International Law Studies - Volume 87
International Law and the Changing Character of War
Raul A. "Pete" Pedrozo and Daria P. Wollschlaeger (Editors)

V

Cyber Operations and the *Jus in Bello*: Key Issues

Michael N. Schmitt*

On August 7, 2008, Georgian forces launched attacks into South Ossetia, including against Russian troops who were in the breakaway region as "peacekeepers." The *jus ad bellum* issues surrounding the conflict remain controversial.[1] However, it is incontrovertible that once Georgian and Russian forces became embroiled in hostilities against each other, an international armed conflict subject to the *jus in bello* (international humanitarian law (IHL) or the law of armed conflict) had begun.

During the conflict, numerous defacement and denial of service cyber operations were directed against Georgian entities.[2] The cyber targets included the websites of the President; Parliament; Foreign Affairs, Defence and Education ministries; domestic and foreign media; banks; and private Internet servers and blogs. For instance, defacement of the Ministry of Foreign Affairs website included the posting of a collage of photos of Adolf Hitler and Georgian President Mikheil Saakashvili. Similarly, the site of the National Bank of Georgia was replaced with one depicting twentieth-century dictators together with Saakashvili. On average, each operation lasted two hours. Although no physical damage or injuries were reported, the disruption of services proved severe. In particular, the Georgian government found itself unable to broadcast information about the

* Chair of Public International Law, Durham University, United Kingdom.

conflict and Georgian banks went off-line, as a self-imposed precautionary measure, for ten days.

The identity of the originators of the operations remains uncertain. As with those against Estonia the previous year, most of the operations were traceable to Russia but there was no conclusive evidence that the Russian government conducted the attacks or was otherwise involved therein. While certain of them were traceable to Russian government computers, the possibility that they were "pwned," that is, taken over for the purpose of mounting attacks, cannot be ruled out. Nevertheless, that a website containing potential Georgian cyber targets and malicious software, StopGeorgia.ru, came on line within hours of the commencement of hostilities aroused suspicions of governmental involvement.

Foreign governments and private sources promptly assisted the Georgians. Google provided hosting services for Georgian sites, an important contribution in light of its advanced security. The Georgian Ministry of Defence and Ministry of Foreign Affairs websites were moved to US and Estonian servers, while the Polish President made his website available for posting Georgian government information about the conflict. Despite these efforts, the attacks significantly disrupted the operation of the Georgian cyber infrastructure.

As the Georgia case illustrates, cyber operations have become embedded in modern warfare. This article examines three central IHL issues raised by cyber operations mounted during armed conflicts: the principle of distinction, direct participation by civilians in hostilities and classification of conflict. It makes no effort to explore the *jus ad bellum*, which is addressed by companion contributions to this volume of the International Law Studies. As the normative architecture governing cyber operations remains indistinct, it must be cautioned that the conclusions drawn are those of the author alone and somewhat tentative. However, attention is drawn to the ongoing efforts of a group of international experts working under the auspices of the NATO Cooperative Cyber Defence Centre of Excellence to craft a *Manual on the International Law of Cyber Warfare*.[3] Said manual, albeit soft law, will help clear much of the legal fog of cyber warfare.

Cyber Operations and the Principle of Distinction

Article 48 of Additional Protocol I requires the parties to a conflict to "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."[4] In doing so, it restates the customary law principle of distinction, which has been labeled by the International Court of Justice as one of two "cardinal" principles of IHL (the other being the prohibition of unnecessary

suffering).[5] It is incontrovertible that the principle applies to cyber operations conducted during an armed conflict.

The devil, however, is in the details. Note the term "operation" in Article 48. Its use would at first glance appear to prohibit any cyber activity directed against civilians or civilian objects. Yet operations aimed at the civilian population are not uncommon during armed conflict, the paradigmatic example being psychological operations, which are generally deemed lawful unless they cause physical harm or human suffering.

Subsequent articles resident in Additional Protocol I shed light on the foundational intent of the principle of distinction. In particular, they "operationalize" Article 48 by setting forth restrictions, prohibitions and requirements that are typically framed in terms of "attacks." Article 51.1 exemplifies this operationalization. It states that the "civilian population and individual civilians shall enjoy general protection against dangers arising from military operations," but goes on to note that "[t]o give effect to this protection, the following rules . . . shall be observed in all circumstances." The rules include the prohibitions on making the civilian population or individual civilians the "object of *attack*,"[6] conducting "indiscriminate *attacks*,"[7] and engaging in "*attacks* against the civilian population or civilians by way of reprisal."[8] Article 51 also illustrates the notion of "indiscriminate" by reference to two types of operations. The first is "an *attack* . . . which treats as a single military objective a number of clearly separated and distinct military objectives located in a city, town, village or other area containing a similar concentration of civilians or civilian objects."[9] The second is an expression of the principle of proportionality, which bars "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."[10]

Other articles take the same approach. Article 52, the property counterpart to Article 51's protection of civilians, forbids making civilian items the "object of *attack*" and limits *attacks* to military objectives.[11] Article 54 notes that it is "prohibited to *attack*, destroy, remove or render useless objects indispensible to the survival of the civilian population,"[12] whereas Article 55 prohibits "[*a*]*ttacks* against the natural environment by way of reprisals."[13] Article 56 provides that "[w]orks or installations containing dangerous forces . . . shall not be made the object of *attack*, even where these objects are military objectives, if such *attack* may cause the release of dangerous forces and consequent severe loss among the civilian population."[14] It further provides that "[o]ther military objectives located at or in the vicinity of these works or installations shall not be made the object of *attack*" if the attack may result in similar consequences.[15]

A central component of the principle of distinction is that "[i]n the conduct of military operations, constant care shall be taken to spare the civilian population, civilians and civilian objects."[16] Despite the reference to "operations," the normatively meaningful aspects of the attendant requirements are set forth in terms of attacks. Indeed, the article itself is titled "precautions in *attack*." According to the article, "those who plan or decide upon an *attack*" are required to "do everything feasible to verify that the objectives to be *attacked* are neither civilians nor civilian objects and are not subject to special protection,"[17] "take all feasible precautions in the choice of means and methods of *attack*" in order to minimize civilian harm[18] and "refrain from deciding to launch an *attack*" that may be expected to violate the rule of proportionality.[19] "*Attacks* must be canceled or suspended if it becomes apparent" that the intended target is not a military objective or if the strike would run counter to proportionality limitations,[20] and "effective advance warning shall be given of *attacks* which may affect the civilian population" should circumstances permit.[21] When considering possible targets, and choice is possible between them without forfeiting military advantage, "the objective to be selected shall be that the *attack* on which may be expected to cause the least danger to civilian lives and civilian objects."[22] None of the provisions of Article 57 may be interpreted as "authorizing any *attacks* against the civilian population, civilians or civilian objects."[23] The focus on attacks appears again in the following article, which imposes an obligation on defending parties to take "precautions against the effect of *attacks*" in order to safeguard civilians and civilian objects.[24]

The emphasis on restricting military operations by reference to attacks appears repeatedly in other chapters of Additional Protocol I. For example, medical units are not to be made the "object of *attack*," may not be used to "shield military objectives from *attack*" and must be located, whenever possible, so that "*attacks* against military objectives do not imperil their safety."[25] Prohibitions exist on making those *hors de combat* due to wounds or surrender and individuals parachuting from a disabled aircraft an object of *attack*.[26] Combatants are obligated to "distinguish themselves from the civilian population while they are engaged in an *attack* or in a military operation preparatory to *attack*,"[27] and "[i]t is prohibited . . . to *attack*, by any means whatsoever, non-defended localities."[28]

As should be apparent, the reference to operations in Article 48 must be interpreted as bearing on a particular type of operation, an attack. Operations not amounting to an attack, such as psychological operations, are generally accepted as lawful.

But what is an attack? Article 49 of Additional Protocol I, in a provision that certainly reflects customary understandings of the term, defines attacks as "acts of violence against the adversary, whether in offence or in defence."[29] The linkage between

operations and violence is further revealed in the International Committee of the Red Cross's (ICRC) *Commentary* to Article 48, which notes that "the word operation should be understood in the context of the whole section; it refers to military operations during which violence is used."[30] That Additional Protocol I and its official commentary define both operations and attacks by reference to the notion of violence further strengthens the conclusion that application of the principle of distinction generally depends on an attack having occurred and that an attack is an action during armed conflict that is violent in nature.

Since the plain text of Article 49 appears to require a violent act for qualification as an attack, by a strict textual interpretation, non-kinetic operations, i.e., operations which themselves do not comprise physical force, would be excluded. This appeared to have been the prevailing interpretation at the time the Additional Protocol was drafted. As noted in Bothe, Partsch and Solf's (all involved in drafting the Protocol) respected commentary on the provision: "The term 'acts of violence' denotes physical force. Thus, the concept of 'attacks' does not include dissemination of propaganda, embargoes, or other non-physical means of psychological or economic warfare."[31] Similarly, the ICRC *Commentary* on Article 49 suggests that "the term 'attack' means 'combat action.'"[32]

It must be remembered that although treaties are to be interpreted "in accordance with the ordinary meaning to be given to their terms," said interpretations must be made in "context and in the light of [their] object and purpose."[33] At the time Additional Protocol I was drafted, cyber operations did not exist; virtually all military "attacks" employed means that released kinetic energy, as through an explosion or the force of a bullet striking an individual. While the text of Article 49 is framed in terms of the nature of the act amounting to an attack, the drafters must have been primarily concerned with its consequences for the civilian population. Protection of the population was the Protocol's central "object and purpose" with regard to the rules of targeting. "Violence" merely constituted useful prescriptive shorthand for use in rules designed to shield the population from harmful effects. Despite being styled as act-based norms (violence), they are in fact consequence-based.

The text of Additional Protocol I's various rules developing the principle of distinction supports this conclusion. Article 51 sets out the general premise that civilians "enjoy general protection against *dangers* arising from military operations" and bars those acts or threats of violence "the primary purpose of which is to spread *terror* among the civilian population."[34] It also frames the principle of proportionality by reference to expected "incidental *loss* of civilian life, *injury* to civilians, *damage* to civilian objects," a formula repeated in Article 57.[35] During attacks, the precautions requirements of Article 57 mandate selection of methods

and means of warfare in order to minimize "incidental *loss* of civilian life, *injury* to civilians and *damage* to civilian objects,"[36] the issuance of warnings if an attack may "*affect* the civilian population,"[37] and choosing among potential targets in part based on the goal of causing "the least *danger* to civilian lives and to civilian objects."[38] With regard to aerial and naval operations, attacks must take all reasonable precautions "to avoid *losses* of civilian lives and damage to civilian objects."[39] In other articles, the environment is protected against "widespread, long-term and severe *damage*"[40] and dams, dykes and nuclear electrical generating stations are protected out of concern for "severe *losses* among the civilian population."[41]

As these examples clearly illustrate, it is not the violence of the act that constitutes the condition precedent to limiting the occurrence of an attack, but the violence of the ensuing result. In other words, the legal prohibition is on attacking, rather than targeting, protected persons and objects. This interpretation should not be considered novel, for it has always been the case that operations employing biological contagions or chemicals have been characterized as attacks, even though non-kinetic in nature, because their consequences could prove harmful, even lethal. Thus, Bothe, Partsch and Solf, despite the extract above from their classic work, correctly defined attacks in a consequence-based fashion by asserting that the term referred to "those aspects of military operations that most directly affect the safety of the civilian population and the integrity of civilian objects."[42]

Cyber operations can unquestionably generate such consequences even though they launch no physical force themselves. For instance, a cyber operation against an air traffic control system would place aircraft, whether military or civilian, at risk. Or one targeting a dam could result in the release of waters, thereby endangering persons and property downstream. In neither case would the actual act be destructive, but in both the consequences would be. Referring back to the requirement of violence, and its development in Additional Protocol I, cyber operations can therefore qualify as "attacks," even though they are not themselves "violent," because they have "violent consequences." A cyber operation, like any other operation, is an attack when resulting in death or injury of individuals, whether civilians or combatants, or damage to or destruction of objects, whether military objectives or civilian objects.

A cyber operation that is intended, but fails, to generate such results would be encompassed in the concept, in much the same way that a rifle shot that misses its target is nevertheless an attack in IHL. Similarly, one expected to cause collateral damage to civilian objects or incidental harm to civilians would qualify, even if no harm befell the military objective targeted. This latter point is somewhat unique to cyber operations since lawful kinetic operations are typically intended to cause the requisite harm to the target, with incidental harm to civilians being a by-product of

the attack, as with civilians caught within the blast radius of a bomb employed against a military facility. In a cyber operation, however, the target may not be physically harmed at all, yet the operation could nevertheless result in collateral damage or incidental injury, as in simply opening the floodgates of a dam.

By this interpretation, the operations against Georgia were not attacks and therefore not unlawful under international humanitarian law. They involved disruption and defacement, but no physical harm to objects or injury to persons.

There is an alternative approach, one suggested by Dr. Knut Dörmann of the ICRC's legal division.[43] Dörmann points to the definition of military objectives in Article 52.2 of Additional Protocol I, one generally accepted as the correct articulation of customary law, as support for his position: "military objectives are limited to those 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."[44] Noting that the definition includes "neutralization," he suggests that "[i]t is irrelevant whether an object is disabled through destruction or in any other way."[45] In doing so, he dispenses with the requirement for damage, destruction, death or injury for an action to qualify as an attack. Consequently, the prohibition on "attacking" civilians and civilian objects extends to cyber operations "targeting" them. By the Dörmann approach, many of the cyber operations conducted against Georgia would qualify as "attacks" and those targeting civilian systems would be unlawful under IHL.

The approach is not unreasonable in light of the severe non-physical harm that can be caused by cyber operations. It responds to concerns that the other approach is under-inclusive. However, Dörmann's poses the opposite risk, that of over-inclusivity. It would encompass, for instance, all denial of service attacks, including those in which mere inconvenience resulted, as in the case of blocking a television broadcast or university website. State practice provides no support for the notion that causation of inconvenience is intended to be prohibited in IHL. On the contrary, inconvenience and interference with the daily lives of civilians are a frequent result of armed conflict and psychological operations directed against the civilian population are common. Dörmann is to be commended for identifying the unsatisfactory result of limiting "attacks" to those operations causing death, injury, damage or destruction, but his proposed remedy goes too far.

It also relies on law that is not directly on point. Military objectives are those objects that may be attacked. But the preliminary question is whether an attack is being conducted or contemplated. Only when that question is answered in the affirmative does the definition of military objective come into play. The issue with regard to the definition of military objectives is *what* may be attacked, not how or with

what consequences. Moreover, the drafters envisioned "neutralization" in the context of an attack. The term was included to encompass cases involving "an attack for the purpose of denying the use of an object to the enemy without necessarily destroying it."[46] Examples include using landmines to render an area of land impassable or firing antipersonnel munitions at enemy surface-to-air missile sites to force gun crews to take cover while an air attack against other targets is under way.[47]

By the principle of distinction, civilian objects may not be attacked during armed conflict. With respect to cyber operations, one unsettled issue is whether data resident in computers comprise an "object." The implications of the answer are momentous. To the extent they do, direct operations against civilian data would constitute an unlawful attack on a civilian object. Further, any harm caused to civilian data during a cyber attack on a lawful military objective would have to be considered in the proportionality calculation and when determining the nature of the precautions required during attack.

No definitive answer to this question exists. It would appear overbroad to characterize all data as "objects." Surely a cyber operation that deletes an innocuous e-mail or temporarily disrupts a television broadcast does not amount to an unlawful attack on a civilian object. For instance, it is well-settled that an operation employing electronic warfare to disrupt civilian media is lawful. It would make no sense to distinguish between such an operation and a cyber operation that destroys data to achieve precisely the same result.

Absent an agreed-upon interpretation in the cyber context, it is perhaps best to tread lightly in characterizing data as an object. Doing so might be appropriate in two situations. First, some data are directly transferable into tangible objects. For instance, banking account data are designed to be immediately transformable into money at an automatic teller machine. To the extent the data are destroyed, so too is the tangible equivalent, the money. There are few examples of such data. Second, some data have intrinsic value. An example would be digital art. If the data are destroyed, the art is as well. Presumably, it should be protected as civilian property and in some cases as cultural property. But again, such cases are rare.

Generally, data should not be characterized as an object in itself. Rather, the determinative question is whether the consequences attendant to its destruction involve the requisite level of harm to protected physical objects or persons. If so, the cyber operation constitutes an unlawful attack.

Cyber operations also bear on certain issues regarding application of the concept of military objectives. Networking means that there is a much higher likelihood that cyber systems will be dual-use (used for both military and civilian purposes), and thereby qualify as military objectives. Similarly, military reliance on software and hardware produced for the civilian population arguably renders facilities

that produce them lawfully targetable war-supporting military objectives. And, since cyber systems are essential to the economy, certain of them may constitute war-sustaining objects, which the United States, as distinct from most other countries, characterizes as military objectives.[48]

The cyber operations against Georgia illustrate these points. In no case did the operations qualify as "attacks" under IHL, since no physical damage or injury resulted. But assuming solely for the sake of analysis that they did, some, such as those against Ministry of Defence servers, would have been lawful as directed against military objectives (although the hacktivists enjoyed no belligerent right to engage in hostilities in the first place). Others, such as those targeting the Ministry of Education and media facilities, would have violated IHL proscriptions.

Additionally, the operations against Georgia illustrate two practical aspects of cyber operations. First, it is likely that attackers will target "soft sites," that is, sites that are not well-secured. The most vulnerable are those in the civilian or non-security governmental sectors. In future conflicts, attacks on civilian cyber targets are therefore highly likely. Second, the attacks on the banking system illustrate the appeal of targeting objects that might fall into the contentious "war-sustaining" category. For instance, it would be simpler and less risky to undermine a State's oil export capacity with cyber attacks that disrupt storage and distribution than to physically destroy the facilities and the transportation links upon which export depends. This is especially so when a State is capable of effectively defending against traditional kinetic attacks.

Cyber Operations and Direct Participation in Hostilities

Those who qualify as combatants enjoy the belligerent right of engaging in hostilities; no reason exists to distinguish cyber from kinetic military operations in this regard. However, cyber operations do present some difficulty as to application of the rules regarding direct participation by civilians in hostilities. According to Article 51.3 of Additional Protocol I, "civilians shall enjoy the protection afforded by this Section [which addresses the conduct of hostilities], unless and for such time as they take a direct part in hostilities." A comparable provision exists for non-international armed conflict, and the notion is undoubtedly customary in nature.[49] The consequence of the rule is that civilians may be targeted while they directly participate in hostilities. Additionally, such direct participants do not factor into either the proportionality analysis or precautions in attack requirements. The question, then, is when do civilians who participate in cyber, as distinct from kinetic, operations become direct participants in hostilities.

Analysis begins by determining whether the individuals concerned qualify as members of the armed forces. If so, the direct participation rules do not apply since they may be targeted directly even when not participating in hostilities. In its *Interpretive Guidance on the Notion of Direct Participation in Hostilities*, the ICRC has included organized armed groups belonging to a party to the conflict in the category of armed forces.[50] Although the *Guidance* has proven controversial in other respects,[51] consensus existed among the experts convened to develop the product that it was appropriate to treat organized armed groups in the same manner as the armed forces for the purposes of targeting law.

But when do hackers and non-military groups engaging in cyber operations qualify as organized armed groups? By definition, an organized armed group must be both organized and armed. With regard to the former criterion, the most troublesome question is whether a group may be "organized virtually." In the virtual domain, groups exist whose members never have any physical contact. Such groups have many purposes—social, educational, financial, charitable and so forth. In fact, it is not rare for dispersed military personnel to organize themselves virtually, as in the case of intelligence sharing.

IHL does not develop the notion of organization to the degree necessary to come to definitive conclusions regarding virtual organization. The ICRC's *Commentary* to Additional Protocol I notes that

> [t]he term "organized" is obviously rather flexible, as there are a large number of degrees of organization. In the first place, this should be interpreted in the sense that the fighting should have a collective character, be conducted under proper control and according to rules, as opposed to individuals operating in isolation with no corresponding preparation or training.[52]

Drawing on this definition, at one end of the continuum would be those "groups" consisting of autonomous actors who are simply all targeting a State, perhaps in response to a broad call to do so from one or more sources. They do not operate under the direction of a particular individual nor does the group have any formal organizational structure. These groups cannot be deemed to be organized, and, therefore, individuals involved therein remain civilians subject to the rules of direct participation.

At the other end are those who act collectively and cooperatively. Albeit virtual, an online group may have a defined command structure and coordinate its activities—for instance, by allocating cyber targets, developing and sharing hacker tools, cooperating in identifying target vulnerabilities and conducting postattack

damage assessments. There is little justification for excluding groups of this nature from "armed forces" on the basis of organization.

A possible counterargument is that the requirement of organization is intended to allow for enforcement of IHL. However, such an assertion confuses a requirement of organization for the purposes of prisoner of war status and for qualification as a party to the conflict with the norms applicable to targeting. As noted in the *Interpretive Guidance*,

> it would contradict the logic of the principle of distinction to place irregular armed forces under the more protective legal regime afforded to the civilian population merely because they fail to . . . conduct their operations in accordance with the laws and customs of war. Therefore, even under the terms of the Hague Regulations and the Geneva Conventions, all armed actors showing a sufficient degree of military organization and belonging to a party to the conflict must be regarded as part of the armed forces of that party.[53]

The difficult case lies between these extremes, that of an informal grouping of individuals who act with shared purpose. For instance, they access a common website containing tools and vulnerable targets but do not coordinate their attacks. Whether a group of this nature meets the organization criterion should depend on such context-specific factors as the existence of a formal or informal leadership entity directing the group's activities in a general sense, identifying potential targets and maintaining an inventory of effective hacker tools. In most cases, collective action alone would not satisfy the organization criterion. However, as activities began to resemble those of a cooperative group, it is increasingly likely that States would treat said group as an "armed force," rather than a collection of civilian direct participants.

An organized group must also be "armed" to qualify as an armed force. The logical construction of "armed" is that the group carries out "attacks," as that term is understood in IHL. After all, while certain members of the armed forces, or even certain components thereof, may have no "violent" function, the concept of armed forces makes no sense in the absence of a *group* purpose of violence. This interpretation is further supported by the notion of "combatants" (who enjoy the belligerent privilege of attacking lawful targets) since they are also defined as members of the armed forces.[54] Without a group purpose of engaging in attacks, whether cyber or kinetic, the members of an organized virtual group remain civilians to whom the rules of direct participation apply. Accordingly, a group that conducts cyber operations not amounting to attacks (whether directed at military or civilian targets) is but a collection of civilians. To the extent the activities of individual members of the group constitute direct participation in hostilities, they become targetable. Of

course, the reach of the adjective "armed" depends on the interpretation adopted vis-à-vis the term "attack."

The *Interpretive Guidance* adds two qualifiers to the notion of organized armed groups, both of which have proven controversial. First, in order to be treated as the armed forces, the group must "belong to a party to the conflict," which requires "at least a *de facto* relationship" between the group and a party to the conflict.[55] The relationship can be either declared or "expressed through tacit agreement or conclusive behaviour that makes it clear for which party the group is fighting."[56] This requirement has correctly been criticized on the basis that the critical issue in targeting is not the entity for whom the potential target is fighting, but rather against whom that group is engaged in hostilities. However, assuming for the sake of analysis that the requirement applies, it would exclude those organized armed groups in an international armed conflict that might be directing cyber attacks against one of the parties for reasons other than support of the opposing party. According to the ICRC, such attacks might nevertheless amount to a separate non-international armed conflict between the group and the target State, although this approach has equally been the subject of criticism.[57] Presumably, the criterion would also exclude patriotic hacker groups unaffiliated with one of the belligerent parties, even if conducting cyber attacks for its benefit, because the group's activities would lack the "agreement" of that party and its actions would in no other way be attributable to the party under the law of State responsibility.[58]

The second qualifier found in the *Interpretive Guidance* is that only members of an organized armed group who have a "continuous combat function" qualify as members of the armed forces for targeting purposes.[59] A continuous combat function is a duty that would meet the requirements of direct participation if the individual concerned was not a group member. Whether group members engaged in cyber operations have a continuous combat function depends on application of the direct participation criteria set forth below.

This criterion is controversial, with critics arguing that it affords greater protection to members of organized armed groups, who enjoy no right to engage in hostilities, than official members of the armed forces, who do.[60] As a general matter the criterion is no more compelling in the cyber context than in that of physical operations. This is so because it derives from concern over the possible difficulty of distinguishing group members from civilians on the battlefield.[61] This prospect is especially likely during cyber operations, in which the identity of those who have launched an operation may be uncertain or where the military and civilian cyber communities share networks and transmission assets. Yet, difficult as distinction may sometimes be, IHL already contains a presumption of civilian status in the case of doubt, thereby obviating the need to impose the continuous combat

function criterion.[62] That presumption would apply equally to those engaging in cyber hostilities.

In the case of Georgia, there appear to have been no organized armed cyber groups. The attacks do not seem to have been coordinated, nor is there any compelling evidence of an overarching group structure. Further, the attacks were not "armed" in the sense that they did not cause physical damage to property or injury to individuals. Therefore, individuals engaged in conducting them would at most have qualified as direct participants in hostilities, who may have been targeted for such time as they directly participated.

The key issues regarding direct participation surround 1) the nature of direct participation and 2) the duration of the "for such time" window. The *Interpretive Guidance* suggests three cumulative constitutive elements that must be present before an act amounts to direct, as distinct from indirect, participation in hostilities. First, the act must "be likely to adversely affect the military operations or military capacity of a party to an armed conflict, or, alternatively, to inflict death, injury or destruction on persons or objects protected against direct attack" (threshold of harm). Second, "there must be a direct causal link between the act and the harm likely to result either from that act, or from a coordinated military operation of which that act constitutes an integral part" (direct causation). Finally, the act must be specifically designed to "directly cause the required threshold of harm in support of a party to the conflict and to the detriment of another" (belligerent nexus).[63] In the cyber context, any act that directly impedes a belligerent's military operations or capabilities or constitutes an attack on protected persons or objects would qualify as direct participation so long as a nexus existed between the act and the armed conflict. Examples would include cyber military intelligence gathering, disrupting enemy cyber networks and manipulating data in the enemy's military systems.

These requirements are generally deemed acceptable, although disagreement does exist at their margins.[64] For instance, it has been suggested that the "threshold of harm" criterion be extended to include operations designed to enhance one's own capabilities. An example would be developing cyber defenses or identifying cyber vulnerabilities in military cyber systems. The second element, causality, is equally necessary, but many critics of the *Guidance* took issue with its example of assembling improvised explosive devices as *in*direct causation. Similar objections would be raised if the analogous case of developing software specific to a particular cyber operation or enemy system were characterized as indirect, vice direct, causation.

The major issue presented by the *Interpretive Guidance* centered on the meaning of the phrase "for such time," referring to the period during which a direct participant is susceptible to lawful attack. The phrase has long been the subject of

controversy, with critics alleging that it created a "revolving door."[65] In other words, while a direct participant is deploying to and from an operation, he may be attacked. However, once he successfully returns home he regains the full immunity from attack that civilians enjoy, at least until such time as he deploys again to directly participate in hostilities. Although the ICRC has argued that this dynamic is not a malfunction of IHL,[66] critics point out that it creates an imbalance between the direct participant and the member of the regular armed forces, since the latter is open to attack at any time based solely on his status. In the view of the critics, these individuals should be deemed to be directly participating for such time as they regularly engage in acts of hostilities; there should be no periods of immunity from attack between the qualifying acts.

Cyber operations bring this issue into even greater focus. First, there may be no "deployment" at all since only a computer, and not proximity to the target, is required to mount the operations. The restrictive interpretation of the for such time criterion would suggest that the direct participant can only be attacked while actually launching the operation. This is problematic in that many cyber operations last mere minutes, perhaps only seconds. Such a requirement would effectively extinguish the right to strike at direct participants. Moreover, the effect of a cyber operation may be long-delayed, as in the case of a surreptitiously emplaced logic bomb. Would the target of such an operation only be entitled to attack the direct participant while the logic bomb is being emplaced? The problem is that the very point of these operations is to avoid detection. Therefore, from a practical perspective, there would appear to be no window of opportunity for the victim of an attack to respond. In the cyber conflict environment, therefore, the only reasonable interpretation of "for such time" is that it encompasses the entire period during which the direct cyber participant is engaging in repeated cyber operations.

Cyber Operations as Armed Conflict

Cyber operations are a particularly attractive means of targeting an opponent, for the technology necessary to conduct them is cheap and accessible. In particular, they represent an effective method for a weaker State to strike at a technologically more advanced, and therefore more vulnerable, adversary. But do cyber operations comprise "armed conflict," as that term is used in IHL? This is "the" threshold question, for IHL does not apply in the absence of armed conflict.

When cyber operations are merely one aspect of an ongoing armed conflict, they must comport with the IHL applicable to that category of armed conflict. For instance, because the conflict between Russia and Georgia was international in character, the ensuing cyber operations were subject to the law of international

armed conflict. Any operations qualifying as attacks under that body of law would, if directed at civilians, constitute violations of IHL and war crimes.

The difficult case involves cyber operations that take place in the absence of kinetic hostilities. Can they constitute an armed conflict, and, if so, what type? Unfortunately, IHL treaty law does not define the phrase "armed conflict" per se. Rather, it only expands on the two subcategories of armed conflict, international and non-international armed conflict.

As to international armed conflict, Common Article 2 to the four 1949 Geneva Conventions is traditionally viewed as the proper articulation of the scope of international armed conflict: "all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties."[67] In explaining the article's reach, the ICRC's commentary thereon notes that

> [a]ny difference arising between two States and leading to the intervention of members of the armed forces is an armed conflict within the meaning of Article 2, even if one of the Parties denies the existence of a state of war. It makes no difference how long the conflict lasts, how much slaughter takes place, or how numerous are the participating forces.[68]

The International Criminal Tribunal for the former Yugoslavia (ICTY) has likewise opined that "an armed conflict exists whenever there is resort to force between States."[69]

This threshold must not be confused with that of an "armed attack," the condition precedent for acts in self-defense under the *jus ad bellum*.[70] The International Court of Justice (ICJ) described armed attacks in the *Nicaragua* case as involving certain "scale and effects," which excluded "a mere frontier incident."[71] Under IHL, however, an "international armed conflict" commences whenever an armed exchange between States occurs, regardless of the scale and effects of the hostilities.

Applied to cyber operations, it is clear that any operation by or attributable to a State that results in damage to or destruction of objects or injury to or death of individuals of another State would commence an international armed conflict. This is because they constitute attacks under IHL. More problematic from a classification of conflict point of view are cyber operations causing no damage or injury, but instead merely inconvenience, disruption, disorder or irritation. The results of such operations might nevertheless be severe, as in significant interference with the economy, transportation system or other critical infrastructure.

One possibility is to limit international armed conflict to situations in which "attacks" have occurred. Since attacks are "acts of violence,"[72] doing so would comport with the fact that IHL only applies once a conflict is "armed," as well as

with the ICRC *Commentary*'s reference to intervention by the armed forces. Although uncontested occupation and detention also constitute armed conflict while harming neither persons nor objects,[73] they both rely on the possibility of enforcement through the use of force. By this interpretation, non-destructive computer network exploitation, espionage, denial of service attacks and other invasive but non-destructive cyber operations would not initiate an armed conflict. The dilemma is that in practice States targeted by non-destructive, yet otherwise severe, attacks might treat the operations as armed conflict that justified, for instance, kinetic attacks on their enemies' military objectives and combatants.

A second possibility for classification of events involving cyber operations is one based on the more liberal Dörmann definition of attacks, which includes operations targeting civilians and civilian objects irrespective of whether they were physically damaged or injured. Because directing operations against protected persons or objects constitutes an attack by this interpretation, an international armed conflict would commence once a State or those under its control launched them. However, the position is arguably over-inclusive in that by focusing on the target of an operation, it has no means to distinguish non-destructive "attacks" from non-destructive military operations that fail to qualify as attacks, such as lawful psychological operations directed at the civilian population.

Both approaches have merit, the former in its fidelity to received understandings of IHL, the latter in that it would respond to concerns that the traditional understanding is under-inclusive since it admits of highly disruptive cyber operations to which IHL would not apply. As it stands, though, the former represents *lex lata*, the latter *lex ferenda*.

A major complication is the current prevalence of cyber operations by non-State actors, as in the case of the Georgia-Russia conflict. Such actions will typically take on the character of the kinetic conflict under way and be dealt with by the relevant rules of targeting, especially those governing direct participation by civilians in hostilities. However, a classification dilemma arises when cyber operations are conducted by non-State actors in the absence of related kinetic operations.

The issue of attribution of a non-State actor's acts to a State is complex. The traditional test was set forth by the International Court of Justice in the *Nicaragua* case. There, the Court articulated the "effective control" test. It held that

> United States participation, even if preponderant or decisive, in the financing, organizing, training, supplying and equipping of the *contras* [Nicaraguan guerrillas], the selection of its military or paramilitary targets, and the planning of the whole of its operation, is still insufficient . . . for the purpose of attributing to the United States the acts committed by the *contras* . . . . All the forms of United States participation mentioned above, and even the general control by the respondent State over a force with a

> high degree of dependency on it, would not in themselves mean, without further evidence, that the United States directed or enforced the perpetration of the acts contrary to human rights and humanitarian law alleged by the applicant State. Such acts could well be committed by members of the *contras* without the control of the United States. For this conduct to give rise to legal responsibility of the United States, it would in principle have to be proved that that State had effective control of the military or paramilitary operations in the course of which the alleged violations were committed.[74]

This test was reaffirmed by the Court in the *Congo* and *Genocide* cases.[75] However, although the test is often cited with regard to conflict classification, the actual issue in *Nicaragua* was State responsibility for alleged actions of the contras.

By contrast, the Appeals Chamber of the ICTY dealt with the issue of conflict classification directly in *Tadic*. Explicitly rejecting the effective control test, it held that the authority of the Federal Republic of Yugoslavia over the Bosnian Serb armed groups "required by international law for considering the armed conflict to be international was *overall control* going beyond the mere financing and equipping of such forces and involving also participation in the planning and supervision of military operations."[76]

The debate over the applicable standard remains unsettled. Nevertheless, there is no question but that a State may be responsible for the actions of non-State actors and that such responsibility may result in the existence of an international armed conflict. Therefore, when a State directs particular cyber *attacks* by non-State actors (*Nicaragua*) or (perhaps) participates in general planning and supervision (*Tadic*) of such attacks, an international armed conflict comes into being between the target State and the State exercising control over the attackers. By contrast, no armed conflict commences when a State simply tolerates or sympathizes with cyber attacks emanating from its territory, although the State may be in breach of its international legal obligation to "police" its territory to ensure it is not used to the detriment of other States.[77]

Determining whether a cyber operation conducted in the absence of kinetic operations comprises *non*-international armed conflict is more challenging still. Common Article 3 to the Geneva Conventions styles non-international armed conflicts as those that are "not of an international character."[78] Specifically, non-international armed conflict is that which occurs between a State and organized armed groups or between such groups. Two criteria exist—organization and intensity.

Organization has been dealt with earlier with regard to qualification as an organized armed group vis-à-vis the rules of direct participation. The criterion would rule out any attacks mounted by either individual "hackers" or groups of hackers who lack the necessary degree of organization as non-international armed conflict.

Such attacks would therefore be governed by domestic criminal law and human rights norms, not IHL. As to "virtually" organized groups, the analysis set forth above would apply. To the extent the group in question qualified as an organized armed group, the first criterion for non-international armed conflict would be met.

Non-international armed conflicts must also evidence a certain degree of intensity. Unlike international armed conflict, non-international armed conflict requires more than mere limited hostilities. In particular, "internal disturbances and tensions, such as riots, isolated and sporadic acts of violence and other acts of a similar nature" are excluded from the ambit of such conflict.[79] According to the ICTY in the *Tadic* case, non-international armed conflicts involve "protracted armed violence between governmental authorities and organized armed groups or between such groups within a State,"[80] a definition embraced by the International Criminal Tribunal for Rwanda and present in the Statute of the International Criminal Court.[81]

This criterion would keep most cyber attacks (in the absence of kinetic operations) from qualifying as non-international armed conflict. In particular, the protracted requirement would rule out individual or sporadic attacks irrespective of their destructiveness. Moreover, non-destructive cyber operations would, as discussed, be unlikely to even qualify as armed conflict at all. Given the intensity criterion, they certainly would not with regard to non-international armed conflict. The result is that cyber attacks conducted against a State must be quite intense before constituting a non-international armed conflict.

It should finally be noted that, although Additional Protocol II also addresses non-international armed conflict for States party thereto, it only applies when an organized armed group involved in the conflict "exercise[s] such control over a part of" a State's territory that it can "carry out sustained and concerted military operations."[82] Obviously, a group conducting solely cyber operations against a State would fail to meet this requirement.

Concluding Thoughts

This article has but scratched the surface of the many problematic issues surrounding application of IHL to cyber operations. Three were singled out for attention and of these none was fully resolved. The dilemma is that IHL was crafted during a period in which the cyber operations were but science fiction. However, today no modern military enters the battlespace without at least some reliance on computers and computer networks. For the modern military, cyber capabilities represent both force multipliers and vulnerabilities. And as demonstrated in the case of the Georgia-Russia conflict, civilian cyber assets are an especially attractive target set,

not only for militaries, but also for individuals or groups intent on involvement in the conflict in question.

IHL must respond to the challenges posed by this new technology. The past decade has witnessed numerous efforts, in particular by the Naval War College, to identify challenges posed by cyber warfare to the extant norms of IHL, and to international law more generally.[83] Today, practitioners and scholars are increasingly sensitive to the challenges, such as those set forth in this article, of applying IHL to cyber operations.[84] Hopefully, the next decade will witness their resolution by the legal, operational and policy communities.

Notes

1. *See, e.g.*, EUROPEAN UNION, INDEPENDENT INTERNATIONAL FACT-FINDING MISSION ON THE CONFLICT IN GEORGIA, REPORT (2009).
2. On cyber operations during the conflict, see ENEKEN TIKK, KADRI KASKA & LIIS VIHUL, INTERNATIONAL CYBER INCIDENTS: LEGAL CONSIDERATIONS 63–90 (2010).
3. Under direction of the author.
4. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts art. 48, June 8, 1977, 1125 U.N.T.S. 3 [hereinafter AP I].
5. Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, ¶ 78 (July 8).
6. AP I, *supra* note 4, art. 51.2.
7. *Id.*, art. 51.4.
8. *Id.*, art. 51.7.
9. *Id.*, art. 51.5(a).
10. *Id.*, art. 51.5(b).
11. *Id.*, arts. 52.1 & 52.2.
12. *Id.*, art. 54.2.
13. *Id.*, art. 55.2.
14. *Id.*, art. 56.1. The protection extends, in specified circumstances, to "installations erected for the sole purpose of defending the protected works or installations from *attacks*." *Id.*, art. 56.5.
15. *Id.*, art. 56.1. Note that Article 56 sets forth certain circumstances in which the special protection ceases. *Id.*, art. 56.2.
16. *Id.*, art. 57.1.
17. *Id.*, art. 57.2(a)(i).
18. *Id.*, art. 57.2(a)(ii).
19. *Id.*, art. 57.2(a)(iii).
20. *Id.*, art. 57.2(b).
21. *Id.*, art. 57.2(c).
22. *Id.*, art. 57.3.
23. *Id.*, art. 57.5.
24. *Id.*, art. 58.
25. *Id.*, art. 12. By reference, arts. 21 & 23.
26. *Id.*, arts. 41.1 & 42.1.

27. *Id.*, art. 44.3.
28. *Id.*, art. 59.1.
29. *Id.*, art. 49. For an example of the definition in a non–AP I treatment of the subject, see HARVARD PROGRAM ON HUMANITARIAN POLICY AND CONFLICT RESEARCH, COMMENTARY ON THE HPCR MANUAL ON INTERNATIONAL LAW APPLICABLE TO AIR AND MISSILE WARFARE rule 1(e) (2009), *available at* http://ihlresearch.org/amw/Commentary%20on%20the%20HPCR%20Manual.pdf [hereinafter AMW Manual].
30. COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949, ¶ 1875 (Yves Sandoz, Christophe Swinarski & Bruno Zimmermann, eds., 1987) [hereinafter AP COMMENTARY].
31. MICHAEL BOTHE ET AL., NEW RULES FOR VICTIMS OF ARMED CONFLICTS 289 (1982).
32. AP COMMENTARY, *supra* note 30, ¶ 1880.
33. Vienna Convention on the Law of Treaties art. 31(1), May 23, 1969, 1155 U.N.T.S. 331.
34. AP I, *supra* note 4, arts. 51.1 & 51.2.
35. *Id.*, arts. 51.5(b), 57.2(a)(iii) & 57.2(b).
36. *Id.*, art. 57.2(a)(ii).
37. *Id.*, art. 57.2(c).
38. *Id.*, art. 57.3.
39. *Id.*, art. 57.4.
40. *Id.*, arts. 35.3 and 55.1.
41. *Id.*, art. 56.1.
42. BOTHE ET AL., *supra* note 31, at 288.
43. Knut Dörmann, *Applicability of the Additional Protocols to Computer Network Attacks* (Paper delivered at the International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law, Stockholm, Nov. 17–19, 2004), http://www.icrc.org/web/eng/siteeng0.nsf/htmlall/68lg92?opendocument.
44. AP I, *supra* note 4, art. 52.2.
45. Dörmann, *supra* note 43.
46. BOTHE ET AL., *supra* note 31, at 325.
47. *Id.*
48. US Navy, Marine Corps & Coast Guard, The Commander's Handbook on the Law of Naval Operations, NWP 1-14M/MCWP 5-12.1/COMDTPUB P5800.7A ¶ 8.2 (2007). Examples of war-sustaining objects include "economic objects of the enemy that indirectly but effectively support and sustain the enemy's war-fighting capability." *Id.*, ¶ 8.2.5.
49. AP I, *supra* note 4, art. 51.3; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts art. 13.3, June 8, 1977, 1125 U.N.T.S. 609 [hereinafter AP II]. On the customary nature of the norm, see I CUSTOMARY INTERNATIONAL HUMANITARIAN LAW rule 6 (Jean-Marie Henckaerts & Louise Doswald-Beck eds., 2005); AMW Manual, *supra* note 29, rules 28–29; MICHAEL N. SCHMITT, CHARLES H.B. GARRAWAY & YORAM DINSTEIN, THE MANUAL ON THE LAW OF NON-INTERNATIONAL ARMED CONFLICT WITH COMMENTARY rule 1.2.2 (2006).
50. NILS MELZER, INTERNATIONAL COMMITTEE OF THE RED CROSS, INTERPRETIVE GUIDANCE ON THE NOTION OF DIRECT PARTICIPATION IN HOSTILITIES UNDER INTERNATIONAL HUMANITARIAN LAW 16 (2009) [hereinafter IG].
51. *See, e.g.*, Bill Boothby, *"And for Such Time As": The Time Dimension to Direct Participation in Hostilities*, 42 NEW YORK UNIVERSITY JOURNAL OF INTERNATIONAL LAW AND POLITICS 741 (2010); W. Hays Parks, *Part IX of the ICRC "Direct Participation in Hostilities" Study: No Mandate, No Expertise, and Legally Incorrect*, *supra* at 769 (2010); Michael N. Schmitt, *Deconstructing*

Direct Participation in Hostilities: The Constitutive Elements, *supra* at 697 (2010); Kenneth Watkin, *Opportunity Lost: Organized Armed Groups and the ICRC "Direct Participation in Hostilities" Interpretive Guidance*, *supra* at 641 (2010); Michael N. Schmitt, *The Interpretive Guidance on the Notion of Direct Participation in Hostilities: A Critical Analysis*, 1 HARVARD NATIONAL SECURITY JOURNAL 5 (2010).

52. AP COMMENTARY, *supra* note 30, ¶ 1672.

53. IG, *supra* note 50, at 22.

54. AP I, *supra* note 4, art. 43.2.

55. IG, *supra* note 50, at 23.

56. *Id.*

57. *Id.* at 24.

58. *Id.* at 23.

59. *Id.* at 26, 33.

60. Since a member of an organized armed group without a combat function would not be targetable, while a member of the armed forces without such a function would be subject to attack.

61. IG, *supra* note 50, at 33.

62. AP I, *supra* note 4, art. 50.1.

63. IG, *supra* note 50, at 16–17.

64. *See generally* Schmitt, *Deconstructing*, *supra* note 51.

65. *See, e.g.*, W. Hays Parks, *Air War and the Law of War*, 32 AIR FORCE LAW REVIEW 1, 118 (1990).

66. IG, *supra* note 50, at 70.

67. Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field art. 2, Aug. 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31; Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea art. 2, Aug. 12, 1949, 6 U.S.T. 3217, 75 U.N.T.S. 85; Convention Relative to the Treatment of Prisoners of War art. 2, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135; Convention Relative to the Protection of Civilian Persons in Time of War art. 2, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287 [hereinafter GC I–IV].

68. COMMENTARY TO GENEVA CONVENTION III RELATIVE TO THE TREATMENT OF PRISONERS OF WAR 23 (Jean Pictet ed., 1960) [hereinafter GC-III COMMENTARY].

69. Prosecutor v. Tadic, Case No. IT-94-1-A, Appeals Chamber Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, ¶ 70 (Int'l Crim. Trib. for the Former Yugoslavia Oct. 2, 1995). *See also* Prosecutor v. Kunarac, Case No. IT-96-23/1-A, Judgment, ¶¶ 56–57 (Int'l Crim. Trib. for the Former Yugoslavia June 12, 2002); Prosecutor v. Milosevic, Case No. IT-02-54-T, Decision on Motion for Judgment of Acquittal, ¶¶ 15–17 (Int'l Crim. Trib. for the Former Yugoslavia June 16, 2004).

70. U.N. Charter art. 51.

71. Military and Paramilitary Activities in and against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, ¶ 195 (June 27). This standard has been subject to careful parsing (*see, e.g.*, Oil Platforms (Iran v. U.S.), 2003 I.C.J. 161, ¶ 72 (Nov. 6)), and criticized by commentators (*see, e.g.*, YORAM DINSTEIN, WAR, AGGRESSION AND SELF-DEFENCE 194–96 (4th. ed. 2005); William Taft, *Self-defense and the Oil Platforms Decision*, 29 YALE JOURNAL OF INTERNATIONAL LAW 295, 300 (2004)).

72. AP I, *supra* note 4, art. 49; AMW Manual, *supra* note 29, rule 1(e).

73. Article 2 of the Geneva Conventions extends to cases of "partial or total occupation . . . even if said occupation meets with no armed resistance." GC I–IV, *supra* note 67, art. 2(1). Similarly,

when the forces of a State detain individuals protected by IHL (especially members of the opponent's armed forces), an armed conflict exists. GC-III COMMENTARY, *supra* note 68, at 23.

74. Military and Paramilitary Activities, *supra* note 71, ¶ 115 (June 27). See also discussion at paragraph 109.

75. Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), 2005 I.C.J. 116, ¶ 160 (Dec. 19); Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Mont.), 2007 I.C.J. 91, ¶¶ 391–92 (Feb. 26).

76. Prosecutor v. Tadic, Case No. IT-94-1-A, Appeals Chamber Judgment, ¶ 145 (Int'l Crim. Trib. for the Former Yugoslavia July 15, 1999) (emphasis added).

77. The ICJ affirmed this principle in *Corfu Channel*, its first case. The Court held that every State has an "obligation to not allow knowingly its territory to be used for acts contrary to the rights of other States." Corfu Channel (U.K. v. Alb.), 1949 I.C.J. 4, 22 (Apr. 9).

78. GC I–IV, *supra* note 67, "Common" art. 3.

79. AP II, *supra* note 49, art. 1.2. The limitation is generally deemed to reflect the standard applicable to Common Article 3 and in customary international law. *See, e.g.*, Statute of the International Criminal Court art. 8(2)(f), July 17, 1998, 2187 U.N.T.S. 90 [hereinafter Rome Statute].

80. Tadic, *supra* note 69, ¶ 70.

81. Prosecutor v. Akeyesu, Case No. ICTR-96-4-T, Judgment, ¶ 619 (Sept. 2, 1998); Rome Statute, *supra* note 79, art. 8(2)(f).

82. AP II, *supra* note 49, art. 1.1. It must also be able to implement the provisions of the Protocol.

83. The first conference on the subject was hosted by the Naval War College in June 1999. The proceedings were published as COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW (Michael N. Schmitt & Brian T. O'Donnell eds., 2002) (Vol. 76, US Naval War College International Law Studies).

84. *See, e.g.*, COMMITTEE ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POLICY, NATIONAL RESEARCH COUNCIL, PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POLICY 151–78 (2010).