

VII

Computer Network Attacks and Self-Defense

Yoram Dinstein

Armed Attack and Self-Defense

The general prohibition of the use of force in the relations between States constitutes the cornerstone of modern international law.¹ It is currently embedded both in the Charter of the United Nations [Article 2(4)²] and in customary international law (which has consolidated under the impact of the Charter).³ Indeed, the International Law Commission has identified the prohibition of the use of inter-State force as “a conspicuous example” of *jus cogens*⁴ (i.e., a peremptory norm of general international law from which no derogation is permitted⁵). The Commission’s position was cited by the International Court of Justice in the *Nicaragua* case of 1986,⁶ and in two Separate Opinions the peremptory nature of the proscription of the use of inter-State force was explicitly emphasized.⁷

The correct interpretation of Article 2(4) of the Charter subsequent to the *Nicaragua* Judgment is that there exists in international law today “an absolute prohibition of the use or threat of force, subject only to the exceptions stated in the Charter itself.”⁸ The only two exceptions spelled out in the Charter are collective security pursuant to a Security Council decision (by virtue especially of Article 42⁹) and individual or collective self-defense (consistent with

Article 51¹⁰). This chapter will focus on self-defense, namely, forcible counter-measures put in motion by States acting on their own (individually or collectively), in the absence of a binding Security Council decision obligating or authorizing them to behave in such a fashion.

In accordance with Article 51 of the Charter, the right of self-defense can only be invoked in response to an "armed attack." The choice of words in Article 51 is deliberately restrictive. The phrase "armed attack" is not equivalent to "aggression" (a much broader and looser term, used, e.g., in Article 39 pertaining to the powers of the Security Council¹¹). An armed attack is actually a particular type of aggression. This is borne out by the French text, which speaks of "*une agression armée*." The expression "armed attack" denotes the illegal use of armed force (i.e., recourse to violence) against a State.

For an illegal use of force to acquire the dimensions of an armed attack, a minimal threshold has to be reached. Since Article 2(4) of the Charter forbids "use of force" and Article 51 allows taking self-defense measures only against an "armed attack," a gap is discernible between the two stipulations.¹² The gap is due to the fact that an illegal use of force not tantamount to an armed attack may be launched by one State against another, but then (in the absence of an armed attack) self-defense is not an option available to the victim. Logically and pragmatically, the gap has to be quite narrow, inasmuch as "there is very little effective protection against states violating the prohibition of the use of force, as long as they do not resort to an armed attack."¹³ If a victim State is barred from responding with counter-force to force, this ought to be confined to the sphere of application of the ancient apothegm *de minimis non curat lex*. In other words, all that the gap conveys is that the illicit use of force has to be of sufficient gravity.¹⁴ When the use of force is trivial—say, a few stray bullets are fired across a frontier—no armed attack can be alleged to have occurred.¹⁵ In that case, there is no room for forcible counter-measures of self-defense.¹⁶ By contrast, when the use of force is of sufficient gravity, an armed attack is in progress even if it is characterized by small magnitude. *Au fond*, whenever a lethal result to human beings—or serious destruction to property—is engendered by an illegal use of force by State A against State B, that use of force will qualify as an armed attack. The right to employ counter-force in self-defense against State A can then be invoked by State B (and, as we shall see *infra*, also by State C).

To better understand the legal position, it is necessary to distinguish between an armed attack, on the one hand, and an ordinary breach of international law—or even a mere unfriendly act—on the other.

State A can commit an unfriendly act against State B without thereby being in breach of any binding norm of international law. Such unfriendly conduct by

State A is liable to upset State B. It may cause the latter psychological embarrassment or even material harm in the political, diplomatic, or economic arena. Yet, as long as no breach of international law is committed, State B does not possess any legal standing (*jus standi*) for objecting to the conduct of State A.

Acts that may highlight the phenomenon of unfriendly acts, carrying with them no connotations of infringement by State A of international law, are: (i) refusal to permit an official visit of State A by the Head of State B;¹⁷ (ii) a notification that a member of the diplomatic staff of State B accredited to State A is *persona non grata*;¹⁸ (iii) the prohibition of the import of certain goods from State B into State A (absent treaty commitments to the contrary);¹⁹ and (iv) espionage carried out by clandestine agents of State A.²⁰ The fact that, strictly speaking, all these activities—and similar ones in the same vein—are legal (albeit unfriendly) does not mean that State B is completely helpless in terms of potential response. State B may opt to indulge in “retorsion” by taking equally legal yet unfriendly steps (such as a reciprocal expulsion of diplomats sent by State A).²¹

A breach of international law transcends unfriendliness, crossing the red line of illegality. If State A ignores the immunity from local jurisdiction enjoyed by duly accredited diplomatic agents of State B;²² if State A’s trawlers fish in the exclusive economic zone off the coast of State B;²³ if State A fails to extradite a fugitive from State B notwithstanding clear-cut obligations in a treaty concluded by them—State A will bear international legal responsibility vis-à-vis State B. In keeping with the international law of State responsibility, “[t]he injured State is entitled to obtain from the State which has committed an internationally wrongful act full reparation in the form of restitution in kind, compensation, satisfaction, and assurances and guarantees of non-repetition, either singly or in combination.”²⁴

Seeking reparation, State B—as the injured party—may present a legal claim against State A before any international court or tribunal which may be vested with jurisdiction over the dispute. Alternative avenues are also open. State B is always free to bring the dispute with State A to the attention of the Security Council [under Article 35(1) of the Charter²⁵]. The Council may then recommend appropriate methods of adjustment [pursuant to Article 36(1)²⁶] or even determine the existence of a threat to the peace (in compliance with the above-mentioned Article 39).²⁷ Acting on its own, State B may also apply non-forcible reprisals against State A²⁸ (e.g., by declining to extradite a fugitive from State A under the same treaty provision). A reprisal differs from retorsion in that the act in question (non-extradition) would have been illegal—in light of the treaty obligations postulated—but for the prior illegal act of State A.²⁹ Whichever channel of response is chosen by State B against State A, the

quintessential point is that, as a rule, the fact that State A incurs international responsibility towards State B does not create for State B a legitimate option to initiate force against State A. Even an ordinary violation of the UN Charter itself does not excuse response by force.

The only time—consistent with the Charter—when State B (without acting at the behest of the Security Council) may lawfully wield force against State A, in response to an illegal act by State A, is when that illegal act amounts to an armed attack and the counter-measures can be appropriately subsumed under the heading of self-defense.

Computer Network Attacks (CNAs)

The scientific and technological revolution, which has rendered the computer ubiquitous, has also “changed the scope and pace of battle.”³⁰ This is evident to all where the computer serves as an instrument of command, control, communications, and intelligence (not to mention simulation, surveillance, sensors, and innumerable other military purposes). But the modern computer can also become a weapon in itself by being aligned for attack against other computer systems serving the adversary. A “computer network attack” (CNA) can occur either in wartime—in the midst of on-going hostilities—or in peacetime. The former situation is governed by the *jus in bello* and does not come within the scope of the present paper. The question to be analyzed here is the latter. More specifically, the fulcrum of our discussion is whether a CNA mounted in peacetime may be categorized as an armed attack, thus justifying forcible counter-measures of self-defense in compliance with the *jus ad bellum*.

A CNA is often defined inadequately as disrupting, denying, degrading, or destroying either information resident in a computer network or the network itself.³¹ This definition is rooted in a presupposition that a CNA is no more than a device to counter the antagonist’s electronic capabilities. Had the definition been legally binding—or had it factually mirrored the whole gamut of the technical capabilities of the computer—the likelihood of a CNA ever constituting a full-fledged armed attack would be scant. However, whereas CNAs recorded heretofore have admittedly been circumscribed to operations of intrusion and disruption, it would be extremely imprudent to extrapolate current restraints into the years ahead. A credible forecasting of future developments must start from the indisputable premise that potential CNAs (by feeding false messages into a target computer system) may also encompass grievous sabotage, designed to leave behind a trail of death and devastation through induced explosions and other malicious “malfunctions.”³²

The determination whether or not an armed attack has taken place—so as to justify response by way of self-defense—does not necessarily depend on the choice of weapons by the attacking party. The International Court of Justice aptly commented, in the *Nuclear Weapons* Advisory Opinion of 1996, that the provision of Article 51 does not refer to specific weapons; it applies to any armed attack, regardless of the weapon employed.³³ Of course, the detonation of weapons of mass destruction (say, nuclear warheads) makes it easier to stigmatize the strike as an armed attack. Still, what counts is not the specific type of ordnance, but the end product of its delivery to a selected objective. After all, even unsophisticated pernicious tools—like the poisoning of wells in a desert area—may give rise to exceedingly grave results.

From a legal perspective, there is no reason to differentiate between kinetic and electronic means of attack. A premeditated destructive CNA can qualify as an armed attack just as much as a kinetic attack bringing about the same—or similar—results. The crux of the matter is not the medium at hand (a computer server in lieu of, say, an artillery battery),³⁴ but the violent consequences of the action taken. If there is a cause and effect chain between the CNA and these violent consequences, it is immaterial that they were produced by high rather than low technology.

When a CNA emanates from within the territory of the same country in which the target is located (assuming that no foreign State is involved in the operation and no attempt is made to route the attack through a conduit abroad), this is a matter that in principle can—and should—be regulated by the domestic law of that country. Generally speaking, subject to few exceptions (see the next section), international law comes into play only at a point when the CNA turns into a cross-border operation.

Even in a cross-border scenario, CNAs are not all of the same nature. It is necessary to distinguish between four discrete rubrics of CNAs originating from State A and directed against State B, depending on whether they are unleashed by: (i) individual computer hackers who are residents of State A, acting on their own initiative for whatever personal motive (benign or otherwise) without any linkage to the government of State A; (ii) terrorists³⁵ based in State A, acting on behalf of any chosen “cause” inimical to State B, unsupported by the government of State A; (iii) terrorists overtly or covertly sponsored by the government of State A; and (iv) official organs—either military or civilian—of the government of State A.

The first two categories usually call for coercive action by the proper authorities of State A itself, with a view to precluding or terminating hostile acts conducted from within its territory by hackers or terrorists against State B. The

International Court of Justice proclaimed, in the *Corfu Channel* case of 1949, that every State is under an obligation “not to allow knowingly its territory to be used for acts contrary to the rights of other States.”³⁶ In implementing this international obligation, State A should take resolute steps to suppress the perpetration of hostile activities from within its territory against State B—optimally by preventing these acts from materializing, but minimally by prosecuting offenders after the acts have already been committed. If the government of State A fails to do what it is supposed to, State B (as we shall see *infra*) can take certain exceptional counter-measures unilaterally.

When terrorists are sponsored by State A, they may be deemed “*de facto* organs” of that State.³⁷ “[T]he imputability to a State of a terrorist act is unquestionable if evidence is provided that the author of such act was a State organ acting in that capacity.”³⁸ When State A chooses to operate against State B at one remove—pulling the strings of a terrorist organization (not formally associated with the governmental apparatus), rather than activating its regular armed forces—this does not diminish one iota from the full international responsibility of State A for the acts taken and their consequences, provided that “it is established” that the terrorists were “in fact acting on behalf of that State.”³⁹

The International Court of Justice, in the *Nicaragua* case of 1986, explicitly held that an armed attack encompasses not only action by regular armed forces but also the employment of “irregulars.”⁴⁰ Granted, not every detail in this delicate area is universally agreed upon. The majority of the Court in the *Nicaragua* Judgment added that the mere supply of arms (or providing logistical and other support) to armed bands cannot be equated with armed attack,⁴¹ whereas Judges Schwebel and Jennings sharply dissented on this point.⁴² Be it as it may, there is a consensus that when State A goes beyond logistical support and dispatches a terrorist group to do its bidding against State B, State B can invoke self-defense against State A.

In 1999, the Appeals Chamber of the International Criminal Tribunal for the Former Yugoslavia pronounced, in the *Tadić* case, that acts performed by members of a military or paramilitary group organized by a State “may be regarded as acts of *de facto* State organs regardless of any specific instruction by the controlling State concerning the commission of each of those acts.”⁴³ The Tribunal concentrated on the subordination of the group to overall control by the State. It opined that the State does not have to issue specific instructions for the direction of every individual operation, nor does it have to choose concrete targets.⁴⁴ Terrorists can thus act quite autonomously and still stay *de facto* organs of the controlling State.

The most crucial flow of events stems from a CNA undertaken overtly by official government organs. The intrusion of the organs of State A into the computer systems of State B may have a whole range of purposes and outcomes, for instance:

- (i) Espionage. As indicated *supra*, espionage activities conducted by clandestine agents are merely unfriendly acts. In singular circumstances, official espionage is openly acknowledged by a State;⁴⁵ the question whether the act can then be viewed as a violation of international law is debatable.⁴⁶ In any event, espionage per se does not constitute an armed attack.
- (ii) Disruption of communications and digitized services through the induced failure of computer systems, without causing human casualties or significant destruction of property. This is a CNA, but since the act (whether merely unfriendly or a transgression of international law) does not entail sufficiently grave consequences, the conclusion is the same.
- (iii) Fatalities caused by loss of computer-controlled life-support systems; an extensive power grid outage (electricity blackout) creating considerable deleterious repercussions; a shutdown of computers controlling waterworks and dams, generating thereby floods of inhabited areas; deadly crashes deliberately engineered (e.g., through misinformation fed into aircraft computers), etc. The most egregious case is the wanton instigation of a core-meltdown of a reactor in a nuclear power plant, leading to the release of radioactive materials that can result in countless casualties if the neighboring areas are densely populated.⁴⁷ In all these cases, the CNA would be deemed an armed attack.

A salient point is that an excessive computer dependency creates a special vulnerability.⁴⁸ The more technologically advanced—and, therefore, computer reliant—a State is, the more susceptible it is to a paralyzing CNA. Overall, State A may be less developed scientifically and technologically than State B.⁴⁹ Yet, the very advantage of State B becomes a debilitating burden once State A manages to penetrate State B's electronic defenses. This, writ large, is the scenario of a nuclear core meltdown. Through a CNA, State A—having no nuclear capability of its own—can in a sense “go nuclear” by exploiting the scientific and technological infrastructure of State B, thus turning the tables on the target State. State B, as it were, provides the nuclear weapon against itself (the weapon being triggered by agents of State A).

CNAs against Private Individuals and Corporations

It must be appreciated that a computer system subjected to a CNA by State A need not belong to the government, or even to any semi-governmental agency, of State B. An attack may be carried out, e.g., inside US territory (or, for that matter, vessels flying the American flag and aircraft registered in the US) against a computer system operated by either a private individual or a non-governmental entity. The American situation is perhaps the most acute, inasmuch as public utilities in the US are privately owned, and, indeed, corporate America is the principal manufacturer of military equipment, naval platforms, and aircraft serving the American armed forces. But anyhow, it is immaterial whether the civilian computer system under attack is operated by a civilian supplier or sub-contractor of the Department of Defense. Even if the CNA impinges upon a civilian computer system which has no nexus to the military establishment (like a private hospital installation), a devastating impact would vouchsafe the classification of the act as an armed attack. There is no immanent difference between a CNA and a kinetic attack targeting ordinary civilian objects within the territory of State B. Needless to say, the bombing by State A of, e.g., an urban population center (apart from being unlawful per se under international humanitarian law, by not being directed against a military objective⁵⁰) constitutes an armed attack, albeit not a single member of the armed forces of State B is injured in the air-raid. The same rule is applicable to a CNA.

Furthermore, a CNA—just like a kinetic use of force—by State A would qualify as an armed attack against State B even if the computer system inside the territory of State B (including its vessels and aircraft) is operated by an individual or a private corporation possessing the nationality of State C. A corporation, on an analogy with an individual, has a distinct nationality (that of the State under the laws of which it was incorporated and in whose territory it has its registered office).⁵¹ But the foreign nationality of the corporate or individual operator of the computer system under attack is irrelevant from the perspective of State B, as long as the CNA is carried out within its territory.

What happens when a CNA is inflicted by State A outside the territory of State B, but it affects a computer system operated by State B or one of its nationals (individual or corporate)? It goes without saying that a lethal kinetic strike against a governmental installation of State B stationed outside its territory, vessels, and aircraft—such as an embassy of State B in the capital city of State C (or even State A)—will be deemed an armed attack against State B, notwithstanding the geographic disconnection from its territory.⁵² This is also true of an

electronic attack against the computer system of State B's embassy in State C (or in State A) culminating with fatalities or destruction of property.

The position differs when the target of an armed attack (kinetic or electronic) by State A is situated in State C, and any injury caused to State B or to its nationals is coincidental. In such a case, State B cannot regard itself as the genuine object of the armed attack. On the other hand, if a destructive CNA is launched by State A within the territorial boundaries of State C (or even State A) against a computer system operated privately by nationals (individual or corporate) of State B—and the target is specifically selected on account of that nationality—State B is entitled to consider the act an armed attack against itself. Thus, if an explosion-inducing CNA strikes a computer operated by US citizens across the ocean—and this is plainly done not at random but because of the American nationality of the operators—the act may be deemed an armed attack against the US (although perpetrated abroad). There are many instances in international relations in which nationals attacked abroad by State A have been protected or rescued by State B in the name of self-defense.⁵³ This is perfectly legitimate, provided that the attack occurred owing to the bond of nationality existing between the victims and State B.⁵⁴ Once more, there is no difference here between an electronic and a kinetic attack.

Self-Defense Responses to CNAs

Just as there are variable settings for the commission of an armed attack by State A in the form of a CNA, there are also several possible responses available to State B in the exercise of its right of self-defense. The most obvious response is “on-the-spot reaction,”⁵⁵ where the computer network under attack strikes instantaneously back at the source of the CNA. The trouble, however, is that frequently the server which is seemingly the source of the CNA has only been manipulated by the true assailants (who have routed their attack through it), and swift responsive counter-measures against the intermediary conduit is liable to be counterproductive, as well as unlawful.⁵⁶ Establishing the genuine identity of the attacker—and attributing the act to the real (as distinct from apparent) actor—is a major challenge in the present stage of technological development (see discussion *infra*).

On the whole, the most effective modality of self-defense against an armed attack in the shape of a CNA is recourse to defensive armed reprisals, to wit, forcible counter-measures undertaken at a different time and place. Armed reprisals as such are generally “considered to be unlawful” in peacetime.⁵⁷ But there is no reason why armed reprisals cannot come within the framework of self-defense

under the Charter. Armed reprisals can constitute a legitimate response to an armed attack within the ambit of Article 51, provided that they are genuinely defensive, namely, future-oriented (deterrent in character) and not past-oriented (confined to punitive retaliation).⁵⁸ State practice definitely shows that defensive armed reprisals are part and parcel of the arsenal of States subjected to armed attacks.⁵⁹ Indeed, falling back on defensive armed reprisals has certain built-in advantages. Above all, it gives State B an opportunity to review the facts (and determine culpability) while considering options for response.

It should be borne in mind that defensive armed reprisals against a CNA can be performed kinetically even though the original armed attack (justifying them) was executed electronically, and vice versa. Again, whatever is permitted (or prohibited) when kinetic means of warfare are used is equally permitted (or prohibited) when the means employed are electronic; the rules of international law are the same whatever the means selected for attack.

The ultimate type of force stimulated by self-defense may amount to (or may result in) war.⁶⁰ In the setting of CNAs, the outbreak of war as a counter-measure of self-defense would be rare. Due to the conditions precedent to the waging of war as an exercise of self-defense (see discussion *infra*), war would constitute a proper response to a CNA only in far-fetched scenarios (such as the calculated prompting of a nuclear core meltdown).

Sometimes, State A—constrained by political or military considerations—would passively tolerate the use of its territory as a base for activities by terrorists against State B, without actively sponsoring those activities or even encouraging them.⁶¹ Such a turn of events would not cloak the terrorists with a mantle of protection from State B. “If a host country permits the use of its territory as a staging area for terrorist attacks when it could shut those operations down, and refuses requests to take action, the host government cannot expect to insulate its territory against measures of self-defense.”⁶² As already epitomized in the classical *Caroline* incident of 1837,⁶³ State B may legitimately invoke self-defense to exert counter-force within the territory of State A—targeting armed bands which use that territory as a springboard for operations against State B—when the host government remains inert. The present writer calls such a mode of self-defense “extra-territorial law enforcement,”⁶⁴ while others prefer the term “state of necessity.”⁶⁵ What counts, however, is the substance of the law and not the formal appellation. The substance of the law in this respect relates to electronic, as much as kinetic, terrorism against State B originating in State A.

The Three Conditions of Self-Defense

Three cumulative conditions to the exercise of self-defense are well-entrenched in customary international law: (i) necessity, (ii) proportionality, and (iii) immediacy. The first two conditions were articulated in the 1986 *Nicaragua* Judgment,⁶⁶ and reiterated in the 1996 *Nuclear Weapons* Advisory Opinion.⁶⁷ Immediacy, while glossed over in the Court's rendering of the law, is of equal specific weight.⁶⁸

Necessity primarily denotes "the non-existence of reasonable peaceful alternative measures."⁶⁹ Differently put, non-forcible remedies must either prove futile *in limine* or have in fact been exhausted in an unsatisfactory manner; the upshot is that there is no effective substitute for the use of force in self-defense. In the context of a CNA, it is requisite to ascertain that the CNA is no accident, to verify the genuine identity of the State—or non-State entity—conducting the attack (so as not to jeopardize innocent parties), and to conclude that the use of force as a counter-measure is indispensable. Should there be an opportunity to settle the matter amicably through negotiations, these must be conducted in good faith.⁷⁰

The second condition is chiefly relevant to defensive armed reprisals undertaken in a situation "short of war." The counter-measures taken by State B (kinetically or electronically) must not be out of proportion with the act prompting them.⁷¹ A modicum of symmetry between force and counter-force—injury inflicted on State B by the armed attack versus damage sustained by State A by dint of the self-defense counter-measures—is called for.

Since CNAs are often discharged in a cluster—and inasmuch as each one of them, when examined in isolation, may appear to have only a minor ("pin-prick") adverse effect, yet, when assessed in their totality, the results may be calamitous—the question is whether defensive armed reprisals may be undertaken in proportion to the cumulative effect of the sequence of attacks.⁷² The issue, which ordinarily arises in the face of assaults by terrorists, is not free of difficulties.⁷³ But there is some authority for the position that a State suffering from a series of small-scale attacks is permitted to respond to them aggregately in a single large-scale forcible counter-measure.⁷⁴ This would equally apply to CNAs.

The balance between the quantum of force and counter-force, which is the key to the legitimacy of defensive armed reprisals, is not germane to war as the ultimate manifestation of self-defense in response to an armed attack.⁷⁵ Once war is in progress, it may be fought to the limit (subject to the exceptions and qualifications decreed by international humanitarian law), and there is no

mandatory correspondence between the scale of force expended by the opposing sides.⁷⁶ The meaning of proportionality in the concrete circumstances of war is that the use of comprehensive counter-force in the exercise of self-defense must be warranted by the critical character of the original armed attack.⁷⁷ Once the vital justification of a war of self-defense by State B against State A is recognized, there is no additional need to ponder the defensive disposition of every single measure taken by State B. From the outset of a war of self-defense until its termination (which is not to be confused with the suspension of hostilities through a cease-fire⁷⁸), the legitimacy of every instance of the use of force by State B against State A is covered by the *jus ad bellum* (albeit not necessarily by the *jus in bello*). Admittedly, where CNAs are concerned, a war of self-defense would be vindicated as an appropriate response only in *outré* circumstances (such as the catastrophic event of a CNA-induced nuclear core meltdown).

Immediacy intrinsically suggests that the activation of self-defense counter-measures must not be too tardy. Still, this condition is construed "broadly."⁷⁹ There may be a time-lag of days, weeks, and even months between the original armed attack and the sequel of self-defense. The delay may be particularly glaring after a CNA, since in cyberspace activities can produce reverberations around the world "in the time that it takes to blink an eye."⁸⁰ Still, lapse of time is almost unavoidable when—in a desire to fulfill the letter and spirit of the condition of necessity—a slow process of diplomatic negotiations evolves, with a view to resolving the matter amicably.⁸¹

Interceptive Self-Defense

The gist of Article 51 of the Charter is that there is no legitimate self-defense *sans* an armed attack. All the same, an armed attack need not start with the opening of fire on the aggrieved party. In fact, at times, it is the victim of an armed attack who fires the first shot. For an obvious example, suffice it to postulate that military formations commissioned by State A intentionally cross the frontier of State B and then halt, positioning themselves in strategic outposts well within the territory of State B (the movement of Pakistani troops into Indian Kashmir in 1999 is a good case in point⁸²). If the invasion takes place in a region not easily accessible and lightly guarded, it is entirely conceivable that some time would pass before the competent authorities of State B grasp what has actually transpired. In these circumstances, it may very well ensue that the armed forces of State B would be instructed to dislodge from their positions the invading contingents belonging to State A, and that fire be opened first by soldiers raising the banner of State B. Nevertheless, since the international frontier has been crossed

by the military units of State A without the consent of State B, State A cannot relieve itself of responsibility for an armed attack.

As a matter of fact (and law), an armed attack may be viewed as a foregone conclusion even though no fire has been opened (as yet) and no international frontier has been crossed. Thus, hypothetically, had the Japanese aircraft en route to Pearl Harbor on December 7, 1941, been intercepted and shot down over the high seas by US air forces, Japan would still have incurred responsibility for the armed attack that triggered the Pacific War.⁸³ A more up-to-date scenario would be that of a missile site whose radar is locked on to a target in preparation for fire.⁸⁴ The linchpin question in analyzing any situation is whether the die has been cast. Resort to counter-force in the exercise of self-defense cannot be purely preventive in nature, inasmuch as threats alone do not form an armed attack. Still, if it is blatant to any unbiased observer that an armed attack is incipient or is on the verge of beginning, the intended victim need not wait impotently for the inescapable blow; the attack can legitimately be intercepted. Interceptive (in contradistinction to anticipatory) self-defense comes within the purview of permissible self-defense under the Charter. The theme of interceptive self-defense is apposite to a CNA when an intrusion from the outside into a computer network has been discovered, although, as yet, it is neither lethal to any person nor tangibly destructive of property. The issue is whether the intrusion can plausibly be construed as the first step of an inevitable armed attack, which is in the process of being staged (analogous to the detection of attack aircraft en route to their objectives). It is a matter of evaluation on the ground of the information available at the time of action (including warnings, intelligence reports, and other data), reasonably interpreted.⁸⁵

The Attribution of CNAs to a State

Reference has already been made to the problem of attribution to State A of a CNA as an armed attack for which responsibility devolves on that State. As observed, in the present state of the art, it is often by no means clear who originated the CNA. The inability to identify the attacker undermines in practice the theoretical entitlement of State B to resort to forcible counter-measures in self-defense.⁸⁶ State B must not rush headlong to hasty action predicated on reflexive impulses and unfounded suspicions; it has no choice but to withhold forcible response until hard evidence is collated and the state of affairs is clarified, lest the innocent be endangered. However, the following points should be recalled:

- (i) The same problem arises in many other situations, for instance when acts of terrorism are committed kinetically. Frequently,

either the perpetrators of the terrorist attack act anonymously—leaving no signature—or those “taking credit” are unfamiliar. Since States sponsoring terrorism usually try to conceal their role: holding such States accountable for their misdeeds may be fraught with great difficulties.⁸⁷ Prior to determining its options in combating terrorism, the victim State must establish a linkage between the terrorists and their sponsoring State.⁸⁸ CNAs invite a similar approach.

- (ii) Not always is attribution shrouded in doubt for long. In the past, wars began with bombings and bombardments. In the future, they are increasingly likely to start with CNAs. But recourse to a CNA does not mean that the enemy wishes to remain incognito indefinitely. It is within the realm of the possible that a CNA will be merely the precursor of a wave of later attacks, which will be mounted with traditional means and be easily traceable to an irrefutable source. Hence, it would be a mistake to assume that a CNA inevitably manifests an attempt at deception and perfidy. The CNA may be designed merely to achieve surprise and cause temporary havoc, without trying to hide the identity of the perpetrator for a prolonged stretch of time.
- (iii) Future advances in technology are likely to make it much easier to identify the attacker, just as current—unlike past—technology enables the immediate registration of the source of an incoming telephone call (although, patently, identification of that source does not conclusively establish which person is actually making the telephone call; the same is true of the user of a computer).

Collective Self-Defense

Pursuant to Article 51 of the Charter, collective—no less than individual—self-defense is permissible against an armed attack. The rule does not discriminate between different classes of armed attacks, and therefore it pertains *inter alia* to a CNA crossing the threshold of an armed attack. The right to collective self-defense means that any third State in the world⁸⁹ (State C) is free to join State B in bringing forcible measures to bear against State A, with a view to repelling an armed attack. The occurrence of an armed attack by State A against State B as a *conditio sine qua non* to the exercise of collective self-defense against State A by State C was underscored by the International Court of Justice in the

Nicaragua case.⁹⁰ The majority of the Court further held that State C may not exercise that right unless and until State B has first declared that it has been subjected to an armed attack by State A.⁹¹ This dictum has been cogently challenged in a dissent by Judge Jennings,⁹² but it may have some merit against the background of a CNA. Certainly, States B and C must see eye to eye on the identification of an elusive attacker. State C is enjoined from taking collective self-defense action against State A if State B (the immediate target) declines to confirm that State A is indeed accountable for a CNA constituting an armed attack.

The exercise of collective self-defense in conformity with the Charter is a right and not a duty. The right can be transformed into a duty should States B and C become contracting parties to a mutual assistance treaty or a treaty of guarantee, and *a fortiori* to a military alliance.⁹³ Thus, if State B happens to be a member of NATO, other members of the alliance are expected to extend military aid when an armed attack occurs against it (within certain geographic bounds).⁹⁴ But there is no need for a collective self-defense treaty to exist between State B and State C. State C is competent to act spontaneously—appraising events as they unfold—and it can do so whether the armed attack against State B is kinetic or electronic.

The Supervision of the Security Council

Article 51 of the Charter sets forth that the right of self-defense may be exercised until the Security Council has taken the measures necessary to maintain international peace and security. Under the article, a State invoking self-defense must immediately report to the Council what steps it has taken, and these steps do not diminish from the authority of the Council to take any action it deems necessary. As the International Court of Justice enunciated in the *Nuclear Weapons* Advisory Opinion, the “requirements of Article 51 apply whatever the means of force used in self-defence.”⁹⁵ There is thus no difference between kinetic and electronic counter-measures.

Three thorny aspects of the Security Council’s supervisory powers deserve to be mentioned. First, as a matter of fact, “[r]elatively few communications have been circulated expressly to meet the Charter obligation to report immediately to the Council on measures taken in the exercise of the right of individual or collective self-defence after an armed attack has occurred (Article 51).”⁹⁶ As a matter of law, however, a failure to report to the Security Council about engaging in self-defense against a CNA may be perilous. In its Judgment in the *Nicaragua* case, the majority of the Court implied that a State may be precluded from relying on the right of self-defense if it fails to comply with the requirement of reporting to the Council.⁹⁷ Judge Schwebel dissented, holding that the reporting

duty is a procedural matter and that therefore nonfeasance must not deprive the State concerned of its substantive cardinal right to self-defense.⁹⁸ The dissent is quite persuasive, but the majority's position cannot simply be disregarded.

Second, the Security Council's record since its inception is not such as to instill much confidence in the likelihood of its taking the necessary remedial action for the maintenance of international peace and security, thus avoiding any further need of unilateral self-defense against an armed attack. Once the Council's inaction was largely due to the Cold War and the abuse of the veto power by Permanent Members, each voting in tandem with the political interests of the bloc which it led or to which it belonged. Regrettably, even recent permutations in Big Power politics have not revived the faith in the Security Council's role as an above-the-fray arbiter of all armed conflicts in the international community.

Third, it is by no means clear what sort of resolution adopted by the Security Council would divest States of the right to embark upon unilateral use of force in self-defense against an armed attack. Surely, the Council is fully empowered to override specious claims to self-defense and adopt a legally binding decision to the effect that allegedly defensive measures must stop forthwith. But this does not mean that "any measure" adopted by the Council "would preempt self-defense."⁹⁹ Short of an explicit decree by the Council to discontinue the use of force, the State acting in self-defense retains its right to do so until the Council has taken measures which have actually "succeeded in restoring international peace and security."¹⁰⁰ Only effective measures that would not leave the victim State defenseless can terminate or suspend the exercise of the right of self-defense.¹⁰¹

Conclusion

The introduction of any new weapon into the arsenal of inter-State conflict raises first and foremost the issue of its legality. Under Article 36 of Additional Protocol I (of 1977) to the Geneva Conventions, any State adopting (or even developing) a new weapon must first determine whether or not it is prohibited by international law;¹⁰² this norm appears to reflect customary international law.¹⁰³ CNAs are not incorporated in any present list of proscribed weapons under the *lex lata*. Evidently, there is a separate issue *de lege ferenda* whether mankind would not be better off by legally banning them altogether. The dilemma will probably be debated with growing intensity as the incidence of CNAs leaves their mark on the evolution of armed conflict.

The novelty of a weapon—any weapon—always baffles statesmen and lawyers, many of whom are perplexed by technological innovations. It is perhaps natural to believe that a new weapon cannot easily intermesh with the

pre-existing international legal system. In reality, after a period of gestation, it usually dawns on belligerent parties that there is no insuperable difficulty in applying the general principles and rules of international law to the novel weapon (subject to some adjustments and adaptations, which crystallize in practice). It can scarcely be denied that, unless legally excluded in advance, CNAs are almost bound to play a pivotal role as a first-strike weapon in the commencement of future hostilities. The challenge is to study now the most efficacious means of response to this ominous prospect.

Notes

1. For a general treatment of the subject, see Y. DINSTEIN, *WAR, AGGRESSION AND SELF-DEFENCE* (3d. ed. 2001).
2. Charter of the United Nations, 1945, 9 INTERNATIONAL LEGISLATION 327, 332 (M.O. Hudson ed., 1950).
3. See the Judgment of the International Court of Justice in Military and Paramilitary Activities in and against Nicaragua (*Nicaragua v. United States.*), 1986 I.C.J. 14, 96–97 (merits).
4. Report of the International Law Commission, 18th Session, [1966] II YEARBOOK OF THE INTERNATIONAL LAW COMMISSION 172, 247.
5. Consult the text of Article 53 of the 1969 Vienna Convention on the Law of Treaties, [1969] UNITED NATIONS JURIDICAL YEARBOOK 140, 154.
6. *Nicaragua* Judgment, *supra* note 3, at 100.
7. *Id.* at 153 (President Singh), 199 (Judge Sette-Camara).
8. J. Mrazek, *Prohibition of the Use and Threat of Force: Self-Defence and Self-Help in International Law*, 27 CANADIAN YEARBOOK OF INTERNATIONAL LAW 81, 90 (1989).
9. UN CHARTER, *supra* note 2, at 343–344.
10. *Id.* at 346.
11. *Id.* at 343.
12. See A. Randelzhofer, *Article 51*, in THE CHARTER OF THE UNITED NATIONS: A COMMENTARY 661, 664 (B. Simma ed., 1995).
13. *Id.*
14. Cf. Article 2 of the consensus Definition of Aggression adopted by the UN General Assembly in 1974. General Assembly Resolution 3314 (XXIX), 29(1) RESOLUTIONS ADOPTED BY THE GENERAL ASSEMBLY 142, 143 (1974).
15. Cf. B. Broms, *The Definition of Aggression*, 154 RECUEIL DES COURS 299, 346 (1977).
16. In the *Nicaragua* case, the majority of the International Court of Justice envisaged legitimate counter-measures “analogous” to but less grave than self-defense in response to use of force which is less grave than an armed attack (without ruling out the possibility that these counter-measures would involve the use of force by the victim State). *Nicaragua* Judgment, *supra* note 3, at 110. However, absent an armed attack, the only counter-measures available to the victim State are short of force; self-defense is ruled out even by analogy.
17. Unless there exists a treaty between the two countries calling for periodic consultations between their respective Heads of States. In such an instance, refusal to allow the visit might rise above mere unfriendliness and be branded as a breach of the treaty.
18. Such a notification is permissible at any time—without any need to explain the decision—under Article 9 of the 1961 Vienna Convention on Diplomatic Relations, 500 UNITED NATIONS TREATY SERIES 95, 102.

19. See [1976] DIGEST OF UNITED STATES PRACTICE IN INTERNATIONAL LAW 577-578 (E.C. McDowell ed., 1977).

20. "Clandestine agents: spies ... are not official agents of states for the purpose of international relations:" the home State usually disavows them, although—if caught in the act—the State upon whom they spied is likely to punish them severely under its domestic law. 1(2) OPPENHEIM'S INTERNATIONAL LAW 1176-1177 (R. Jennings & A. Watts eds., 9th ed. 1992).

21. See J.P. Partsch, *Retorsion*, in 9 ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW 335, 336 (R. Bernhardt ed., 1986).

22. As prescribed in Article 31 of the Vienna Convention on Diplomatic Relations, *supra* note 18, at 112.

23. See Part V (Articles 55-75) of the 1982 United Nations Convention on the Law of the Sea, Official Text, 18-27.

24. International Law Commission, Draft Articles on State Responsibility [Article 42(1)], 37 INTERNATIONAL LEGAL MATERIALS 440, 454 (1998).

25. UN CHARTER, *supra* note 2, at 341.

26. *Id.* at 342.

27. It is important to distinguish between the function of the Security Council in recommending appropriate methods of adjustment [under Article 36(1)] and its authority to legally bind Member States to comply with such procedures (or other measures) pursuant to Chapter VII of the Charter (Article 39 *et seq.*). See V. Gowlland-Debbas, *Security Council Enforcement Action and Issues of State Responsibility*, 43 INTERNATIONAL AND COMPARATIVE LAW QUARTERLY 55, 83 (1994).

28. The International Law Commission calls reprisals "countermeasures" and subjects them to certain conditions. See Articles 47-50 of the Draft Articles, *supra* note 24, at 456-458.

29. See O. SCHACHTER, INTERNATIONAL LAW IN THEORY AND PRACTICE 185 (1991).

30. See J.R. Sculley, *Computers, Military Use of*, 2 INTERNATIONAL MILITARY AND DEFENSE ENCYCLOPEDIA 617 (T.N. Dupuy ed., 1993).

31. See M.N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUMBIA JOURNAL OF TRANSNATIONAL LAW 885, 888 (1999).

32. See M.N. Schmitt, *Future War and the Principle of Discrimination*, 28 ISRAEL YEARBOOK ON HUMAN RIGHTS 51, 78 (1998).

33. Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons, 1996, 35 INTERNATIONAL LEGAL MATERIALS 809, 822 (1996).

34. It is noteworthy that nowadays there is less to the distinction than meets the eye, inasmuch as a modern artillery battery is likely to be directed by a computer.

35. The term "terrorists," as used in this paper, includes not only political groups but also crime rings, esoteric cults, and any other violent non-State actors who may acquire the technological capability to engage in a CNA. See D.C. Gompert, *National Security in the Information Age*, 51(4) NAVAL WAR COLLEGE REVIEW 22, 33 (1998).

36. *Corfu Channel (U.K. v. Alb.)*, 1949 I.C.J. 4, 22 (merits).

37. See R. Ago, *Fourth Report on State Responsibility*, [1972] II YEARBOOK OF THE INTERNATIONAL LAW COMMISSION 71, 120.

38. L. Condorelli, *The Imputability to States of Acts of International Terrorism*, 19 ISRAEL YEARBOOK ON HUMAN RIGHTS 233, 234 (1989).

39. The quotation is from Article 8(a) of the International Law Commission's Draft Articles, *supra* note 24, at 444. Cf. G. Townsend, *State Responsibility for Acts of De Facto Agents*, 14 ARIZONA JOURNAL OF INTERNATIONAL AND COMPARATIVE LAW 635, 638 (1997).

40. *Nicaragua Judgment*, *supra* note 3, at 103.

41. *Id.* at 104.

42. *Id.* at 349, 543.
43. International Tribunal for the Prosecution of Persons Responsible for Serious Violations of International Humanitarian Law Committed in the Territory of the Former Yugoslavia since 1991, *Prosecutor v. Dusko Tadić*, Appeals Chamber, Case No. IT-94-1-A (July 15, 1999), Judgment, para. 137.
44. *Id.*
45. See Q. Wright, *Legal Aspects of the U-2 Incident*, 54 AMERICAN JOURNAL OF INTERNATIONAL LAW 836, 850 (1960).
46. See E. Rauch, *Espionage*, in 3 ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW 171, 172 (R. Bernhardt ed., 1982).
47. See L.R. Beres, *On International Law and Nuclear Terrorism*, 24 GEORGIA JOURNAL OF INTERNATIONAL AND COMPARATIVE LAW 1, 28 (1994-1995).
48. See R.G. Hanseman, *The Realities and Legalities of Information Warfare*, 42 AIR FORCE LAW REVIEW 173, 191-195 (1997).
49. State B may recruit foreign professional "hackers" as mercenaries in its service. For a recent treatment of the intricate topic of mercenaries, see D. Kritsiotis, *Mercenaries and the Privatization of Warfare*, 22(2) FLETCHER FORUM OF WORLD AFFAIRS 11-25 (1998).
50. See H.B. Robertson, *The Principle of the Military Objective in the Law of Armed Conflict*, THE LAW OF MILITARY OPERATIONS: LIBER AMICORUM PROFESSOR JACK GRUNAWALT 197-223 (M.N. Schmitt ed. 1998) (Vol. 72, US Naval War College International Law Studies).
51. Barcelona Traction, Light and Power Company, Limited (Second Phase), 1970 I.C.J. 3, 42.
52. "The massively destructive bombings of the [US] embassies in Kenya and Tanzania [in 1998], with a horrific loss of life, were clearly 'armed attacks' that allowed forcible measures of self-defense, even under the most stringent reading of UN Charter requirements." R. Wedgwood, *Responding to Terrorism: The Strikes against Bin Laden*, 24 YALE JOURNAL OF INTERNATIONAL LAW 559, 564 (1999).
53. For international practice confirming that the protection and rescue of nationals abroad is carried out in the exercise of self-defense, see N. RONZITTI, RESCUING NATIONALS ABROAD THROUGH MILITARY COERCION AND INTERVENTION ON GROUNDS OF HUMANITY 30-44 (1985).
54. See DINSTEIN, *supra* note 1, at 204-207.
55. For "on-the-spot reaction," see *id.* at 192-194.
56. On this problem, see M.R. Shulman, *Legal Constraints on Information Warfare*, Air War College, Center for Strategy and Technology, Occasional Paper No. 7, at 6 (1999).
57. See Advisory Opinion, *supra* note 33, at 823.
58. See DINSTEIN, *supra* note 1, at 199-200.
59. The best illustration of a defensive armed reprisal (against State-sponsored terrorism) is the US air-raid on Libyan targets in 1986 (in response to a bomb, which exploded in Berlin, killing two American servicemen and wounding many others). See W.V. O'Brien, *Reprisals, Deterrence and Self-Defense in Counterterrorism Operations*, 30 VIRGINIA JOURNAL OF INTERNATIONAL LAW 421, 463-467 (1989-1990).
60. See P.C. JESSUP, A MODERN LAW OF NATIONS 163 (1948).
61. On the difference between State terrorism, State-assisted or State-encouraged terrorism, and State-tolerated terrorism, see S. Sucharitkul, *Terrorism as an International Crime: Questions of Responsibility and Complicity*, 19 ISRAEL YEARBOOK ON HUMAN RIGHTS 247, 256-257 (1989).
62. Wedgwood, *supra* note 52, at 565.
63. For the facts of this famous incident, see R.Y. Jennings, *The Caroline and McLeod Cases*, 32 AMERICAN JOURNAL OF INTERNATIONAL LAW 82, 82-89 (1938).
64. See DINSTEIN, *supra* note 1, at 213-221.

65. See O. Schachter, *The Lawful Use of Force by a State against Terrorists in Another Country*, 19 ISRAEL YEARBOOK ON HUMAN RIGHTS 209, 228–229 (1989).

66. *Nicaragua Judgment*, *supra* note 3, at 94.

67. Nuclear Weapons Advisory Opinion, *supra* note 33, at 822.

68. On immediacy, see DINSTEIN, *supra* note 1, at 183–184.

69. L. Stuesser, *Active Defense: State Military Response to International Terrorism*, 17 CALIFORNIA WESTERN INTERNATIONAL LAW JOURNAL 1, 31 (1987–1988).

70. See C.A. Fleischhauer, *Negotiation*, in 1 ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW 152, 153 (R. Bernhardt ed., 1981).

71. This was established already in 1928, in the well-known Arbitral Award in the *Naulilaa* case, 2 REPORTS OF INTERNATIONAL ARBITRAL AWARDS 1011, 1028 (French text). For a summary in English, see [1927–1928] ANNUAL DIGEST OF PUBLIC INTERNATIONAL LAW CASES 526, 527.

72. See N.M. Feder, *Reading the UN Charter Connotatively: Toward a New Definition of Armed Attack*, 19 NEW YORK UNIVERSITY JOURNAL OF INTERNATIONAL LAW AND POLITICS 395, 415–416 (1986–1987).

73. See J.F. Murphy, *Force and Arms*, in 1 UNITED NATIONS LEGAL ORDER 247, 260 (O. Schachter & C.C. Joyner eds., 1995).

74. See R. Ago, *Addendum to Eighth Report on State Responsibility*, [1980] II (1) YEARBOOK OF THE INTERNATIONAL LAW COMMISSION 13, 69–70.

75. There is no support in the practice of States for the notion [advocated by J.G. Gardam, *Proportionality and Force in International Law*, 87 AMERICAN JOURNAL OF INTERNATIONAL LAW 391, 404 (1993)] that proportionality remains relevant—and has to be constantly assessed—throughout the hostilities in the course of war.

76. Presumably, this is why R. Ago said in his Report to the International Law Commission that “the action needed to halt and repulse the attack may well have to assume dimensions disproportionate to those of the attack suffered.” Ago, *supra* note 74, at 69.

77. See DINSTEIN, *supra* note 1, at 208–209.

78. Such confusion is apparent when redundant legitimation is sought for the American and British air campaign against Iraq since December 1998 [see, e.g., S.M. Condrón, *Justification for Unilateral Action in Response to the Iraqi Threat: A Critical Analysis of Operation Desert Fox*, 161 MILITARY LAW REVIEW 115–180 (1999)]. The Gulf War, which started with an Iraqi armed attack against Kuwait in August 1990, is not over at the time of writing. The cease-fire of 1991 did not terminate the war.

79. K.C. Kenny, *Self-Defence*, in 2 UNITED NATIONS: LAW, POLICIES AND PRACTICE 1162, 1167 (R. Wolfrum ed., 1995).

80. D. Goldstone & B.E. Shave, *International Dimensions of Crimes in Cyberspace*, 22 FORDHAM INTERNATIONAL LAW JOURNAL 1924, 1941 (1998–1999).

81. The Gulf War is a prime example. The invasion of Kuwait by Iraq took place on August 2, 1990. The Security Council authorized the use of “all necessary means” as from January 15, 1991 (namely, after almost half a year). Security Council Resolution 678 (1990), 29 INTERNATIONAL LEGAL MATERIALS 1565, *id.* (1990).

82. For the Kashmir incident, see 45 KEESING’S RECORD OF WORLD EVENTS 42997 (1999).

83. See DINSTEIN, *supra* note 1, at 172.

84. See T.D. Gill, *The Forcible Protection, Affirmation and Exercise of Rights by States under Contemporary International Law*, 23 NETHERLANDS YEARBOOK OF INTERNATIONAL LAW 105, 111–112 (1992).

85. “Hindsight can be 20/20; decisions at the time may be clouded with the fog of war.” G.K. Walker, *Anticipatory Collective Self-Defense in the Charter Era: What the Treaties Have Said*, THE LAW OF MILITARY OPERATIONS, *supra* note 50, at 365, 393. Although the statement is made about

anticipatory action (which is inadmissible in the opinion of the present writer), it is equally applicable to interceptive self-defense.

86. See W.G. SHARP, SR., *CYBERSPACE AND THE USE OF FORCE* 133 (1999).

87. See A.D. Softer, *Terrorism, the Law, and the National Defense*, 126 *MILITARY LAW REVIEW* 89, 98 (1989).

88. See J.P. Terry, *An Appraisal of Lawful Military Response to State-Sponsored Terrorism*, 39(3) *NAVAL WAR COLLEGE REVIEW* 59, 60–61 (1986).

89. That is to say, Greece may respond to an armed attack against Peru. See M. AKEHURST, *MODERN INTRODUCTION TO INTERNATIONAL LAW* 317–318 (P. Malanczuk ed., 7th ed. 1997).

90. *Nicaragua* Judgment, *supra* note 3, at 110.

91. *Id.* at 104.

92. *Id.* at 544–545.

93. On the different categories of collective self-defense treaties, see DINSTEIN, *supra* note 1, at 226–236.

94. North Atlantic Treaty, 1949, 34 *UNITED NATIONS TREATY SERIES* 243, 246.

95. Nuclear Weapons Advisory Opinion, *supra* note 33, at 822.

96. S.D. BAILEY & S. DAWS, *THE PROCEDURE OF THE UN SECURITY COUNCIL* 103 (3d ed. 1998).

97. *Nicaragua* Judgment, *supra* note 3, at 121–122.

98. *Id.* at 376–377.

99. See O. Schachter, *United Nations Law in the Gulf Conflict*, 85 *AMERICAN JOURNAL OF INTERNATIONAL LAW* 453, 458 (1991).

100. M. Halberstam, *The Right to Self-Defense Once the Security Council Takes Action*, 17 *MICHIGAN JOURNAL OF INTERNATIONAL LAW* 229, 248 (1996–1997).

101. See N.D. WHITE, *KEEPING THE PEACE: THE UNITED NATIONS AND THE MAINTENANCE OF INTERNATIONAL PEACE AND SECURITY* 56 (1993).

102. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), 1977, *THE LAWS OF ARMED CONFLICTS: A COLLECTION OF CONVENTIONS, RESOLUTIONS AND OTHER DOCUMENTS* 621, 645 (D. Schindler & J. Toman eds., 3d ed. 1988).

103. See C. Greenwood, *The Law of Weaponry at the Start of the New Millennium*, *THE LAW OF ARMED CONFLICT: INTO THE NEXT MILLENNIUM*, 185, 231 (M.N. Schmitt and L.C. Green eds., 1998) (Vol. 71, US Naval War College International Law Studies).