Some Thoughts on Computer Network Attack and the International Law of Armed Conflict

Louise Doswald-Beck

Introduction

It seems one has to accept as inevitable that when something useful for the improvement of man’s life has been invented, thoughts will either turn to how to weaponize or destroy it, or, in the case of computer network technology, both.

The task of the international lawyer in the face of a new weapon or intended military activity is to establish how existing law applies and with what effect. Would existing law prohibit the weapon or activity or restrict it in any particular way? Would it be appropriate, for one or more policy reasons, to impose prohibitions or restrictions that do not already apply? Might it be the case, on the contrary, that the new weapon or method might be an improvement from both a policy and humanitarian point of view?

The purpose of this short chapter is to explore certain aspects of how computer network attack (CNA) could be affected by international humanitarian law (IHL), including the law of neutrality, based on the knowledge generally available so far on the military possibilities presented by computer networks. It

The opinions shared in this paper are those of the author and do not necessarily reflect the views and opinions of the U.S. Naval War College, the Dept. of the Navy, or Dept. of Defense.
may be that these possibilities are overstated, but the chapter will base itself on the premise that a variety of the indicated effects would be possible.

**Applicability of the International Law of Armed Conflict (International Humanitarian Law)**

It is perfectly reasonable to assume that CNA is subject to IHL just as any new weapon or delivery system has been so far when used in an armed conflict. The only real difficulty in this regard would arise if the first, or only, “hostile” acts were conducted by these means. Would this amount to an armed conflict within the meaning of the 1949 Geneva Conventions and other IHL treaties? This question is close to, but not necessarily identical with, whether the behavior amounts to an armed attack within the meaning of Article 2(4) of the UN Charter. The ICRC Commentary to the 1949 Geneva Conventions indicates that in the case of a cross-border operation, the first shot suffices to create an international armed conflict, which can therefore be of very short duration. There are, of course, other views which would require a threshold of intensity or time, but this approach would lead to the need for evaluations that would create inevitable uncertainties and ultimately to the same problems faced when establishing whether “war” existed without a formal declaration; this issue led to the abandonment for the need for a “war” for the “law of war” to apply. The problem is still with us, however, in non-international armed conflicts where there remain many cases of uncertainty (or denial) as to whether the threshold and nature of violence has reached that of an armed conflict, rather than “just” internal violence requiring “police” operations. If the first or only “hostilities” that occur in a non-international situation were computer network attacks, the degree of doubt would be even greater.

The problem is, of course, that so far hostilities have involved weapons which launch projectiles, or other types of energy transfer, that lead to visible physical damage. In the case of IHL, the motivation for the application of the law is to limit the damage and provide care for the casualties. This would militate in favor of an expansive interpretation of when IHL begins to apply. The likelihood of this threshold being linked with the perception that an armed attack within the meaning of Article 2(4) has occurred in the case of a cross-border CNA is, of course, high, given the historical development of the *jus ad bellum* and the *jus in bello*. This would not be problematic if it had a restraining effect on the commencement of hostilities through CNA, either because of the Article 2(4) prohibition, or because the Security Council decided the CNA amounted to a threat to the peace and dealt with it in a way that avoided more damage.
However, the danger lies in the possibility of the CNA being perceived as an armed attack justifying measures of self-defence, for such a characterization might escalate the situation further than would otherwise have been the case. Whether or not these linkages occur, there is an argument to be made in favor of the implementation of IHL when CNA is undertaken by official sources and is intended to, or does, result in physical damage to persons, or damage to objects that goes beyond the bit of computer program or data attacked. CNA alone in non-international contexts is even more problematic—it is far more likely to be seen solely as criminal behavior, although the potential for damage could be enormous and the groups undertaking this could be at least as well organized as “armed” groups. Once “normal” weapons are used, there is no problem at all. CNA will be an attack (in the sense of the *jus in bello*) as any other. Whether CNA alone will ever come to be seen as amounting to an armed conflict for the purposes of IHL implementation will probably be determined through practice, rather than a formal decision by the international community in the abstract, although the latter should not be ruled out. It will probably also depend on the degree of damage that CNA causes (the more it creates, the more likely it will be treated in the same way as an armed conflict). Perhaps even the term “armed” conflict will one day start sounding as outdated as “*jus in bello!*”

**How the Existing Law of Armed Conflict Would Affect the Use of Computer Network Attack**

As indicated earlier, one can safely assert that the whole body of IHL applies to the use of CNA. Three areas of this law seem, however, particularly pertinent: the principle of distinction and all the rules that flow from it, the use of ruses of war and the prohibition of perfidy, and whether the rules relating to combatant status could be affected. In addition, some thought needs to be given to the law of neutrality during armed conflict.

**The Principle of Distinction**

Whereas in the eighteenth and nineteenth centuries methods of warfare meant that civilians were only directly affected by sieges and otherwise only indirectly by the general economic advantages or misfortunes caused by war, the advent of air and missile warfare in the 20th century brought the need for special protection for civilians against attack to the fore. The principle of distinction has therefore taken on an importance, and led to detailed treaty and customary law, that goes well beyond the few rules articulated in the 1899 and 1907 Hague
Conventions. Although heartily derided by the "realists," those persons who strove to ban the dropping of bombs from the air were obviously far-seeing people who realized the potential for massive destruction that this new method represented. Even restrictions on air warfare were slow to come about, only being accepted, in the form of the 1977 Protocols Additional to the Geneva Conventions, once the potential military utility of air warfare had been thoroughly explored. Although the form and probable effect of warfare is quite different, the same pattern may be showing itself in relation to CNA. Here is a new tool that in civilian life opens up access to the world through rapidity and ease of communication in a way that has been heretofore unseen. Moreover, it allows technological development that could lead to all kinds to extraordinary steps in human development. One suggestion that has been made is to consider banning at least some forms of CNA; however, it has been rejected, probably because of the desire to further explore CNA's military potential. As always, there are those who argue that "progress" cannot be stopped, that new means and methods of warfare are inevitable, and that therefore there is really no point in trying to stop or regulate anything. Others prefer to see which new methods are useful in that they are more accurate, militarily more effective, do not cause unnecessary damage, and are not more trouble than they are worth. Needless to say, IHL in general, and the principle of distinction in particular, are based on the latter premise. It is hoped that, unlike bombardment from the air, careful thought will be given to CNA before launching into experimentation.

The principle of distinction involves a number of rules that will be of particular relevance for CNA: (i) the evaluation that objects considered for attack are indeed "military objectives" within the meaning of IHL; (ii) the prohibition of indiscriminate attacks; (iii) the need to minimize collateral damage and to abstain from attacks if such damage is likely to be disproportionate to the value of the military objective to be attacked; and (iv) the need to take the necessary precautions to ensure that the above three rules are respected. From what is known at present, there are potential problems as regards all of these rules in relation to CNA.

Only Military Objectives May Be Attacked

The definition of military objective contained in Additional Protocol 1 is not only that accepted by the 155 States party to the treaty, but was also referred to as being the appropriate one to use by the representatives of several major non-party States at the recent diplomatic conference that adopted the Second Protocol to the Hague Convention for the Protection of Cultural Property of 1954. In order for something to be a military objective, it must meet two cumulative conditions: it must make an effective contribution to the military
action of the adversary and, in the circumstances ruling at the time, its attack must offer a definite military advantage to the attacker. It is clear that this definition does presuppose a plan to be followed with a view to achieving a particular military result. It also presupposes a knowledge of what the adversary is using, and how it is being used, for its military action. The terminology was chosen carefully to prohibit certain behaviors of the Second World War, specifically, it addressed the attack of persons and objects on the basis that they are “quasi-combatants” or in one way or another help the “war effort.” Such reasoning leads sooner or later to no restraints, for anything can be justified this way. Indeed, it rapidly led to the United Kingdom deciding that “civilian morale” was to be a target and, as a result, to the wholesale destruction of cities.

The specification that the object must effectively help the “military action” of the adversary means that the link to the military operations must be a close and obvious one. The reference to the “circumstances ruling at the time” requires that the military advantage to the attacker be equally clear and obvious in the context of the attacker’s military plan to achieve the particular military aim. During the negotiation of the Additional Protocols, this was considered to represent both economy of force and military professionalism, thereby leading to the military result needed while moving away from generally attacking anything in the hope that in due course the adversary would surrender. The decision not to adopt a list of “military objectives” was part of the same reasoning. Any list could either exclude something that in the circumstances could be of great importance in achieving the particular military mission, or alternatively include things of little or no importance in the particular circumstances. It is for this reason that any “list” in a textbook or manual can never offer more than examples of what have at one point or another been considered to be military objectives in past conflicts—they will not necessarily be so in any particular future one.

It is to be hoped that planning and precision will not be lost. Computer networks can easily be seen as “communications.” Many manuals refer to “means of communication” as typical military objectives—a simple reference to existing lists could lead to the appalling result that any computer network used by the adversary State and its citizens could be attacked. Quite apart from the fact that this would almost certainly hit protected objects, and in addition amount to an indiscriminate attack, it would not result from the necessary process of evaluation described above. In order to amount to a military objective, either the piece of network being affected or the object that the network is controlling must meet the two conditions.

There could also be the temptation to try to totally remove the technological framework which the whole of society bases itself on (although this may well be
Computer Network Attack and the International Law of Armed Conflict

technically impossible through CNA), on the reasoning that this would make that society's life so generally unpleasant that surrender would surely follow. The temptation is likely to be all the greater because military networks will probably be better protected from hacking than a number of civilian networks. It could also be asserted that this method would be more "humanitarian" than sending bombs. It is clear that this reasoning is quite different from that underlying the Protocols, which stress choices of target for the specific desired military goals. Is there a possibility that sophisticated military practice (which was the basis for the rules in the Protocols) will change? What would happen to the principle of distinction? An approach based on technological siege warfare would in effect make it disappear, or at least radically change its characteristics. It could require that specially protected objects, e.g., hospitals, organize themselves so that they are not within the normal computer network (if this were practicable) in order to be protected. In effect, this would represent a return to the reasoning behind the rules of Geneva Convention IV of 1949\(^1\) and the Hague Convention of 1954,\(^1\) which rely on the concept of the creation of various safe areas because they assumed that the practices of World War II would prove inevitable. Such reasoning would amount to abandoning the approach of the Protocols and present customary law, i.e., that all objects that are not military objectives are safe from being deliberately targeted.

Careful thought should be given before going down the road of technological siege warfare. Quite apart from the fact that it would be contrary to present customary and treaty law, the presumptions that such a practice would be based on are dubious for at least two totally separate reasons. First, society is increasingly becoming so dependent on modern technology that computer systems failure for a lengthy period would not be just "unpleasant"—it could easily lead to mass disease, starvation and other catastrophes\(^1\) (it is probable that such a scenario could not be accomplished by CNA alone, but it may well be possible when undertaken in conjunction with other methods). On the other hand, and despite the recent example, it would not necessarily lead to surrender in a short period of time. Both reasons lead to the conclusion that surgical technological strikes, to the degree that this is technically possible, would make more sense.

The Prohibition of Indiscriminate Attacks

Additional Protocol I defines indiscriminate attacks in Article 51(4).\(^1\) An attack is indiscriminate when it either is not carefully aimed at each military objective (through carelessness or use of inappropriate weapons) or when its effects on a military objective are uncontrollable and unpredictable (an obvious and
uncontroversial example would be the use of a bacteriological weapon against a group of soldiers).

From what has been written so far on CNA, this appears to be potentially the most serious problem, i.e., aiming accurately at what the intended target is and, even if one manages to strike it with precision, not at the same time creating a host of unforeseen and unforeseeable effects.\(^\text{16}\)

**The Problem of Collateral Damage**

The need to avoid, or at least minimize, damage to civilians and civilian objects is reflected in Article 57(2)(a)(ii) of Protocol I, which indicates that "those who plan or decide upon an attack shall . . . take all feasible precautions in the choice of means and methods of attack with a view to avoiding, and in any event to minimizing, incidental loss of civilian life, injury to civilians and damage to civilian objects." An attack only becomes in itself illegal, however, if it violates the rule of proportionality, a long-standing rule of customary law. The wording used in Article 51(5)(b) of Protocol I is "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."

The evaluation as to whether likely civilian damage would be disproportionate has an inherent difficulty in that one is comparing two different things. Whereas the need to avoid or at least minimize collateral injury is a straightforward rule relating to the choice of means or methods that should be preferred, an evaluation as to possible illegality is fraught with difficulty. A certain subjectivity seems inevitable, but as an anticipated result could be illegal, there ought to be some objective factors to follow. State practice in this regard is scant—just a few examples have been given on when such attacks have been desisted from—and they have usually been when either the possible target was something that was military in nature but in the circumstances unusable or where the object’s value as a military objective could not be verified.\(^\text{17}\) To complicate matters, certain statements of understanding indicate that the attack is to be considered as a whole when making the evaluation.\(^\text{18}\) However, these statements should not be interpreted as meaning proportionality of the civilian damage caused during the entire campaign compared with military advantages obtained during a specific attack. Such an interpretation is impossible because the only evaluation that could be possible would be at the end of the conflict, whereas the rule requires the evaluation to be done **before** the attack concerned. Proportionality evaluations pursuant to the *jus in bello* should also not be confused with proportionality in self-defence, which is the *jus ad bellum* rule that requires the military action as a
whole to be limited to what is necessary to restore one's territorial integrity.\textsuperscript{19} Rather, based on a number of sources, the statements of understanding can only be logically interpreted as referring to the fact that the military value of attacking an object (which has to be weighed against the likely civilian casualties) will obviously be assessed taking into account its role in the broader strategic purpose of a particular military operation that may consist of various individual actions.\textsuperscript{20}

There could be, of course, a temptation to consider that whatever collateral damage was caused by CNA, it would surely be proportional to the military advantage gained. This would be an abuse of the rule, as it requires a careful advance evaluation of the likely effects on the civilians. If the likely effects are quite unclear and unforeseeable (which appears to be the technical situation at present), the attack would be an indiscriminate one and therefore illegal as such—the rule of proportionality would not even be relevant.\textsuperscript{21}

\textit{Precautions in Attack}

It is obvious that in order to respect the rules relating to the principle of distinction, a certain amount of thought and planning is necessary. Such precautions are therefore nothing more than the expression of a \textit{bona fide} implementation of the law.\textsuperscript{22} The advance evaluations indicated above are of particular importance, but it also ought to be possible to call off an attack once it becomes clear that what was thought to be a military objective is not one after all or ceases to be one, or if it becomes clear that the consequent collateral damage would be excessive.\textsuperscript{23} This would be particularly relevant in cases of CNA methods that would not have an immediate effect on the target.

The other aspect of great importance, in order to evaluate military objective or incidental damage, is that of sufficient intelligence information. The advantage of computer operations is that they can be conducted from the comparative security of a computer terminal far from the actual military operations. Computer network exploitation (CNE) could help gain maximum information on an adversary's situation, provided that such data is available on reachable networks and that the data is not itself deliberate misinformation. However, although it is a valuable tool for gaining intelligence and does not pose the risks of physical presence, CNE cannot totally replace intelligence gathering by other means, especially the most reliable one, direct observation.\textsuperscript{24} CNE combined with other intelligence sources could well provide for the possibility of good precautions being taken in attack.

On the other hand, CNA conducted from a distance poses two particular problems in relation to precautions in attack. First, if one suspects that one is the object of such an attack, taking out the attacker is likely to prove to be very
difficult because of the immense difficulty of being sure where the attack originated. The likelihood, therefore, of attacking back in quite the wrong place is high.

Second, lack of physical presence near the object to be affected means that the likelihood of making mistakes as to whether something really is at that moment a military objective is high. Protocol I speaks in terms of the attacker doing “everything feasible” to verify that the target is a military objective. The word “feasible” clearly indicates that perfection is not expected. It is a matter of common sense and good past military practice that commanders take into account the need to reduce exposure of their own armed forces (an eliminated army cannot win an armed conflict). However, it is only a recent practice that so much care is given to avoiding any military casualties on one’s own side, and one can see how tempting CNA would be in such an endeavor. The law requiring precautions in attack cannot be simply eliminated if such precautions involve some physical risk to the attacker. Although not articulated anywhere as such, when such a practice means that there are many more civilian casualties than military, the concept of the principle of distinction is badly battered, perhaps even turned on its head. Once again, apart from amounting to a violation of existing law, such inaccuracy gives rise to concern as to the effectiveness of the intended military operation.

Ruses of War and Perfidy

Computer data provides new avenues for practicing ruses of war. The more CNE is undertaken, the more likely it is that misinformation will be deliberately planted to confuse the adversary. Such misinformation about one’s own affairs is perfectly lawful, for it is analogous in principle to any other vehicle for misinformation. Moreover, it is clear from traditional sources that ruses of war need not be limited to creating misinformation about oneself. However, it must also be true that computer generated attacks cannot be undertaken whilst giving the impression that they come from the adversary’s own side. This would be the equivalent to attacking while wearing the enemy’s uniform, which is clearly illegal. As with all ruses of war, care must be taken that they do not cross the line into perfidy. Therefore, misinformation implicating protected persons or objects would be unlawful, as would CNE amounting to a breach of good faith, such as pretending to surrender or to create a truce.

Combatants and CNA

It is most likely that CNA and CNE would be carried out by specialized personnel. What would be the legal situation of such persons? Could they be
attacked by any means and in any place? What would be their status if captured? There is probably no reason why the rules should be any different than in traditional armed conflict.

If incorporated into the armed forces, such personnel would have all the rights and liabilities of combatants. Therefore, they certainly could be attacked like any other combatant and should endeavor to be in uniform if captured. The narrow exception in Article 44(3) of Protocol I (for those party to it), which would allow POW status if captured without uniform, may well not apply to such persons, as this provision is generally interpreted as applying only to combatants in occupied territory, and only then in certain situations. Persons captured in the adversary’s territory without uniform carrying out CNE would also qualify as spies. If conducted from outside the territory, however, the situation should be no different from someone gathering data from a spy satellite.

Technicians that act for the military, but are not part of it, pose more of a problem. The persons listed in Article 4(4) of Geneva Convention III of 1949 are entitled to prisoner of war status if captured, but the type of persons listed are more analogous to computer technicians that keep the machines in order, and not ones that actually undertake the attacks. It could well be, therefore, that persons who actually undertake CNA would be considered civilians who would have no POW status if captured. They would also be subject to attack, as they would be taking a “direct part in hostilities.” Whether those undertaking CNE are in exactly the same situation is less clear, and this is because State practice is not consistent as to whether intelligence collection falls into the category of taking a “direct” part in hostilities. However, there is no reason why gathering intelligence by this means should be treated any differently from intelligence gathering by other means. The possibility of being treated as a spy would only occur if the CNE were carried out clandestinely in the territory of the adversary. The Hague Regulations of 1907, in particular Article 21, do not exclude the possibility that civilians could be spies for the purposes of IHL, although Article 46 of Protocol I only refers to members of the armed forces. However, both treaties conceptually indicate the need to be caught in the act in the territory controlled by the adversary, although this is not the exact wording used. However, if the civilian undertaking CNA or CNE is not “claimed” by the army using him, he could be simply treated as an individual breaking national law and therefore be subject to criminal law should he be captured on return to the country; the rule that he cannot be treated as a spy once he returns to his own army would not apply and there is no reason why POW status would be considered either.
The Effect on Neutral States

Although there are a number of discussions on whether there is a formal difference between "non-belligerent" and "neutral" States, and a resulting difference of legal regime,\textsuperscript{32} this author believes that there is insufficient basis in State practice to support such an assertion. Therefore, for the purposes of this chapter, all States not party to a conflict will be treated as "neutral."

As many networks link up and/or are owned by different countries or their private citizens, and given that it is the general view that the effect of any CNA might not be limited to the intended target, the law relating to neutral States is of particular significance. The law of neutrality in cyberspace poses difficulties, beyond those of other aspects of IHL, because neutrality law has led to legal regimes that differ depending on the region of operations. Thus, there are significant differences between the law applicable to land, sea (which is subdivided into different maritime areas), and outer space operations. It is not self-evident what the regime should be in relation to cyberspace. To suggest that it should vary depending on whether the data affected are supposed to be at any particular moment in a country’s territory, passing via a satellite, or being conducted through an underwater cable would create a factual and legal nightmare.

One could, of course, simply wait to see what happens and deduce customary law based on practice, rather like what initially happened in relation to the law of outer space, which began to take shape when the first satellites were actually put into orbit. However, this new area of activity did not escape formal regulation through a series of international instruments that began to be adopted after only a few years, initially in the form of UN resolutions and later a number of treaties which confirmed the practice that outer space and other planets could not be acquired by any nation nor be used to base certain weapons.\textsuperscript{33} Therefore, the likelihood of CNA being left entirely to practice without more formal international legal regulation is somewhat slim. It would make sense at this stage to consider the kind of regime that would be appropriate, and, rather than be totally inventive, see whether basic principles of the law of neutrality could provide some answers.

The basic premise of the law of neutrality is that a neutral State should not, through its actions, deliberately affect the outcome of armed conflict between belligerents. In return, the neutral expects not to be drawn into the conflict. An excellent description of the concept of neutrality and the basic rules that flow from it is contained in Volume II of Oppenheim’s \textit{International Law}. Certain passages in this description remain of fundamental importance. After indicating that all States that are not drawn into the war are presumed neutral, it provides that:
Since neutrality is an attitude of impartiality, it excludes such assistance and succour to one of the belligerents as is detrimental to the other, and, further, such injuries to the one as benefit the other. But it requires, on the other hand, active measures from neutral States. For neutrals must prevent belligerents from making use of their neutral territories, and of their resources, for military and naval purposes during the war. . . . Further, neutrals must, by all means falling short of becoming involved in hostilities or of abandoning their attitude of impartiality, prevent each belligerent from interfering with their legitimate intercourse with the other belligerent through commerce and the like, because a belligerent cannot be expected passively to suffer vital damage resulting to himself from the violation by his enemy of a rule, which, while it operates directly in favour of neutrals, indirectly operates in his favour as well.

The required attitude of impartiality is not incompatible with sympathy with one belligerent, and disapproval of the other, as long as these feelings do not find expression in actions violating impartiality. . . . Moreover, acts of humanity on the part of neutrals and their subjects . . . can never be construed as acts of partiality, even if these comforts are provided for the wounded and the prisoners of one belligerent only.34

The same thought is put across even more succinctly by Professor Leslie Green:

So long as the activities of these non-participants do not interfere with the legitimate activities of the belligerents or benefit one at the expense of the other, neutrals are entitled to have their territory and doings respected and unaffected because of the conflict.35

These passages indicate the importance of distinguishing between, on the one hand, the right of the neutral State to carry on its life, including commerce with belligerents, as normal, from, on the other hand, the prohibited behavior of actively favoring the outcome of the war through State acts. This is also the reasoning, cited in Oppenheim, behind some of the more detailed rules, including those that distinguish between State acts and the acts of a State's citizens:

International Law is primarily a law between States. . . . In the first instance, neutral States are bound by certain duties of abstention, e.g., in respect of supply of loans and munitions to belligerents, which they are not bound to exact from their nationals. Secondly, neutral States are under a duty to prevent their territory
from becoming a theatre of war as the result of passage of foreign troops or aircraft or of prolonged stay of belligerent men-of-war in their territorial waters. Thirdly, they are bound to control the activities of their nationals insofar as these may tend to transform neutral territory into a basis of war operations or preparations. At the same time, International Law renders unlawful certain activities of nationals of neutral States, like carriage of contraband or breach of blockade, without, however, imposing upon these States the duty to prevent or to penalise such acts. These are punished by the belligerent against whom they are directed. 36

Oppenheim then recognizes the rather thin line between individual activity and State activity in regulated economies, but indicates that the rule still exists. Although this text was published 48 years ago, practice has not really changed significantly, especially in the light of the precision given on export licences:

From the case of actual governmental responsibility for the production of and trade in certain articles there must be distinguished that of governmental control over exports by the system of licensing and the like. The fact that the Government permits export which it could prevent by means of withholding the licence does not make it a party to the transaction. Its responsibility is engaged only when in thus acting it discriminates between the opposing belligerents. . . .

. . . Apart from certain restrictions necessitated by impartiality, all intercourse between belligerents and neutrals takes place as before, a condition of peace prevailing between them in spite of the war between the belligerents. This applies particularly to the working of treaties, to diplomatic intercourse, and to trade. 37

The same point is made by Professor Green:

A neutral does not have to forbid the supply of war matériel by resident individuals or companies, nor is it required to stop the passage of such goods across its territory. It is under no obligation to forbid the use of privately-owned communication equipment on behalf of belligerents, but if it limits the freedom of its nationals to provide such facilities this restriction must operate against all the belligerents. 38

This passage stresses the fact that neutral States have, for the most part, the right to carry on life as normal. Their specific duties are relatively narrow, concentrating primarily on preventing their territory from being used as a base.
of operations by one belligerent or the other. If they choose to grant specific facilities (that must not directly concern military operations), they must be granted to all the belligerents equally, e.g., if the neutral allows one belligerent to bring prizes to one of its ports, it must allow the other belligerent the same rights.⁴⁹ Therefore, any negative effect of the war on the neutral State would be indirect.

The specific rights of belligerents in relation to neutral merchantmen in this context are more in the character of an exception to the general rule than otherwise. They are based on the rather special combination of being acts that are carried out against individuals, in an area that is not national territory, and stem from very long and peculiar practice specific to naval warfare. Any analogy between computer networks and these special rules of neutrality relating to merchantmen on the high seas would be highly dubious; it would certainly not be based on the general principles which for the most part allow neutral citizens to carry on life as normal. State practice over the last 50 years is essentially consistent with this position. Arguments that most States are not really “neutral” because of the degree of relations that they and their citizens have with belligerents appear to be founded on an exaggerated interpretation of the degree of restrictions and duties that such States are supposed to have.⁴⁰ Therefore, a belligerent State would have to be very certain that a neutral State has indeed violated its duties of neutrality before considering self-help measures involving force to stop the violation. Such a violation of the duty of neutrality by the State cannot be easily asserted. In addition, the prohibition of the use of force in Article 2(4) of the UN Charter means that such a use of force by a belligerent could, if not clearly lawful, be not only a breach of the law of neutrality, but also a violation of the UN Charter.⁴¹

Returning specifically now to the question of computer networks, which are for the most part owned by companies that are more or less subject to a limited degree of State regulation, basic principles of neutrality law would militate in favor of their continuing to be used as normal, even if some States are in an armed conflict with each other. The nearest equivalent to computer networks in existing neutrality law is reflected in Article 8 of Hague Convention V of 1907:

A neutral Power is not called upon to forbid or restrict the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraphy apparatus belonging to it or to companies or private individuals.
In so far as much of the computer network does indeed use telephone lines, this provision is directly applicable. In other cases, both its implication and the basic principles of neutrality law would support application of the same rule. As far as transmission via satellite is concerned, there is no reason why the rule should be any different; freedom of the use of outer space in international law is extensive and the 1967 Outer Space Treaty does not contain any specific provisions that would prevent the use of neutrally owned satellites by belligerents or give the right to a belligerent to interfere with such satellites. Despite the indication in Article III that the use of outer space should be pacific, and in Article I that it should be in the interests of all countries, the prohibitions that are clearly enunciated are limited to weapons of mass destruction, and, at any rate, use must be in conformity with international law. Without taking a stand on whether any type of military use of satellites is in conformity with the letter or spirit of the 1967 treaty, it contains nothing that would change the law of neutrality as such, nor, to this author’s knowledge, has it been interpreted as having done so. This brings us back to general neutrality law.

It would appear, therefore, that a breach of neutrality would only occur if a neutral State specifically allowed a network to be built on its territory for the purposes of supporting the armed conflict of one or more belligerents or if it specifically allowed a network to be devoted to this purpose, for doing so would be the equivalent of allowing its territory to become a base of operations. This conclusion mirrors Article 3 of Hague Convention V:

Belligerents are . . . forbidden to

(a) Erect on the territory of a neutral Power a wireless telegraphy station or other apparatus for the purpose of communicating with belligerent forces on land or sea;

(b) Use of any installation of this kind established by them before the war on the territory of a neutral Power for purely military purposes, and which has not been opened for the service of public messages.

Article 5 of the same treaty indicates that neutral States must not allow any of these acts to occur on its territory.

So much for the use of computer networks by neutrals and belligerents. What would be the case if a CNA was directed at a target in a belligerent country but affected a neutral country. If such an effect was unforeseeable and unlikely, then it would be purely accidental. However, if such an effect was probable or even
possible, then the situation would not be the same. The law of neutrality is very strict in its prohibition of any violation of neutral territory. As Article 1 of the 1907 Hague Convention V puts it, “the territory of neutral Powers is inviolable.” The fact that military operations must not adversely affect neutral territory is further reflected in the traditional rule that a blockade must not bar access to the ports and coasts of neutral States.\(^4\)

State practice also indicates that all due precautions must be taken by belligerents to avoid any, even collateral, damage to neutral States. During the Second World War, US bombers unintentionally damaged a Swiss border town on April 1, 1944. Not only did Switzerland protest, but the US government also recognized that due precautions had not been taken, formally apologized for the incident, and promptly paid four million dollars in reparations. The US then issued directives prohibiting bombings within 50 miles of Switzerland.\(^4\)

Such a clear and strict approach means that a computer network attack that could well have an adverse effect on neutral territory would be a violation of international law.

**Conclusions and Further Considerations on Possible Future Legal Developments**

It is clear that CNA could only be undertaken to the degree and in a fashion that would respect existing law. Certain uses would probably be not only violations of the law of armed conflict, but also amount to war crimes, in which case the individuals involved would be subject to punishment both at the national and international levels within the context of applicable international law. It should also not be forgotten that such breaches require payment of compensation, especially in the context of international armed conflicts, where compensation is a long-standing requirement.\(^4\) In addition, the trend towards requiring reparation to be made to victims of international crimes is reflected in Article 75 of the Statute of the International Criminal Court.

In addition to these considerations, further steps deserve careful consideration. First, some thought needs to be given, after technical analysis, as to whether certain types of actions (for example, the introduction of worm viruses) would be inherently indiscriminate. If so, in principle they would automatically be illegal weapons\(^4\) and ought to be formally banned as such. This is probably the reasoning behind part of paragraph 3 of the draft Russian resolution (that was presented to the First Committee of the 1998 General Assembly):
Invites all Member States to inform the Secretary-general of their views and assessments concerning . . . :

advisability of developing international legal regimes to prohibit the development, production or use of particularly dangerous forms of information weapons . . . .

This suggestion was not accepted by the United States which took the position that: "it is premature at this point to discuss negotiating an international agreement on information warfare" and that "there seems to be no particularly good reason for the United States to support negotiations for new treaty obligations in most of the areas of international law that are directly relevant to information operations." The resolution finally adopted, therefore, does not contain this proposal, but this does not make such a suggestion any less valid.

Second, given that there does appear to be more support for the idea of international cooperation to suppress unwelcome private actions, there may well be a move towards creating universal jurisdiction for the punishment of certain hackers, either on the basis of permissive universal jurisdiction (based on the model of the customary law relating to piracy and most war crimes), or of compulsory universal jurisdiction (such as that created by treaty for grave breaches, torture, and certain types of terrorist acts). Even if universal jurisdiction as such is not created, it is likely that there will be arrangements to facilitate the extradition and punishment of such offenders.

Finally, a careful policy evaluation ought to be made as to the advantages and disadvantages of embarking on computer network attacks. On the one hand, if military advantages can be gained through this method which not only respect existing law but also reduce physical damage and casualties, then this would be a definite "plus." On the other hand, computer network attacks do have the potential to seriously mess up a wonderful new human achievement. In this regard, the most technologically advanced societies would be the most at risk. These anxieties are clearly reflected in the preambular paragraphs of the two General Assembly resolutions adopted in 1998 and 1999, which are virtually identical. The operative paragraphs in effect only call on States to think about existing threats and what could be done about them, in particular the "Advisability of developing international principles that would enhance the security of global information and telecommunications systems and help to combat information terrorism and criminality." The fact that military applications are possible is recognized in the first preambular paragraph which does not exclude as such this use but goes on the say that it is important to maintain and encourage civilian use. The policy question remains, therefore, "is CNA worth it?" Or would it be
more intelligent to outlaw this form of warfare before serious damage begins? It is hoped that we will not just "wait and see!"

Notes

* This chapter reflects the personal views of the author and in no way engages the responsibility of the International Commission of Jurists.

1. These terms are generally accepted as being interchangeable. Some might question whether aspects of the law of neutrality that are more concerned with the protection of the sovereign territory of neutral nations than humanitarian aspects could be properly characterised as "international humanitarian law." However, dividing up neutrality law for the purpose of making such a distinction would be awkward and unnecessary.

2. The ICRC Commentary to Article 2 of all four Geneva Conventions states that:

Any 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. ... It makes no difference how long the conflict lasts, or how much slaughter takes place. The respect due to the human person as such is not measured by the number of victims.

The ICRC Commentary to Geneva Convention Article 6, elaborates further:

By using the words "from the outset of the conflict" the authors of the Convention wished to show that it became applicable as soon as the first acts of violence were committed, even if the armed struggle did not continue. Nor is it necessary for there to have been many victims. Mere frontier incidents may make the Convention applicable, for they may be the beginning of a more widespread conflict.

3. Id. at 59. Lieutenant Goodman, shot down by the Syrians on December 4, 1983, was held for one month, during which he was visited by the ICRC "in accordance with standard criteria" on the basis that the incident did amount to an armed conflict, albeit very short. 1983 ICRC ANNUAL REPORT 63.


6. Declaration (IV, 1) to Prohibit, for the Term of Five Years, the Launching of Projectiles and Explosives from Balloons and other Methods of Similar Nature, July 29, 1899, 1 AMERICAN JOURNAL OF INTERNATIONAL LAW 153 (Supp., 1907). See also, DAVID H.N. JOHNSON, RIGHTS IN AIR SPACE, 1965:

It was to the Disarmament Conference in 1932 that the French Government submitted, in addition to a proposal to prohibit air attacks against civilians and indeed to abolish bombardment from the air altogether, a plan for the internationalisation of civil air transport under a regime organised by the League of Nations. The proposal came to nothing. (p. 38) ... At the Disarmament Conference in 1932 four various proposals were put forward for the abolition of bombing, and even of air forces; but these came to nothing. (p. 45).

During discussions on the problem of aerial bombardment during this period, the ICRC also indicated its view that a total prohibition of bombardment from the air would be the best solution to protect civilians:
Le Comité international estime que la seule manière de mettre les populations civiles à l'abri de certains des plus graves périls créés par l'état de guerre est l'interdiction pure et simple du bombardement aérien. . . . Il adresse dans ce sens un appel pressant à la Conférence.


7. A notable failed attempt was the drafting of the “Rules concerning the control of wireless telegraphy in time of war and air warfare” by a Commission of Jurists at The Hague, December 1922–February 1923 (see esp. arts. 22–24) [herein after Draft Resolution]. This Commission was constituted in accordance with a resolution of the Washington Conference (1922) on the limitation of armaments. These rules were never codified. Johnson (supra note 6, at 53) quotes military commanders as saying, in short, that in the past towns would have been besieged to win wars, which caused much more suffering than air raids during the Second World War. Johnson, who wrote in 1965, and therefore before negotiations for Additional Protocols to the Geneva Conventions, refers to Professor Georg Schwarzenberger, who concluded that under modern conditions the standard of civilisation has retreated before the necessities of war, that the traditional distinction between combatants and non-combatants has largely disappeared and that the only persons who may still expect immunity from acts of warfare are persons who are both unconnected with military operations or the production of war materials and reside in areas that are ‘sufficiently remote’ from likely target areas.


9. Article 52(2), which reads as follows:

In so far as objects are concerned, 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 neutralisation, in the circumstances ruling at the time, offers a definite military advantage.

10. This Protocol, adopted on March 26, 1999, repeats the same definition. The States that supported this definition as the appropriate one to use in the new Protocol, because of its articulation in Additional Protocol I, were the United States, India, Turkey, France and Israel.


12. Convention (IV) Relative to the Protection of Civilian Persons in Time of War, August 12, 1949, art. 14, 6 U.S.T. 3516, 75 U.N.T.S. 287 [hereinafter GC IV]. GC IV relates to hospital and safety zones and localities. A hospital zone or locality is generally of a permanent character and is established outside the combat zone in order to shelter military or civilian wounded and sick from long range weapons, especially aerial bombardment. A safety zone or locality is generally of a permanent character and is established outside the combat zone in order to shelter certain categories of the civilian population, which, owing to their weakness, require special protection.
(children, elderly people, expectant mothers, etc.) from long-range weapons, especially aerial bombardment. Article 15, GC IV, relates to neutralized zones, that are generally of a temporary character and are established in the actual combat zone to protect both combatant and non-combatant wounded and sick, as well as all members of the civilian population who are in the area and not taking part in the hostilities, from military operations in the neighborhood.

13. Convention for the Protection of Cultural Property in the Event of Armed Conflict, May 14, 1954, 249 U.N.T.S. 240. Article 2 states that the protection of cultural property shall comprise the safeguarding of and respect for such property. Article 3 states that the High Contracting Parties undertake to prepare in time of peace for the safeguarding of cultural property situated within their own territory against the foreseeable effects of an armed conflict, by taking such measures as they consider appropriate. Article 8, relating to Special Protection, makes it clear that this protection can only be given if the special shelters that are created or the monuments to be listed in a special list are not in any industrial center nor near any military objective, including communications lines. This restriction, which reflects the old system, has been remedied in the new Protocol II of the 1954 Convention, adopted in 1999, which reflects the new reasoning and therefore does not repeat these restrictions for property under “enhanced protection.”


15. Which reads as follows:

Indiscriminate attacks are: (a) those which are not directed at a specific military objective; (b) those which employ a method or means of combat which cannot be directed at a specific military objective; or (c) those which employ a method or means of combat the effects of which cannot be limited as required by this Protocol; and consequently, in each such case, are of a nature to strike military objectives and civilians or civilian objects without distinction.

Paragraph 5 refers to two other situations “to be considered as indiscriminate.” In this author’s view they are not, strictly speaking, indiscriminate, but rather behaviors that are outlawed for specific reasons. Paragraph 5(a) refers in effect to target area bombardments which deliberately treat as one target clearly separated and distinct military objectives even though civilians lie between them. This behavior is correctly outlawed because, in this author’s view, it amounts to a deliberate targeting of civilians, i.e., those in between the military objectives. Paragraph (b) represents the customary rule that incidental damage (i.e., damage that is inevitable or likely, but not in itself intended) during attack may not violate the rule of proportionality. Once again, this is not really a description of an “indiscriminate” attack, but rather a prohibition on attacks on military objectives that, although as well aimed as possible, are still likely to create more civilian damage than the objective is worth. It is for this reason that the issue of proportionality is treated in the next section of this article.


of the Persian Gulf War, 31 INTERNATIONAL LEGAL MATERIALS 612, 626 (1992), in which reference is made to the decision not to attack two fighter aircraft next to the ancient temple of Ur:

Commander in Chief Central Command . . . elected not to attack the aircraft on the basis of respect for cultural property and the belief that positioning of the aircraft . . . effectively had placed each out to action, thereby limiting the value of their destruction . . . when weighed against the risk of damage to the temple.

Otherwise the same report refers rather vaguely to military targets not being attacked because of the risk to civilian persons or property:

Coalition forces also chose not to attack many military targets in populated areas or in or adjacent to cultural . . . sites, even though attack of those military targets is authorised by the law of war.

Id. at 624.

18. Several countries have made interpretative declarations concerning Article 51(5)(b) of Additional Protocol I (1977) that references to the "military advantage" are intended to mean the advantage anticipated from the military attack considered as a whole and not only from isolated or particular parts of that attack. See, e.g., declarations upon ratification by Australia (June 21, 1991), Canada (November 20, 1990), Italy (February 27, 1986), the Netherlands (June 26, 1986), and the United Kingdom (January 28, 1998).

19 There are different views as to whether, and if so what, other ends can be justified as needs of self-defence. This chapter does not intend to go into this issue.

20. See, in particular, an analysis of this question in the ICRC document on Elements of Crimes prepared for the Preparatory Commission for the International Criminal Court, UN Doc. PCNICC/1999/WGEC/INF.2/Add.1 at 29–32.

21. Unless, of course, the perpetrator were to be indicted as a war criminal under this rule. The fact that he or she was aware that an evaluation of likely results was not even possible would be an interesting test case, as Article 85(3)(b) of Protocol I and the ICC Statute both indicate that the accused needed to have knowledge of the extent of the civilian damage that would be caused.

22. They are spelled out in Article 57 of Protocol I

23. This is spelled out in Article 57(2)(b) of Protocol I

24. It is somewhat ironic that the most accurate intelligence, which is the best way to restrict attacks to clearly identified military objectives, is probably that collected directly by undercover agents. However, the price to be paid is that spies are not entitled to prisoner-of-war status. One could wonder whether this very long-standing custom is still appropriate.

25. See, e.g., LASSA OPPENHEIM, II INTERNATIONAL LAW 429 (Hersch Lauterpacht ed., 1952), which offers the following examples: "the watchword of the enemy may be used, deceitful intelligence may be disseminated, the signals and bugle calls of the enemy may be mimicked to mislead his forces.”

26. Id.

27. Id. and art. 37 of Protocol I.

28. Interpretative declarations upon ratification of Additional Protocol I (1977) by Australia (June 21, 1991), Belgium (May 20, 1986), Canada (November 20, 1990), Germany (February 14, 1991), Ireland (May 19, 1999), Republic of Korea (January 15, 1982), and United Kingdom (January 28, 1998) state that the situation described in the second sentence of paragraph 3 of Article 44 can exist only in occupied territory or in armed conflicts covered by paragraph 4 of Article 1. The interpretative declarations by Italy (February 27, 1986) and Spain (April 21, 1989) state that the situation described in the second sentence of paragraph 3 of Article 44 can exist only in occupied territory.

183
29. Which reads as follows:

Prisoners of War, in the sense of the present Convention, are persons belonging to one of the following categories, who have fallen into the power of the enemy: . . . Persons who accompany the armed forces without actually being members thereof, such as civilian members of military aircraft crews, war correspondents, supply contractors, members of labour units or of services responsible for the welfare of the armed forces, provided that they have received authorisation from the armed forces which they accompany, who shall provide them for that purpose with an identity card . . .

30. Article 51(3) of Protocol I, which represents long-standing customary law.

31. See arts. 29 and 31 of the Hague Regulations and art. 46(3) & (4) of Protocol I.

32. Discussions on this issue took place during one of the meetings of experts (Geneva 1993) that led to the SAN REMO MANUAL ON INTERNATIONAL LAW APPLICABLE TO ARMED CONFLICTS AT SEA (text and commentary published by Cambridge University Press, 1995) [hereinafter SAN REMO MANUAL]. Two papers were prepared on this issue, one by Wolff Heintschel von Heinegg entitled “Neutrality and Non-Belligerency” and the other by Dietrich Schindler on “Neutrality and Non-Belligerency in Armed Conflicts at Sea” (filed in the ICRC Archives). Both reach the conclusion that there is no such legal difference and the Manual treats equally all States not taking part in the conflict as “neutral.” Reference is also made to this idea, but likewise rejected, in III ENCYCLOPAEDIA OF PUBLIC INTERNATIONAL LAW 552 (Jan Mayen ed., 1997).

33. In particular: G.A. Res. 1721(1961) and 1962 (1963); the 1967 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies; the 1972 Convention on International Liability for Damage Caused by Space Objects; the 1979 Agreement Governing the Activities of States on the Moon and Other Celestial Bodies; and the various telecommunications INTELSAT agreements

34. OPPENHEIM, supra note 25, at 654–655 (para. 294).


36. OPPENHEIM, supra note 25, at 656 (para. 296).

37. Id., at 659 (pars. 296a and 297).

38. GREEN, supra note 35, at 262–63.

39. OPPENHEIM, supra note 25, at 675–76 (para. 316). See also, art. 9, Hague Convention XIII of 1907.

40. Oppenheim stresses over and over again the right of neutral States to continue their commerce with belligerents. See, e.g., 674 (pars. 314 and 315), 675 (para. 316), 676 (para. 318), and 677 (para. 319).

41. This issue was hotly debated during the discussions leading to the San Remo Manual on International Law Applicable to Armed Conflict at Sea (supra note 32). The result in Paragraph 22 is more restrictive than the traditional right of self-help in such a circumstance.

42. Art. IV.

43. Art. III.
44. SAN REMO MANUAL, supra note 32, para. 99, which reflects art. 18 of the 1909 London Declaration. During the drafting of the San Remo Manual, this provision was totally uncontested.


Le profond regret de tous les Américains pour le tragique bombardement par les bombardiers américains de la ville suisse de Schaffhouse le 1er avril ... un groupe de bombardiers ... n'ont pas pris les larges precautions prevues pour eviter des incidents de ce genre ... Le Secrétaire de la Guerre ... a demandé en même temps au Secrétaire d'Etat d'assurer votre Gouvernement que toutes précautions seront prises pour prévenir autant qu'il est humainement possible la répétition de pareil malheureux accident.

15 DOCUMENTS DIPLOMATIQUES SUISSES 1848–1945, at 315.

46. 1907 Hague Convention IV, art. 3, repeated in Additional Protocol I, art. 91.

47. See, e.g., the articulation of basic rules of IHL in the Advisory Opinion of the International Court of Justice on the Legality of the Threat or Use of Nuclear Weapons, para. 95, July 8, 1996: “Thus, methods or means of warfare, which would preclude any distinction between civilian and military targets ... are prohibited.”


49. Office of the General Counsel, Department of Defense, An Assessment of International Legal Issues in Information Operations (Nov. 1999) [hereinafter DoD/GC Paper]. The paper is appended to this volume as the Appendix.

50. G.A. Res. 53/70 (Jan. 4, 1999), Developments in the field of information and telecommunications in the context of international security, UN Doc. A/RES/53/70.

51. E.g., “current U.S. efforts to improve mutual legal assistance and extradition agreements should continue to receive strong emphasis. Another idea that might prove fruitful is to negotiate a treaty to suppress information terrorism...” DoD/GC Paper, supra note 49, at Appendix. This thought is also reflected in the final preambular paragraph of the resolution adopted (note 51): “Considering that it is necessary to prevent the misuse or exploitation of information resources or technologies for criminal or terrorist purposes.” This provision is repeated in a resolution of the same name adopted the following year, UN Doc. A/54/558 which is essentially the same as the previous one, G.A. Res. 54/49 (Dec. 1, 1999) UN Doc. A/54/558.

52. See supra notes 9 & 51. Paragraphs 2, 3, and 7 of the 1999 resolution read as follows:

Noting that considerable progress has been achieved in developing and applying the latest information technologies and means of communication;

Affirming that it sees in this process the broadest positive opportunities for the further development of civilisation, the expansion of opportunities for co-operation for the common good of all States, the enhancement of the creative potential of mankind, and additional improvements in the circulation of information in the global community;

Expressing concern that these technologies and means can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the security of States.

53. Id., both resolutions operative para. 2(c).