–54, 56–57; and Schmitt, "Deconstructing Direct Participation in Hostilities," pp. 732–34.
44. Melzer, *Interpretive Guidance,* p. 58.
45. Tikk, Kaska, and Vihul, *International Cyber Incidents,* p. 73.
46. See generally Bill Boothby, "'And for Such Time As': The Time Dimension to Direct Participation in Hostilities," *New York Journal of International Law and Politics* 42 (2010), p. 741. Note that neutrality rules would also limit a state's options in striking back at direct participants operating from neutral territory; *Tallinn Manual,* chap. 7.
47. Melzer, *Interpretive Guidance,* pp. 69–73.
48. Other aspects of international law may also limit the targetability of an individual. For instance, as mentioned above, the law of neutrality will generally bar conducting operations against a person located on neutral territory; *Tallinn Manual,* rules 91–94.
49. Additional Protocol I, arts. 51(4)(b), (c); Henckaerts and Doswald-Beck, *Customary International Humanitarian Law,* rule 71; *Commander's Handbook,* para. 9.1.2; *Tallinn Manual,* rule 43.
50. Additional Protocol I, art. 57(1); Henckaerts and Doswald-Beck, *Customary International Humanitarian Law,* rule 15; *Commander's Handbook,* para. 8.1; *Tallinn Manual,* rule 52.
51. Additional Protocol I, art. 57(2)(a)(i); Henckaerts and Doswald-Beck, *Customary International Humanitarian Law,* rule 16; *Tallinn Manual,* rule 53.
52. Additional Protocol I, arts. 57(2)(a)(ii), 57(3); Henckaerts and Doswald-Beck, *Customary International Humanitarian Law,* rules 17, 21; *Tallinn Manual,* rules 54, 56.
53. Additional Protocol I, art. 57(2)(b); Henckaerts and Doswald-Beck, *Customary International Humanitarian Law,* rule 19; *Tallinn Manual,* rule 57.
54. Additional Protocol I, art. 57(2)(c); Henckaerts and Doswald-Beck, *Customary International Humanitarian Law,* rule 20; *Tallinn Manual,* rule 58.
55. Additional Protocol I, arts. 57(2)(a)(iii), 57(2)(b); Henckaerts and Doswald-Beck, *Customary International Humanitarian Law,* rule 14; *Commander's Handbook,* para. 8.3.1; *Tallinn Manual,* rule 51.
56. Harvard Program on Humanitarian Policy and Conflict Research, *Manual on International Law Applicable to Air and Missile Warfare* (Cambridge, U.K.: Cambridge Univ. Press, 2013), p. 96.

Michael N. Schmitt is the Charles H. Stockton Professor of International Law and the director of the Stockton Center for the Study of International Law at the Naval War College, Newport, R.I. He is also Senior Fellow, NATO Cooperative Cyber Defence Centre of Excellence, in Tallinn, Estonia; Professor of Public International Law at Exeter University, in the United Kingdom; and a Fellow in the Harvard Law School Program on International Law and Armed Conflict.

Naval War College Review, Spring 2015, Vol. 68, No. 2