Applying International Humanitarian Law to Cyber Warfare

Eitan Diamond

This article seeks to shed some light on the application of international humanitarian law (IHL), otherwise known as the law of armed conflict or the laws of war, to the phenomenon of cyber warfare.

For the purposes of this essay, the term "cyber warfare" describes cyber operations conducted in or amounting to an armed conflict. Such cyber operations, which involve the development and dispatch of computer code from one or more computers to target computers, can be aimed at either infiltrating a computer system to collect, export, destroy, change, or encrypt data, or to trigger, alter, or otherwise manipulate processes controlled by the infiltrated system.[1]

Even while directed at computers rather than people, such operations could potentially cause a tremendous degree of human suffering. In times of armed conflict in particular, there are grounds for concern that cyber operations will be used to undermine the functioning of infrastructure needed for the provision of resources and services of crucial importance to the civilian population. Critical installations such as power plants, nuclear plants, dams, water treatment and distribution systems, oil refineries, gas and oil pipelines, banking systems, hospital systems, railroads, and air traffic control all rely heavily on computer systems susceptible to infiltration and manipulation via cyber operations. The risk that civilians and civilian objects will come to harm as a result of cyber warfare is heightened by the high level of interconnectivity and interdependence between civilian and

---

Eitan Diamond is a legal advisor in the International Committee of the Red Cross (ICRC) Delegation in Israel and the Occupied Territories. The views expressed in this article are those of the author and do not necessarily reflect those of the ICRC.

military computer infrastructure, which can make it extremely difficult to differentiate between them.[2] Thus, an attack on a military computer system is very likely to damage civilian computer systems as well. These in turn may be vital for some civilian services such as water or electricity supply, or the transfer of assets.

In view of these potential risks, it is clear why there is a humanitarian need for the law to regulate and constrain cyber warfare. At the same time, despite some notable attempts to create greater clarity,[3] many questions remain open about how existing legal frameworks might be applied to this relatively new phenomenon about which much is still unknown.

This article will not provide comprehensive answers to all such questions. For one thing, it will not attempt to address questions relating to all of the bodies of law that may be applicable to cyber warfare, and will instead address only questions relating to the application of IHL. Furthermore, even while the analysis will be confined to the challenges that cyber warfare poses for IHL, a number of significant questions will remain unanswered. Rather than attempting to provide answers, which – for reasons that will be explained – is not currently possible, the article will endeavour to map out the most pressing questions and indicate what challenges must be overcome if IHL is to attain its goal of preserving human dignity and preventing unnecessary human suffering even in the wake of this novel form of warfare.

As a backdrop for the analysis, the article will first highlight the general difficulty of applying the long-established rules of IHL to hostilities involving new methods and means of warfare, a difficulty that is particularly evident in the case of cyber operations. The lack of transparency and the overall dearth of information surrounding cyber operations create further obstacles for the application of IHL. The article will then discuss problems that may arise in determining whether cyber operations have occurred within a situation of armed conflict. This is significant, because IHL only applies in an armed conflict. Once it has been determined that a situation of armed conflict exists, it is necessary to ascertain how the applicable rules of IHL are to be interpreted and applied to cyber operations. In this regard the article will consider in what circumstance cyber operations trigger the IHL rules on the conduct of hostilities, and how the principle of distinction, the principle of proportionality, and the duty to take precautions are to be implemented in the case of cyber warfare.

Adapting Old Laws to New Cyber Technologies

Legal norms are by nature general and forward looking. They establish rules of conduct that are to be applied in diverse and as yet unknown future situations. To accomplish this task the law must paint with a broad brush. It cannot possibly spell out specific rules for all sets of circumstances that may arise, and so instead, it applies rules across different general categories that it defines and distinguishes from one another. The transition from such general norms to concrete and ever-changing realities is not seamless and requires a regular process of adaptation.

In the realm of domestic law, this task is achieved in large part through acts of interpretation by national courts, which are constantly called upon to apply the law to specific incidents, and through legislative amendments, which can be enacted in response to changing sensibilities and new realities. In the realm of international law, the process of adaptation is far more cumbersome. For one thing, an international norm cannot be enacted by the legislature of a single state, but instead emerges only when multiple states express their consent to be bound by it.[4] Since states are driven by different and often contrasting interests and incentives, such consensus is difficult to achieve. Adapting international law through judicial interpretation is also complicated since relevant jurisprudence occurs haphazardly in instances from diverse jurisdictions, and it is therefore not always possible to extract a coherent and authoritative interpretation.

The process of adapting law to change is particularly challenging when it comes to IHL, as it regulates situations of armed conflict that naturally evoke contrasting positions between states. Indeed, states so rarely reach the necessary consensus on such matters that the key provisions of IHL are still found in treaties that are many decades old and in some cases date back more than a century.[5] But while the law evolves slowly, new means and methods of warfare develop continually and the battlefield is rapidly changing. Bridging the temporal and contextual gap between the moment of the law's formation and the moment of its application is thus becoming an ever growing and more urgent challenge.

Fortunately, and precisely because of the types of challenges just described, the IHL rules governing the conduct of hostilities, including such core principles as the principles of distinction and proportionality and the duty to employ precautionary measures, are broadly and flexibly defined and can therefore accommodate even far-reaching developments. These general

rules regulate all means and methods of warfare, including the use of all weapons, and are thus applicable to cyber warfare as well. However, in the case of cyber warfare, their capacity to accommodate change is tested to the extreme. The IHL framework governing the conduct of hostilities was designed to apply to methods and means of warfare involving the use of kinetic force in the physical world, and therefore makes an awkward fit for hostilities that consist of the manipulation of data in cyberspace. In fact, as we shall see, even some of the basic assumptions underlying IHL come into question, and categories and distinctions fundamental to IHL – such as "armed conflict," "attack," "civilian object," and "military objective" – are not easily retained when applied to cyber warfare.

Applying IHL to Technologies and Operations Veiled in Secrecy

The difficulty of adapting IHL to cyber warfare is compounded by the veil of secrecy enveloping cyber security operations. Law, after all, must be applied to facts. When the facts are not well known it is not possible to have a clear legal reading. More precisely, key information needed in order to make an informed evaluation of cyber operations compatibility with IHL is often lacking, including details about (a) the technology available, (b) the attacks conducted, (c) the identity of the parties conducting the attacks, and (d) the policies, guidelines, and rules that states apply in relation to cyber warfare, along with their reading of the applicable rules of IHL.

Information about the technological capabilities that exist or are under development is necessary to evaluate whether the methods and means of warfare facilitated by these technologies meet the requirements of IHL. In practice, however, states are rarely forthcoming about the offensive and defensive capabilities they already have or are developing for cyber warfare, and little is known about the types of cyber operations or cyber weapons available to other actors. States are equally unwilling to divulge details about cyber operations they have undertaken against others or about those that have been directed against them. Thus, it is hardly possible to review the ways in which belligerent parties engaged in armed conflict actually employ such operations in the conduct of hostilities. In other words, it is not properly known what attacks have been conducted using cyber technology, let alone what such attacks might have entailed. Likewise, since cyber operations are typically anonymous, it will in most cases be difficult, if not impossible, to identify the party responsible for the operation. Thus, it will often not be

possible to determine if the operation was conducted by a party to an armed conflict and, consequentially, if IHL even applies.

The secrecy surrounding state capabilities and practices in the field of cyber warfare also extends to the rules and regulations that states apply in relation to cyber operations. In light of this, and since states have for the most part refrained from disclosing directly what they consider to be the proper application of IHL to cyber warfare,[6] it is very difficult to discern their legal position on the matter.

Given that states are the authors of international law, the lack of transparency regarding both their practice and legal position in relation to cyber warfare undermines efforts to attain legal clarity in this area. Commentators are left to speculate what such warfare does or could entail, and to propose, without the benefit of supporting state practice or legal opinion, how it ought to be conducted.

Does Cyber Warfare Fall within the Confines of Armed Conflict?

Since IHL applies only in the context of armed conflict, what must first be ascertained when considering if a given cyber operation is subject to IHL is whether the operation in question was conducted in the context of and with a nexus to an armed conflict.

Seemingly the applicability of IHL would be relatively easy to establish in relation to cyber operations occurring against the backdrop of an existing armed conflict, but even then it is by no means self-evident and complicating factors are likely to come into play. In particular, it will not necessarily be possible to determine that the operations are in fact related to the armed conflict. Indeed, since the nature of cyber operations is such that the identity of the actor carrying them out may very well be unknown, there may be no grounds to assert that the operations were conducted by or on behalf of a party to an armed conflict. For such time as the connection to armed conflict remains in doubt, so too would the applicability of IHL.

Still more problematic would be cases in which cyber warfare does not occur alongside other forms of hostilities. In such situations the additional question arises whether cyber operations can themselves amount to armed conflict. In addressing this question, it is necessary to distinguish between the two different types of armed conflict that are regulated by IHL, i.e., international armed conflicts, occurring between states, and non-international

armed conflicts, in which at least one of the belligerent parties is a non-state actor.

An international armed conflict occurs whenever there is a resort to armed force between states.[7] Accordingly, cyber warfare would constitute an international armed conflict only if (a) the cyber operations involved are attributable to a state, and (b) they amounted to a resort to armed force against another state.

Again, the question of attribution is difficult in the context of cyber warfare. It has been suggested that this difficulty might be mitigated to some extent by adopting appropriate legal presumptions.[8] Thus, for example, a state would be presumed responsible for any cyber operation originating from its governmental infrastructure unless it could prove otherwise. However, there is no basis in existing international law for such a presumption. Moreover, given the ease with which different guises can be assumed in cyberspace and the difficulty of shielding computer infrastructure from manipulation, the presumption could be extremely artificial and might be said to place an unreasonable burden on states.[9]

Besides the factual difficulties in determining the source of a cyber operation, the attribution of a cyber operation to a state may also be complicated by questions concerning the scope of states' legal responsibility for cyber operations that were not conducted directly by them, but rather by private persons or groups. The potential attribution of acts of private agents to the state is not unique to cyber warfare. The general rule under international law in this regard is that the conduct of a person or group of persons is attributable to a state "if the person or group of persons is in fact acting on the instructions of or under the direction or control of that State in carrying out the conduct."[10] This has been interpreted variously to conclude that (a) the actions of private agents are attributable to a state only with respect to specific operations over which the state had effective control;[11] or that (b) it is sufficient for a state to have "overall control" over a group for the latter's actions to be attributed to it.[12] Either way, applying these tests to cyber warfare, where the relevant facts may be more difficult to establish, is likely to prove challenging and may be further complicated by the need to interpret the notion of "control" in relation to actions and actors operating in cyberspace.

Assessing whether cyber operations satisfy the second criterion for an international armed conflict, namely that they amount to the resort to armed

force against a state, presents another significant hurdle. The traditional concept of armed force is of hostilities involving means and methods of warfare entailing the use of kinetic force. Applying this concept to the act of developing and sending computer code is not a straightforward exercise. When can such acts be considered to amount to "armed force"? There is broad agreement among analysts that computer network attacks that lead to physical destruction parallel to the destruction produced by attacks employing kinetic force would amount to an armed attack.[13] However, cyber operations are capable of effecting other forms of harm. Rather than physically destroying a target system, they could be used to hamper its functioning. The harm thus caused would take direct effect not in the physical world but in cyberspace. Indeed, this type of cyber network attack might very well go undetected, while the indirect effects of such an attack – which could, for example, disrupt the supply of vital resources (such as water, electricity, or oil) or the provision of essential services – could be most harmful indeed. If IHL is to be interpreted in accordance with its underlying humanitarian purpose,[14] then presumably cyber operations producing such grave humanitarian consequences ought to be considered as within the ambit of armed force and thus subject to the protective provisions of IHL.

On the other hand, the classification of a situation as an armed conflict brings into play not only the restrictive provisions of IHL, but also its permissive aspects. IHL allows for – or at least does not prohibit – the intentional use of lethal force against certain categories of people (such as enemy combatants[15] and civilians directly participating in hostilities) and the intentional destruction of certain categories of property (military objectives), and also tolerates a degree of incidental harm to other categories of persons and objects ("collateral damage") that would all be prohibited by the law applicable outside of armed conflict. Those seeking to restrict the scope of force legally permissible might therefore have good reason to favor a more restrictive approach in interpreting when cyber warfare amounts to resort to armed force. In any event, in the absence of state practice or clarification of states' legal positions (*opinio juris*), it remains an open question whether, and if so, under what conditions, cyber warfare can be said to constitute resort to armed force even when not producing direct physical destruction.

A non-international armed conflict exists whenever there is protracted armed violence, meaning armed violence of a certain degree of intensity, between governmental authorities and organized armed groups or between

such groups within a state.[16] In other words, in order for a situation to be classified as a non-international armed conflict it must entail armed violence involving at least one non-state actor where (a) the parties involved satisfy a minimum level of organization and (b) the armed violence reaches a minimum level of intensity. However, applying these criteria to cyber warfare raises a number of difficulties.

For one thing, the nature of virtually organized groups of the type active in cyberspace – such as groups of hackers cooperating in joint cyber operations – is such that they will rarely, if ever, satisfy the requirement of a minimum level of organization as thus far understood. Under this requirement, the group should have a command structure with a level of hierarchy and discipline sufficient to enable it both to carry out sustained acts of warfare and to implement the basic rules of IHL.[17] It is difficult to see how groups whose members are linked only by virtual communication and who may never have met in person or even know each other's identity would fit this mold.[18] For this reason it seems that while the activities of such groups could certainly constitute criminal behavior, it would be incorrect to say that they also amount to an engagement in armed conflict. However, this conclusion might be met with some unease when it is observed that the cyber operations conducted by virtually organized groups could potentially result in levels of harm and destruction akin to that produced by armed conflict.

When cyber operations indeed bring about levels of physical destruction similar to those produced by kinetic operations, it would not seem contentious to say that they could meet the threshold of intensity required to bring a non-international armed conflict into play. However, as with the criterion of resort to armed force discussed above in relation to international armed conflict, it is by no means clear when and under what conditions the calamitous results produced by cyber operations through the manipulation of computer networks (rather than direct physical destruction) might also be deemed of such intensity as to have generated a non-international armed conflict. Here, again, there is no instructive state practice or *opinio juris*, and humanitarian considerations do not point conclusively in favor of a particular interpretive approach.

Applying IHL Rules on the Conduct of Hostilities to Cyber Warfare

If occurring in the context of armed conflict, cyber operations would be subject to IHL, including in particular the IHL rules governing the conduct of hostilities. It is clear, however, that the application of these rules to operations involving the deployment of computer code in cyberspace, as opposed to the use of kinetic force in the physical world, is no simple matter.

The first challenge in this regard would be to determine what types of cyber operations would be subject to the rules governing the conduct of hostilities. This question is pertinent because of cyber operations' capacity to severely disrupt the functioning of key infrastructure without causing physical destruction of the type produced by traditional methods and means of warfare. With respect to the types of cyber operations that do fall within the conduct of hostilities framework, it will then be necessary to consider how the relevant rules, and most fundamentally the principles of distinction, proportionality, and precaution, are to be adapted and applied to cyber warfare.

When are Cyber Operations Subject to the Rules on the Conduct of Hostilities?

The rules on the conduct of hostilities codified in the First Additional Protocol to the Geneva Conventions (Additional Protocol I) are broadly recognized as reflective of customary international law applicable both in international and non-international armed conflicts.[19] Most of the specific rules contained in this framework are formulated as restrictions on those military operations that constitute an "attack."[20] This has prompted many to conclude that the rules on the conduct of hostilities apply only to cyber operations constituting an attack as defined in IHL.[21] However, this position is difficult to reconcile with the fact that the provisions of Additional Protocol I establishing the principles of distinction, proportionality, and precaution all contain clauses relating to military operations in general.[22] If these clauses are not to be deemed superfluous, the core principles governing the conduct of hostilities should be understood to apply not only to attacks, but also to hostilities in broader terms, i.e., to other military operations carried out in the context of an armed conflict with the purpose of harming the adversary.

Still, it would seem that all of the specific rules on the conduct of hostilities focusing on attacks as distinct from other types of military operations do indeed apply only to those cyber operations amounting to an attack. Since

much, even if not all, of the body of rules governing the conduct of hostilities is thus confined to attacks, it is clearly important to ascertain what cyber operations would in fact amount to an attack.

Article 49 of Additional Protocol I, which reflects customary IHL, defines attacks as "acts of violence against the adversary, whether in offence or in defence." It is accepted that the violence relates to the consequences of the attack and not the means used to effect those consequences. Accordingly, the sending of computer code, though not itself an act of physical violence, could nonetheless constitute an attack if it produces a violent outcome.

This view is reflected in the Tallinn Manual when it defines "cyber attack" as "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."[23] A pressing question that this definition does not resolve and remains subject to debate, however, is whether harmful outcomes produced by cyber operations might be deemed as constituting an attack even when they do not involve direct physical destruction, but instead cause other forms of damage to an object such as impaired performance. On the one hand, it would not make sense to maintain that cyber operations disrupting the functionality of critical infrastructure with deleterious consequences for potentially a great many people would not constitute an attack merely because they did not entail physical destruction. On the other hand, it would also be unreasonable to maintain that any interference with a computer system would amount to an attack that brings into play all of the rules governing the conduct of hostilities.

While the exact line of demarcation between cyber operations amounting to an attack and those that do not remains elusive, some considerations can help distinguish between them. For one thing, since the IHL concept of attack does not apply to non-physical means of psychological or economic warfare, such as the dissemination of propaganda or the establishment of an embargo,[24] cyber operations equivalent to such forms of "warfare" do not amount to an attack. Unlike attacks, which may never justifiably target civilians, IHL does not prohibit blockades and economic sanctions intentionally directed at the civilian population. Accordingly, cyber operations tantamount to economic sanctions cannot be said to constitute an attack.[25] Moreover, just as interferences with communications such as the jamming of radio or television broadcasts are not considered an attack under IHL and can therefore be directed at civilian communication systems as well, so

too not every disruption of computer based communication systems would constitute an attack. Of course, some types of interference with computer-based communications could have far reaching impact (e.g., disrupting the operation of financial institutions), and it therefore remains necessary to clarify exactly when, if ever, such interferences would constitute an attack. Indeed, while it is relatively straightforward to assert that cyber operations disrupting the functioning of objects in the physical world constitute an attack, the situation is far less clear when it comes to operations aimed merely at disrupting communication in cyberspace.

Applying the Principle of Distinction in Cyberspace

Under the principle of distinction, the parties to an armed conflict are obligated to distinguish at all times between the civilian population and combatants, and between civilian objects and military objectives, and may direct their operations only against military objectives.[26] Accordingly, cyber operations must only be directed at military objectives, namely "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."[27] Any object that does not fall within this definition is considered a civilian object and may not be the target of an attack.[28] Moreover, in case of doubt whether an object normally dedicated to civilian purposes is being used to make an effective contribution to military action, it must be presumed not to be so used and, consequently, may not be made the target of an attack.[29]

The main difficulty in applying these rules to cyber warfare lies in the fact that most cyber infrastructure is dual use, serving both civilian and military purposes. The currently prevailing position is that dual use objects are military objectives because of the military purpose they serve.[30] When applied to cyberspace, this position implies that almost all elements of international cyber infrastructure should be classified as military objectives and (subject to other IHL rules) could be susceptible to attack. Indeed, in this view, the cables, nodes, routers, and satellites on which so many civilian systems depend would all be deemed military objectives because they have the dual function of transmitting military information. With so many objects in the cyber realm thus considered military objectives, the principle of distinction – which is conceived as the foundational rule for shielding civilians from the dangers arising from hostilities – becomes largely devoid of protective

value. Whatever protection IHL might provide to civilian cyber infrastructure and to the civilian systems and services dependent on it would have to be derived from the principles of proportionality and precaution.

Even civilian cyber infrastructure that is not dual use and would therefore be protected from direct attack might nevertheless come to harm because of the interconnectedness of cyberspace. In order to avoid this outcome, and in accordance with the prohibition on indiscriminate attacks,[31] belligerent parties are prohibited from employing cyber weapons that are indiscriminate by nature, such as malware computer programs that replicate without control (viruses, worms) and whose harmful effects could not be limited as required by IHL. Furthermore, a belligerent intending to mount a cyber attack would have to first verify that in the given circumstances, the cyber weapon employed can be and is in fact directed at a military objective and that its effects can be limited as required by IHL.

The wide ranging list of military objectives in cyber warfare gives rise to questions concerning the geographical limits of the armed conflict. After all, cyber operations can utilize cyber infrastructure located anywhere in the world and could involve thousands or even millions of computers in diverse locations around the globe. If all such infrastructure were to be deemed a military objective, an armed conflict involving cyber warfare could be expanded to cover every corner of the earth. Every cyber war would be a potential cyber world war. In international armed conflicts the consequences would be checked to some degree by the laws of neutrality, which would limit the belligerent states' right to attack infrastructure located in the territory of a neutral state to those cases where the neutral state itself fails to terminate breaches of neutrality emanating from its territory; where such breaches constitute a serious and immediate threat to the attacked state's security; and when there is no other feasible and timely alternative response available.[32] In non-international armed conflicts, in which the law of neutrality is not applicable, questions about the geographical limitations of the battlefield are the subject of ongoing debate and become all the more vexing when the conflict involves cyber warfare.[33]

Applying the Principle of Proportionality in Cyberspace

Under the principle of proportionality, an attack is prohibited if it "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."[34] Here again a key question when applying the principle to cyber warfare will be to determine to what extent the term "damage" encompasses loss of functionality. In view of the severity of the consequences that may arise when the functionality of civilian infrastructure is disrupted, it seems only reasonable that such harm should figure in the proportionality calculus. On the other hand, and as already noted, it remains to be clarified exactly what types of disruptions to functionality fall within the relevant category of damage.

A further challenge in applying the principle of proportionality would be to determine whether the incidental damage to civilian objects that may be expected is excessive in relation to the military advantage anticipated. To be sure, the exercise of weighing expected harm to civilians or civilian objects against anticipated military advantage is always problematic, but in the case of cyber warfare the problems are exacerbated by the difficulty to assess with any accuracy what scope of incidental damage can be expected. This is so both because cyber operations are a relatively novel phenomenon and so little is known about their impact, and because the interconnected nature of cyberspace makes it particularly difficult to foresee all of the possible effects of such operations.

Applying the Principle of Precaution in Cyberspace

IHL requires belligerents to take precautions in attack,[35] as well as precautions against the effects of attack.[36]

Precautions in attack are mandated by a general rule, applicable to all military operations, whereby constant care must be taken to spare the civilian population and civilian objects,[37] and by additional rules establishing specific precautionary requirements. *Inter alia*, these rules require those who plan or decide upon an attack to do everything feasible to verify that targets are military objectives[38] and to take all feasible precautions in the choice of means and methods of warfare with a view to avoiding and in any event minimizing incidental harm to civilians.[39] Belligerents are further required to cancel or suspend an attack if it becomes apparent that it will entail a breach of the principle of proportionality.[40]

In light of these rules, a party to an armed conflict planning to implement a cyber attack would have to do everything feasible to gain the information necessary to verify that the projected target is a military objective and to

ascertain that the attack will not cause excessive harm. This may require employing technical experts to analyze the target network and the systems with which it is interconnected as best possible. When the expertise necessary to gain and to evaluate the required information properly is missing, the attack must be avoided altogether. In any event, attacks must be limited to those targets about which sufficient information is available.[41]

In certain circumstances, the duty to choose means and methods of warfare with a view to minimizing incidental harm to civilians could conceivably require belligerents to pursue their military objective via cyber attack rather than resorting to more destructive means involving kinetic force.

The duty to take precautions against the effects of attacks requires that to the maximum extent feasible, the parties to an armed conflict will endeavor to keep military objectives apart from civilians and civilian objects and will take other necessary precautions to protect civilians and civilian objects under their control against the dangers resulting from military operations.

In principle, belligerents may thus be required to do everything feasible to separate their military and civilian cyber infrastructure. In practice, however, military and civilian cyber infrastructures are so thoroughly interwoven that the endeavor to separate them is not likely to be deemed feasible. Perhaps more promisingly, and to the maximum extent feasible, belligerents would also need to take all necessary precautions to ensure that critical civilian infrastructure will be protected as much as possible from the effects of cyber attacks, e.g., by ensuring that necessary data is safely stored and effectively backed up and by providing for timely repair of civilian systems that come to harm.

Conclusion

Cyber warfare does not occur in a legal void. To be sure, cyber operations are governed by law, and when amounting to or occurring in the context of an armed conflict they are regulated by IHL. However, even while there is no question that IHL applies to cyber warfare, when considering *how* it is to be applied many questions emerge that have yet to be given a comprehensive and satisfactory answer.

Because of the shroud of secrecy surrounding cyber operations and because they involve methods and means of warfare so drastically different from those that IHL has evolved to regulate, it will often be difficult even to ascertain whether they occur within and in connection to an armed conflict.

Even when this is established and the applicability of the IHL rules on the conduct of hostilities is not in doubt, it is not entirely clear which cyber operations would be subject to these rules. Nor is there any clarity as to how the long established rules are to be interpreted when applied to this new form of warfare.

From a humanitarian perspective it is of the utmost importance that these questions be answered and that IHL be applied in such manner as to provide civilians and civilian infrastructure with effective protection from the harmful effects of cyber warfare. This will require careful interpretation of existing rules in light of the underlying humanitarian purpose of IHL and may also necessitate the development of some more stringent rules to ensure that humanitarian values will not be compromised.

Notes

1 For details on this definition see Cordula Droege, *Get off My Cloud: Cyber Warfare, International Humanitarian Law, and The Protection of Civilians* 886 International Review of The Red Cross 533, 538 (2012).

2 Due to internet interconnectivity, most military networks rely on civilian, mainly commercial, computer infrastructure. Conversely, civilian vehicles, shipping, and air traffic controls are increasingly equipped with navigation systems relying on global positioning system (GPS) satellites, which are also used by the military.

3 The most comprehensive of these efforts is the Tallinn Manual on the International Law Applicable to Cyber Warfare (hereinafter "Tallinn Manual"), which was drafted by a group of experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence. See Tallinn Manual on the International Law Applicable to Cyber Warfare (Michael N. Schmitt, gen. ed., 2013), http://www.ccdcoe.org/249.html.

4 States express their consent to be bound by an international norm either by becoming party to an international treaty containing it, or via international custom which in turn emerges from the consistent practice of states combined with the view that such practice is mandated by law (*opinio juris*). A norm of customary international law is binding on all states apart from those which expressed a consistent objection to the applicability of the norm in question.

5 These treaties include, notably, the Hague Conventions of 1899 and 1907, The Four Geneva Conventions of 1949 and the 1977 Additional Protocols to the Geneva Conventions of 1949.

6 In something of an exception to this general tendency, some general aspects of the United States' positions on the application of IHL (and other areas of international law) to cyber warfare were discussed in a speech delivered on 18 September 2012 by US State Department Legal Advisor Harold Koh at a conference sponsored by United States Cyber Command (USCYBERCOM). In his speech, Mr. Koh did not provide a detailed account of the United States' position but did offer brief

answers to "fundamental questions" on the issue and identified several "unresolved questions" with which the United States would likely be forced to grapple in the future. *See* Harold Hongju Koh, *International Law in Cyberspace: Remarks of Harold Koh*, 54 Harvard International Law Journal (December 2012), http://www.harvardilj.org/2012/12/online_54_koh/.

7 This commonly accepted definition of international armed conflict was articulated by the International Tribunal for the former Yugoslavia (hereinafter "ICTY") in *Prosecutor v. Tadic*, Case No. IT-94-1-A, Appeals Chamber Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, 2 October 1995, Para. 70. International treaties do not contain a detailed definition of international armed conflict. That said, common Article 2 of the Four Geneva Conventions of 1949 does establish that the conventions apply to any armed conflict that may arise between two or more states. Article 1(4) of the First Additional Protocol to the Geneva Conventions extends the scope of application to other situations, but this applies only in relation to states party to the Additional Protocol and is thus not applicable to Israel.

8 *See* discussion in Droege, *supra* note 1, at 543.

9 Rule 7 of the Tallinn Manual (*supra* note 3) provides that "[t]he mere fact that a cyber operation has been launched or otherwise originates from governmental cyber infrastructure is not sufficient evidence for attributing the operation to that state but is an indication that the state in question is associated with the operation."

10 *See*, International Law Commission, Draft Articles on the Responsibility of States for Internationally Wrongful Acts, *Yearbook of the International Law Commission*, 2001, Vol. II (Part Two) at Article 8.

11 This was the position taken by the International Court of Justice (ICJ). *See*, International Court of Justice, *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, Judgment of 27 June 1986, paras. 115–116.

12 This position was articulated by the ICTY in relation to the attribution of the actions of organized armed groups to a state. *See*, ICTY, *Prosecutor v. Dusko Tadic*, IT-94-1, Appeals Chamber Judgment of 15 July 1999, para. 120. It should be noted, first, that the ICTY was relating only to the attribution of responsibility for the actions of an organised armed group and not private actors in general. Second, the ICTY itself clarified that more compelling indications of state control would apply in cases where the armed group is not acting from within the territory of the state in question. *See*, *Ibid.* at paras. 138-140.

13 *See*, Droege *supra* note 1, at 546; Michael N. Schmitt, *Classification of cyber conflict,* 17(2) Journal of Conflict and Security Law, 251 (Summer 2012); Knut Dörmann, *Applicability of the Additional Protocols to Computer Network Attacks*, International Committee of the Red Cross 3 (2004), http://www.icrc.org/eng/resources/documents/misc/68lg92.htm; Heather Harrison Dinniss, Cyber Warfare and the Laws of War, 131 (2012); Nils Melzer, *Cyberwarfare and International Law*, United Nations Institute for Disarmament Research, Resources Paper, 24 (2011), http://www.unidir.ch/pdf/ouvrages/pdf-1-92-9045-011-L-en.pdf.

14 A purposive interpretation of IHL has been regularly pursued by the ICTY. *See*, e.g., Prosecutor v. Delalic et al. (Celebici Case), Judgment, Case No. IT-96-21-T, T.

Ch. IIqtr, 16 Nov. 1998, para. 170. For a general and authoritative discussion about the purposive interpretation of law see Aharon Barak, Purposive Interpretation in Law (Sari Bashi trans, 2005).

15 The term combatant applies only to fighters on behalf of the rival parties to an international armed conflict who would be entitled to prisoner of war (hereinafter "POW") status if captured by the adverse party. Fighters in a non-international armed conflict are not entitled to POW status, but can be made the target of direct attack by the rival belligerent.

16 This definition was articulated in ICTY, *Prosecutor v. Tadic*, *supra* note 7, at para. 70.

17 *See* ICTY, *Prosecutor v. Boskoski*, IT-04-82-T, Trial Chamber Judgment of 10 July 2008, paras. 199–203. *See* also, ICTY, *Prosecutor v. Limaj*, IT-03-66-T, Trial Chamber Judgment of 30 November 2005, paras. 94–134; ICTY, *Prosecutor v. Haradinaj*, IT-04-84-T, Trial Chamber Judgment of 3 April 2008, para. 60.

18 *See* Tallinn Manual, *supra* note 3, Commentary on Rule 23, paras. 13-15.

19 *See*, International Committee of the Red Cross, Customary International Humanitarian Law, Vol. I, Rules (Jean-Marie Henckaerts and Louise Doswald-Beck eds., 2005).

20 Multiple references to attack are found, notably, in Articles 51, 52, and 54-58 of Additional Protocol I.

21 *See*, e.g., Michael N Schmitt, *Cyber Operations and the Jus in Bello: Key Issues*, 87 Naval War College International Law Studies, 91 (2011). For alternative views see Melzer, *supra* note 13, at 28 (arguing that that the rules apply to all cyber operations constituting part of 'hostilities') and Dinniss, *supra* note 13, at 196-202 (arguing that the rules apply to all computer network attacks that constitute military operations by virtue of being associated with the use of physical force even while not themselves resulting in violent consequences).

22 The formulation of the principle of distinction in Article 48 of Additional Protocol I stipulates that the parties to an armed conflict "…shall direct their *operations* only against military objectives." The first paragraph of Article 51 thereto stipulates that civilians "shall enjoy general protection against the dangers arising from *military operations*" and Article 57, para. 1 thereto instructs that "in the conduct of *military operations*, constant care shall be taken to spare the civilian population, civilians and civilian objects" (emphasis added).

23 *See*, Tallinn Manual, *supra* note 3, rule 30.

24 *See*, Michael Bothe, Karl Josef Partsch and Waldemar A. Solf, New Rules for Victims of Armed Conflicts: Commentary to the Two 1977 Protocols Additional to the Geneva Conventions of 1949, 289 (1982).

25 *See*, Droege, *supra* note 1, at 559.

26 *See*, Article 48 of Additional Protocol I, which reflects customary IHL.

27 *See*, Article 52(2) of Additional Protocol I, which reflects customary IHL.

28 *See*, Article 52(1) of Additional Protocol I, which reflects customary IHL.

29 *See*, Article 52(3) of Additional Protocol I, which reflects customary IHL.

30 *See*, Tallinn Manual, *supra* note 3, Commentary on Rule 39, para. 1.

31 *See*, Article 51(4) of Additional Protocol I, which reflects customary IHL.

32 *See*, Tallinn Manual, *supra* note 3, Chapter 7, in particular the Commentary on Rule 94.
33 *See, Id.,* Commentary on Rule 21. *See* also, International Humanitarian Law and the Challenges of Contemporary Armed Conflicts, Report of the 31st International Conference of the Red Cross and Red Crescent, 21-22 (Geneva, 28 November - 1 December 2011; report prepared by the International Committee of the Red Cross, October 2011).
34 *See*, Article 51(5)(b) of Additional Protocol I, which reflects customary IHL.
35 *See*, Article 57 of Additional Protocol I, which reflects customary IHL.
36 *See*, Article 58 of Additional Protocol I, which reflects customary IHL.
37 *See*, Article 57(1) of Additional Protocol I.
38 *See*, Article 57(2)(a)(i) of Additional Protocol I.
39 *See*, Article 57(2)(a)(ii) of Additional Protocol I.
40 *See*, Article 57(2)(b) of Additional Protocol I.
41 *See*, Droege, *supra* note 1, at 574.