International Law Studies - Volume 76
Computer Network Attack and International Law
Michael N. Schmitt & Brian T. O'Donnell (Editors)

# VI

# Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter

Daniel B. Silver

## Introduction

Awareness has been growing in recent years that modern societies, increasingly computer-dependent, are highly vulnerable to malicious intrusion into their computers and computer networks. Concern about this issue is especially high in the United States; in all likelihood, no other country is more at risk. The reality of these concerns is underscored by news reports chronicling an active "cyberwar" that appears currently to be underway. This is not, however, a conflict involving another State or even a terrorist group as the adversary. Instead, this struggle pits federal law enforcement officials against computer "hackers" who have defaced US Government Internet sites (including the website of the National Infrastructure Protection Center) and have threatened the electronic destruction of Internet servers if the federal government continues the battle.[1]

At the moment, the reality of such computer network attack (CNA) by private individuals and non-State actors may be more pressing than the use of CNA as an instrument of hostile action by one State against another. Whether CNA

actually has been used as an instrument of State action is uncertain as of this writing. According to numerous press reports, President Clinton approved a covert action against Serbian leader Slobodan Milosevic that was intended to include computer network attacks against Milosevic's financial assets held outside Yugoslavia.[2] It also has been reported that General Henry H. Shelton, Chairman of the Joint Chiefs of Staff, acknowledged that the United States used CNA against Serbian computer networks in the course of the Kosova conflict and that the Defense Department is actively engaged in organizing for the coordination not only of defensive measures to protect military computer networks from "cyberterrorists," but of offensive CNA operations.[3] However, unnamed "senior defense officials" also have been quoted as saying that the United States refrained from implementing plans to use CNA against Serbian computer networks for purposes of disrupting military operations and basic civilian services, due in part to legal guidance from the Defense Department's Office of General Counsel that certain uses of CNA could be considered as "war crimes."[4]

Thus, it remains unclear whether the United States attempted to use CNA in connection with the Kosova conflict. There is no doubt, however, that the Department of Defense has made an extensive study of the international legal issues that such use could engender[5] and that US military and national security experts, looking to the possibility of using CNA in future conflicts, have an understandable interest in understanding the implications of CNA under international law.

Such legal issues can arise under both the *jus ad bellum* and the *jus in bello*. This discussion is confined to the former, specifically to the extent to which peacetime use of CNA by or on behalf of a State (including use in the course of hostilities that do not attain the status of a war under international law) can be characterized as an exercise of "force" under Article 2(4) of the United Nations Charter.[6] Because the discussion is limited to this threshold question, it will not extend into other areas, in particular, when CNA that constitutes force under Article 2(4) might also rise to the level of an "armed attack" under Article 51 of the Charter or might be lawfully used as a defense against such an attack.[7]

At the outset, it may be useful to define the "rules of engagement" for this discussion. Reisman has pointed out that jurists' formulations, which characteristically take the form of "this is the law," often refer "simultaneously and without discrimination to descriptions about flows of decisions in the past, predictions about the way decisions may be taken in the future, or statements of preference."[8] This criticism seems particularly applicable to statements about international law. It thus is appropriate to make clear what kind of statements this chapter is intended to make.

It is too early for any legal authority to have emerged on the status of CNA under Article 2(4). Consequently, analysis of the question must proceed on the basis of analogy to such possibly relevant authority and doctrine as exists in other contexts. The statements about the law set forth in this chapter, therefore, do not purport to describe the flow of past decisions directly on point. Nor do they state a policy preference unless explicitly identified as such. Rather, they are predictive of where it appears that existing legal doctrine, found in other contexts, reasonably would carry a court seized with an issue concerning the status of peacetime CNA under Article 2(4).

The conclusion to which such predictive analysis leads is that there is no "bright-line" rule. Instead, certain applications of CNA are likely to be held to constitute force under Article 2(4), but many other applications are likely not to. This nebulous conclusion may disappoint the proponents of two positions that have emerged in scholarly and military circles. The first, focusing on the inherently malicious and destructive nature of CNA, advocates that it should be considered to be a prohibited use of force under Article 2(4) and thus to violate international law, except when otherwise authorized under the Charter. The second, viewing CNA as having the beneficial potential to achieve military or political objectives with less violence than traditional means of warfare, points in the opposite direction—CNA (except maybe in its most extreme applications) should not be viewed as a prohibited use of force, because to do so would promote the application of more lethal techniques. Approaching the question in a predictive mode, however, leads one to conclude that both these extremes are examples of wishful thinking, conflating a policy objective with a fair reading of the state of the law.[9]

## Preliminary Questions

Before addressing the core question, several preliminary issues merit discussion, namely the definition of CNA, the techniques that it encompasses, and, finally, whether there is any real prospect that the status of CNA under Article 2(4) will be clarified without creating a new legal regime or clarifying instrument for that purpose.

### The Definition of "Computer Network Attack"

A threshold question is what is meant by "computer network attack." CNA has been defined in Joint Chiefs of Staff doctrine as "operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks,

or the computers and networks themselves."[10] For the sake of convenience, this definition will be adopted for present purposes. But it should be noted that it sweeps too broadly to be truly useful, because it includes a range of physical techniques of attack that could be directed at almost any target.

Unless it be contended that computer facilities have a different status in international law than other facilities (a proposition for which there is no authority), targeting a kinetic weapon, such as a missile, bomb or other explosive device, at a computer (or, more likely, a structure known to house computing facilities) should not raise any different question under international law than if the same weapon were targeted at another piece of equipment or a structure used for a different purpose. The operation itself almost certainly will be characterized as a use of force.[11] Thus, because it includes techniques of physical attack that are not unique to computers but instead are widely applicable without distinction as to target, the Joint Chiefs' definition of CNA has limited utility as a tool of legal analysis.

At the same time, the definition contains an ambiguity that also may limit its usefulness, in that it is unclear whether it encompasses the manipulation of a computer network to achieve an effect extrinsic to the network itself, as opposed to merely rendering the network ineffective. An example of such an extrinsic effect would be the hostile manipulation of a computerized railway control system as to produce train wrecks.[12] Similar hypothetical examples abound, running from the potentially catastrophic[13] to the merely vexatious.[14] While such operations could be viewed as a form of "degrading" the information resident in the computer, the definitional fit is awkward. Since these manipulative variants of CNA are, however, potentially among the most important from a force perspective, they will be assumed to be included within the definition for purposes of this discussion.[15]

## Techniques of CNA

How CNA is accomplished can have a bearing on the legal analysis. CNA is not a monolithic technique. On the contrary, there are many methods by which computer networks have been, or could be, attacked. Nor is CNA capable only of being directed at a single objective. Instead, a broad array of purposes can be served by hostile intrusion into computers or computer networks. These include, among others: (i) extracting the information held in the target computer (espionage); (ii) disseminating information through the adversary's information network in order to deceive the adversary or stimulate political instability; (iii) preparing the battlespace by incapacitating the adversary's command, control, and communication capabilities; or (iv) causing property damage, physical

injury, or death by manipulating infrastructure or operational systems controlled by the target computer.

It should be obvious that which technique is being considered, as well as the purposes for which it is to be employed, can make a significant difference to the legal outcome. As noted above, a traditional physical attack (e.g., bombing the building that houses the computers) seems to present no legal issues specific to the fact that the target is a computer or computer network. The legally most interesting applications of CNA are those methods of attack which are highly specific to computers because they make use of the methods by which computers themselves operate.

Concern about infrastructure security and the potential vulnerability of the United States to malicious intrusion on computers and computer networks has generated considerable discussion of the non-kinetic technical means by which computers might be attacked.[16] It is not necessary here to rehearse the technical details. It is sufficient to note their general outlines. What is unique to computers is their vulnerability to what has been called "digital data warfare" [17] namely the covert introduction of malicious computer code into a computer system or network to achieve an objective.

There is a rich lexicon describing variants of malicious computer code (e.g., "virus," "worm," "Trojan horse," "flying Dutchman," "time bomb," "logic bomb"[18]), but the labels do not matter here. What is significant in the present context is that malicious computer code can be designed to lie dormant until triggered and to self-destruct and eliminate evidence of its presence after the mission has been accomplished. Also significant is that most computer systems are linked electronically to other systems and that malicious code usually can be introduced into a computer system by electronic data transfer (over the Internet or directly) as long as the attacker can evade or overwhelm whatever defenses are built into the system. Malicious code also can be introduced into a computer system by concealing it in hardware or software that the operator of the target system unwittingly incorporates into the system. There also reportedly are back-door techniques for introducing malicious code into computer systems without any use of media for which the system was designed, for example by manipulating the power system or using high-energy radio frequencies or carefully controlled electromagnetic pulses.[19]

## The Prospects that the Law will be Clarified

Although the application of UN Charter Article 2(4) to CNA is an intellectually interesting question, there is reason to wonder whether, as a practical matter,

the issue ever will arise in a context requiring an actual decision. The most important obstacle may be the difficulty of attributing CNA to State action. Moreover, even if State use of CNA were to emerge as a recognizable phenomenon, such CNA would have to occur in relative isolation in order squarely to pose the relevant legal issue. Because this seems improbable, it likely will be a long time, if ever, before the practice of States, decisions of the International Court of Justice (ICJ), or other recognized sources of international law yield a clarification of how Article 2(4) applies to CNA. Thus, the best prospect for a prompt and authoritative elucidation of the status of CNA under Article 2(4) would be if States were to agree to define the legal parameters of CNA through an appropriate international instrument.

**1. State action.** Although various authors have posited a number of forms that an incident of CNA could take, from disrupting air traffic control systems to "busting" dams or oil pipelines, the rub is that, at least up to the time of this writing and to the best of the author's knowledge, none of these imaginable instances of CNA actually has been perpetrated by a State or with publicly-discernible State sponsorship.[20] Indeed, the more extreme (and therefore more interesting) examples apparently have not occurred at all.

It certainly is true that numerous instances of intrusion into computer networks by private individuals (generally called "hacking") have taken place recently.[21] Some of these have been fairly primitive, such as the flooding of US Government Internet websites with messages ("spamming") emanating from Serbia and protesting US bombing of that country.[22] Others have been more sophisticated and potentially quite harmful, including attacks on Defense Department and other US Government computer networks. But most appear to have been the work of individuals or groups not identified (at least not in any source accessible to the public) as sponsored by a State.

Lacking acknowledged, or at least provable, State action or State sponsorship, such events must be considered as raising problems in international criminality, not public international law. Moreover, to date there appears to have been no State reaction to CNA in the international legal arena. Because no State has yet taken any action or asserted a legal position vis-à-vis another State arising out of an incident of CNA, there is a lack of the State practice that could illuminate the international legal analysis of CNA, whether under Article 2(4) or under customary international law.

This state of affairs is not surprising. CNA is a new phenomenon. Moreover, unlike many other putative techniques of force, most forms of CNA may be difficult or impossible to trace to the real perpetrator. Indeed, the most effective forms of CNA are likely to be contrived so as to conceal the fact that they

occurred at all, leaving the target State in doubt as to whether the affected computer network was externally attacked or simply failed for other reasons. Obviously, to the extent that it is not possible plausibly to demonstrate the existence of an event of CNA, even less the identity of the perpetrator and a nexus to a State sufficient to imply State responsibility, any State response based on an alleged violation of Article 2(4), or indeed any other norm of international law, would lack credibility.

This issue is exacerbated by the amorphous structure of the Internet. If an incident of CNA is effected by "indirect penetration"[23] over the Internet, it may be difficult to determine where it originated. There is no inherent reason why the point from which the attack is launched must be in the territory of the State that caused the act to be done. Moreover, even if the identity of the immediate perpetrator is discovered, it may be impossible to demonstrate a link between that person or organization and a State to which responsibility for the CNA can be attributed. To date, the mode of CNA in actual practice is the computer "hacker," wreaking havoc for sport or, occasionally, for some ideological motive. One would expect any State that chose to use CNA as a weapon to attempt to make its efforts look like those of a hacker.

Moreover, the contexts in which a State is most likely to use CNA unaccompanied by an array of traditional military instruments are intelligence collection and covert action, for example, the use of CNA to sow unrest in the target State's population. Such applications of CNA, however, probably are also the least likely to be publicly acknowledged by, or credibly attributable to, the State that perpetrates them.

**2. Unlikelihood of Isolated Use.** In order for the status of CNA under Article 2(4) to emerge as an issue, the incident in question probably would have to be considered in isolation. If, as may have been the case in the Kosova conflict, CNA is used in the context of a military operation conducted by traditional means that indubitably constitute force, the target State would have little interest in raising a legal dispute on the sole issue of CNA. (Thus, Serbia may have tenable claims that the entire operation conducted against it was a violation of international law, but it is unlikely that it would single out US hacking into its computer networks, if it occurred, as a separate violation, even less one worthy of an individualized response.)

## The Status of CNA Under Article 2(4)

Lacking any directly applicable precedents or other sources of international law, the status of CNA under Article 2(4) only can be predicted by drawing

analogies to other phenomena whose status is better established. If CNA in all its manifestations easily could be assimilated to armed force, further discussion would be superfluous, since Article 2(4) indisputably encompasses armed force. Neither every form of CNA nor every purpose for which CNA can be used, however, readily can be analogized to armed force. Some applications of CNA (including, notably, those the United States is reported to have contemplated using against Slobodan Milosevic) operate only in the economic or political sphere, thus making highly relevant the question whether Article 2(4) encompasses measures of economic or political coercion, or, if not all such measures, at least those that threaten the target State's territorial integrity or political independence. Moreover, because it may be unclear (given the inherent problems of tracing CNA to its source) whether an incident of CNA has been conducted by military forces, another relevant issue, if one is to reason by analogy, is whether non-military uses of physical force can fall within the scope of Article 2(4).

## Economic and Political Coercion as Force

Virtually since the Charter was adopted, controversy has existed as to whether measures of economic and political coercion constitute force under Article 2(4). The weight of scholarly opinion supports the negative view,[24] but that does not appear to have put the question to rest, at least as applied to CNA. Thus, one recent analysis of CNA under Article 2(4), while admitting that the "prevailing view" among scholars would confine Article 2(4) to "armed force," asserts that a more balanced, contextual view of Article 2(4) would conclude that economic and political sanctions can threaten international peace and a target State's territorial integrity and political independence and therefore can fall within the ambit of Article 2(4); the author's conclusion that CNA generally falls within Article 2(4) derives from this premise.[25] In contrast, another recent analysis of the status of CNA under Article 2(4) adopts the opposite conclusion, that "the prohibition of the threat or use of force includes armed, but not economic or political coercion."[26] The same author goes on to comment, however, that the borders of force do not necessarily "precisely coincide with armed force, i.e., physical or kinetic force applied by conventional weaponry."[27]

On balance, the latter perspective is better founded. Although a conclusion that economic or political coercion standing alone constitutes force under Article 2(4) might well contribute more to the purposes of the Charter and to the maintenance of world order than the contrary, that does not make it tenable as a matter of legal analysis. A number of points sustain the view that Article 2(4) does not apply to measures of political or economic coercion. These include the following:

- The historical background of Article 2(4) shows that it was conceived against a background of international efforts to eliminate unilateral recourse to armed force.[28] Measures of economic and political coercion were not the issue.
- The *travaux preparatoires* of the Charter indicate that the San Francisco Conference declined to adopt a proposal that was advanced to extend the prohibition on the use of force to include economic sanctions. Subsequent General Assembly declarations, principally the Declaration on Friendly Relations[29] and the Declaration on the Enhancement of the Effectiveness of the Principle of Refraining from Threat or Use of Force in International Relations,[30] provided an opportunity for the General Assembly to clarify the issue by delineating economic and political coercion as equivalents of armed force for purposes of Article 2(4). Efforts were made by some Members to this end, but they met resistance from other Members and were unsuccessful,[31]demonstrating that there is no common understanding among Members that would support extending Article 2(4) to economic or political coercion.
- There is no decision of the International Court of Justice (ICJ) holding that measures of economic or political coercion constitute force under Article 2(4). Indeed in the *Nicaragua* case,[32] in which the Court generally considered the customary international law prohibition against the use of force to be coterminous with Article 2(4) (which was not itself at issue), Nicaragua complained of substantial measures of economic pressure. These were considered to be violations of the bilateral treaty of Friendship, Commerce and Navigation between Nicaragua and the United States, however, and were not even mentioned as possible violations of the customary international law prohibition on the use of force. Moreover, the Court held that even the United States' furnishing of substantial financial support to insurgent forces in Nicaragua, support that was used to sustain acts of violence, did not constitute the use of force under customary international law.[33] It would seem, if financing an armed insurrection is not force, that, *a fortiori*, other economic measures that have a less direct nexus to armed violence would not be either.

Thus, despite arguments advanced to the contrary, the fact remains that the drafting history of the Charter is inconsistent with such an extension, that this question generally has divided Western States from significant components of the "Third World," and that no international consensus has emerged defining economic and political coercion, standing alone, as force, although there is a

strong basis for concluding that such forms of coercion may violate other norms of international law, such as the principle of non-intervention.[34]

An argument can be made that the prevailing view regarding economic and political measures of coercion should not apply to CNA. Although ultimately not convincing, it proceeds along the following lines. In more than half a century of debate over the application of Article 2(4) to economic and political coercion, the kind of coercion that has been envisaged has been primarily external and gradual—trade sanctions, withholding economic benefits, unequal trading practices, interference with the target State's external commercial relations. In contrast, the kind of economic coercion that CNA might make possible, crippling the banking system, or shutting down the securities markets, operates on the internal economic structures of the target State and does so through a swift and devastating blow. Therefore, since CNA is a different phenomenon, it can be argued that the earlier debate over economic and political sanctions as force is irrelevant.

While the factual premise underlying this argument may be valid, all it demonstrates is the neutral fact that CNA is a new form of hostile activity. That CNA may differ from earlier forms of economic and political coercion does not tell us whether CNA comes within the intended scope of Article 2(4) or instead should be viewed as another manifestation of the types of economic and political coercion that various states have failed to persuade the international community to acknowledge as falling within the definition of "force."

In analyzing the application of Article 2(4) to CNA in order to predict how the ICJ and the world community will view CNA, it seems prudent, in light of existing legal authority, to acknowledge, however much a different conclusion might be desired on policy grounds, that there is little likelihood that purely economic or political coercion, even if effectuated in novel ways, will be considered to violate Article 2(4). If this proposition is correct, it suggests that the touchstone in any future analysis of CNA under Article 2(4) will be whether the specific application of CNA at issue more closely resembles economic and political coercion, on the one hand, or, on the other hand, military force as the latter concept is commonly understood.

## Non-Military Physical Force

Another interpretive issue under Article 2(4) that bears on the status of CNA is whether non-military physical measures can also constitute force for purposes of Article 2(4). Examples of such measures would include: a State intentionally acts to cause flooding in an adjacent down river State; a State sets a forest fire in a

frontier region intending that it spread into the target State; a State releases noxious substances into the environment, knowing that the effect will be felt in the target State. Opinion is divided as to the status of such acts under Article 2(4) and there is no decisional authority directly on point. Some scholars admit the possibility that in certain circumstances a hostile use of such non-military forms of physical force could fall within Article 2(4), especially if the results rose to a level of magnitude that could be viewed as the equivalent of an armed attack triggering the right of self-defense under Article 51.[35]

The better view would appear to be that non-military physical force can indeed fall within Article 2(4), even if the consequences do not rise to the level of an armed attack. The principal reason why scholars have opposed such an extension of Article 2(4) appears to be a "slippery slope" fear that applying Article 2(4) to non-military physical force when its effects approximate those of military force would open the door to applying Article 2(4) to measures of economic and political coercion that have similarly devastating effects. This fear is misplaced. In the case of non-military physical force, the fact that the force is physical is enough, first, to distinguish it from coercive economic and political measures and, second, to support an analogy to those military forms of physical force that clearly lie at the core of Article 2(4).

If one is prepared to admit that non-military physical measures can constitute force for purposes of Article 2(4), it is hard to see why this should be the case only if the consequences are of a type and degree of seriousness that would rise to the level of an armed attack. It is widely recognized that not all force under Article 2(4) necessarily constitutes an armed attack under Article 51. The ICJ implicitly so stated when it indicated in the *Nicaragua* case that supplying arms and other support to armed rebel bands in another State is not an armed attack but could constitute a violation of the customary international prohibition on the use of force.[36] To require non-military force to rise to the level of an armed attack in order to violate Article 2(4) would obliterate the important distinction between Articles 2(4) and 51. Such a position would either legalize under Article 2(4) a broad range of hostile and destructive physical acts that fail to reach the armed attack threshold or would provide an incentive to lower the Article 51 threshold, with a concurrent risk of expanding violence under the pretext of legitimate self-defense. Thus, on balance, it seems better to conclude (although admittedly without the benefit of any supporting authority) that intentional, hostile uses of non-military physical force by one State against another can fall within the scope of Article 2(4) when they sufficiently resemble military force in their physically destructive effect, whether or not the criteria of an armed attack are met.

## Flexibility of the Concept of Military Force

Even if one were to accept the restrictive view that force under Article 2(4) means military force, it should be noted that the latter concept carries a large measure of flexibility. As the techniques of warfare evolve, so too does the general understanding of what constitutes "military" force. If this were not so, the prohibition of Article 2(4) would become ossified at the level of military technology that existed at the end of World War II and would become increasingly irrelevant to the modern world. Thus, we have no difficulty in recognizing that new forms of biological and chemical warfare, directed energy, lasers, and other innovative technologies, if used intentionally by a State to cause physical injury or property damage in another State, will constitute forms of military or armed force. This applies even when the instrument itself, like a laser beam, is not inherently harmful but also is used for a range of beneficent purposes.

The hard question is how one recognizes when a new technology has become a form of military or armed force. The answer is not always obvious, but one significant criterion is whether the technique is associated with the armed forces of the State that uses it. Thus, in the case of CNA, if this technique were to be deployed only by intelligence agencies in conducting covert actions, it seems less likely that it would be generally accepted as a form of military or armed force than if it were used by the armed forces. Consequently, it is likely that the fact that the US Department of Defense (apparently joined by the military forces of other countries) is making preparations for the military use of CNA will hasten the day when a State's offensive use of CNA, at least for purposes of causing physical injury or property damage, will be considered a use of force under Article 2(4).

## Preliminary Conclusions

Against the background of the foregoing discussion, what preliminary conclusions can be reached about the application of Article 2(4) to CNA? The basic conclusion appears to be that force is like pornography: the law will recognize certain forms of CNA as force when it sees them. The present state of legal development does not permit laying down any hard and fast rules as to when that will be. It does, however, permit one to make some predictions about the circumstances in which State use of CNA may be likely to be held to constitute force under Article 2(4).

- CNA is not a single form of activity, nor is it potentially capable only of being directed at a single purpose. Thus there is no basis for concluding

that all forms of CNA per se constitute a violation of Article 2(4). Consequently, whether and when CNA will fall within the force category must be determined on a case-by-case basis. The question is how.

- CNA is most like traditional military force, and thus most likely to constitute force under Article 2(4), if its direct and foreseeable effects are physical injury or property damage.
- CNA that directly and foreseeably produces physical injury or property damage similar to that resulting from the use of traditional forms of weaponry is likely to be viewed as a use of force under Article 2(4), especially if that CNA is carried out by a State's armed forces.
- CNA that produces effects (even if direct and foreseeable) that are only of an economic or political nature is not likely to be held to be within the scope of Article 2(4). (Thus a program of CNA that crippled the financial infrastructure of a target State would not be a use of force under Article 2(4). Even if angry investors rioted and tore down the stock exchange, that physical damage would not be direct and foreseeable.)

The notion that CNA will be recognized as force under Article 2(4) when it sufficiently resembles military force implies that views on particular forms of CNA are likely to evolve in light of developments in military operations. These may lead to surprising conclusions. For example, before NATO's campaign against Serbia, one might have predicted that using CNA to produce transitory power outages in a target State would not be recognizable as an analog or equivalent of military force, because it causes no permanent damage to the targeted power system, and the effects on users of power, including the military, are uncertain, indirect and incalculable. Transitory outages seem more of an economic measure or a psychological weapon (intended, if one may put it this way, to induce a sense of powerlessness in the target State's population and leadership) than a military one.

In the last year, however, it was reported that the United States, on behalf of NATO, employed an innovative form of weapon against Serbia, a type of carbon filaments used against electric power facilities.[37] The filaments were dropped from aircraft, like a bomb, with the intention of causing property damage. Thus, it seems incontrovertible that their use was a form of armed force, even though the attacks did little or no permanent damage, merely shorting out the power system and disabling it for a brief period, thereby producing some disruption to the economy and the military effort, but having principally a psychological effect.

The same kinds of effects on the power system could be produced by CNA. Should this ever occur, it is likely that the earlier military use of the analogous

weapon described above will color the way the world looks at such use of CNA to shut down a target State's power system through manipulating its computerized controls. The existence of a military, non-CNA precedent, it is submitted, will create a predisposition to try to fit such an incident of CNA into the force category.

## The Views of Other Commentators

A small number of commentators have addressed the status of CNA under Article 2(4) and have come to widely divergent conclusions. A few assert that CNA causing destructive effects is *ipso facto* a use of "force." Others espouse the view advanced in this chapter, that CNA will only constitute force under Article 2(4) if it sufficiently resembles what the world recognizes as armed or military force and focus on attempting to provide a more precise way of identifying the principles that underlie such recognition.

**1. Destructive effect as the touchstone.** In one of the most extensive examinations of this issue to date, Sharp has proposed a rule that appears both sweeping and simple: "*Any* computer network attack that intentionally causes *any* destructive effect within the sovereign territory of another state is an unlawful use of force within the meaning of Article 2(4) that may produce the effects of an armed attack prompting the right of self-defense."[38]

It should be noted that this rule is not without its own interpretive issues. Does the term "destructive" mean only physical destruction, for example, or does it include economic harm? Sharp suggests that it could include the latter in some circumstances. He concludes that Article 2(4), while not including all coercive economic and political sanctions that are intended to influence another State's policy or actions, does extend to coercive political and economic sanctions that threaten the territorial integrity or independence of another State.[39] Thus, a non-physical destructive effect (such as disruption of financial markets) should be considered force under Article 2(4) if it is sufficiently serious to threaten the target State's territorial integrity or independence.

Aside from the fact that this conclusion is inconsistent with the weight of legal authority, extending the concept of "destruction" to include coercive economic and political measures, but only if they threaten another State's territorial integrity or independence, seems likely to deprive the posited rule of much of its apparent objectivity and simplicity, because it is not easy to determine when economic and political measures are likely to have such an effect unless the judgment is being made after the effect already has been produced.

For example, the Arab boycott of Israel manifestly was intended to threaten that country's territorial integrity and independence; it was carried out by States

that had declared war on Israel and espoused as their war aim the total elimination of the target country. Did that set of economic measures, or the associated political measures intended to delegitimize Israel in the international arena, really "threaten" Israel's territorial integrity and independence? With the benefit of hindsight, the answer clearly seems negative, but at different points in time the outcome was not so clear. Would we therefore conclude that the Arab boycott was a violation of Article 2(4) at certain periods in Israel's history and not at others? Such a result seems an unworkable rule of law. The example illustrates the difficulty, except perhaps in the most extreme cases, of applying a rule that depends on determining when a threat exists to territorial integrity or political independence.

In advancing the "destructive effect" standard, Sharp reasons on the basis of the proposition that other forms of non-military physical force constitute force under Article 2(4),[40] citing as examples the release of floodwaters or the spreading of fire across a border.[41] The argument then proceeds to adumbrate types of significant property damage, as well as possible human fatalities, that could be effected through CNA, such as flooding, train wrecks, plane crashes, chemical explosions, and fires. If these physically destructive events would constitute force under Article 2(4) if produced by a State agency using non-military means, it is argued, why should they not also be considered force when produced by CNA?

Although the underlying premise does not seem to be supported by judicial decision or State practice, the conclusion nonetheless is reasonable and should be widely accepted if confined to the examples given above. The analysis becomes markedly less compelling, however, when this already untested proposition is used as a springboard to make a leap into the arena of the financial, political, or psychological. The analogy to flood or fire is not convincing as a basis for concluding that causing "a run on banks or a massive financial crisis by crashing national stock exchanges"[42] also would constitute force. It pushes the underlying principle too far. (It should be noted that this assessment is not intended as a value judgment. Such State intervention in the affairs of another ought to be prohibited by international law and, indeed, may well may be on other grounds, such as the principle of non-intervention. The sole question, here, is whether Article 2(4) provides the norm.)

There might well be narrow circumstances in which Article 2(4) could be held applicable to an attack having effects solely or primarily in the economic or political sphere, but, if so, it is submitted, this would be because of the *means* employed, not the nature of the target. For example, if a State were to use physical but non-military means to achieve these results (e.g., dispatching intelligence

operatives into the target State to cut a fiber-optic cable on which essential financial information is transmitted), scholars might well conclude that an incident of force had occurred. Suppose instead, however, that a State sought to achieve the same end, financial disruption in the target State, through purely non-physical means, such as large-scale falsification of trading orders or dissemination of false market information. These seem to be quintessential measures of economic coercion, and it is very unlikely that scholarly opinion would sustain the view that such acts constituted force under Article 2(4). Thus, identity of ultimate effects, standing alone, simply does not supply a sufficient basis for concluding that Article 2(4) applies. The reason why the act of sabotage might be held to constitute force is not the end result (that the stock exchange crashes), but cutting the cable would involve an intrusion on the target State's territory that, although arguably "non-military," would achieve a physical effect closely resembling the use of kinetic action.

**2. Characteristics of armed force as the touchstone.** In a recent analysis, Schmitt, recognizing that within the existing framework of international law, CNA will be deemed to be Article 2(4) force only when it sufficiently resembles armed force, embarks on an impressive effort to delineate a principled basis for identifying those cases of CNA that meet this test.

He notes that traditional notions of force are instrument-based: the Article 2(4) prohibition against using a particular instrument, namely military force, against another State is tied to the high degree of congruence between its use and reprobated consequences, primarily physical destruction and injury. This, it is posited, explains why armed force, which almost always results in physical destruction or injury, is prohibited force, while economic or political coercion, whose tie to predictable physical destruction or injury is tenuous, is not.[43]

This observation is not entirely satisfying, however, because, as Schmitt has recognized, "the instruments do not precisely track the threats to shared values which, ideally, the international community would seek to deter."[44] It is clear that many technologies that would be recognized as weapons when used for the purpose of causing physical damage or personal injury, e.g., laser beams, can be entirely beneficent in other uses, such as medicine. Thus, when we assign one of those technologies to the "armed force" category, it is not because of its inherent lethality but because of the potential destructiveness of the way it is being used or the purpose for which it is deployed. The same could be said of CNA. And, for this reason, it seems unlikely that many would debate that CNA used directly to cause physical destruction or injury (busting a dam, rupturing a pipeline, causing airplanes or trains to crash) is tantamount to a weapon for purposes of Article 2(4), making its use force. The question is whether, applying criteria that will be

recognized as consistent with the current understanding of Article 2(4), any other use of CNA is sufficiently similar to these easy cases to be placed confidently in the force category.

To answer this question, Schmitt has suggested that, unless the international community is prepared to adopt a new normative structure to apply to inter-State coercion, the analysis of CNA must be fit into the traditional instrument/consequence based frame of reference by looking to see whether particular uses of CNA meet the criteria that distinguish armed force from political or economic coercion.[45] These criteria, he suggests, are: *severity*—the higher threat of physical injury or property damage associated with armed force; *immediacy*—the comparative swiftness of harm arising from armed force, as compared with other forms of coercion; *directness*—the relatively direct connection between armed force and negative consequences, as compared with other forms of coercion; *invasiveness*—the fact that in the case of armed force the act causing harm generally crosses into the territory of the target State whereas measures of economic or political coercion normally do not; *measurability*—the greater ease and certainty of assessing the consequences of armed force as compared with other forms of coercion; and *presumptive legitimacy*—the fact that violence is presumptively illegal under domestic and international law, whereas most (or at least many) techniques of economic and political coercion are presumptively legal.[46]

It would be desirable to be able to delineate criteria for identifying those types of CNA that should be treated as analogous to armed force. Yet, it is not clear that Schmitt's proposed six criteria reliably serve this purpose. Rather, examination of the criteria suggests that virtually any event of CNA can be argued to fall on the armed force side of the line, except perhaps as regards the criterion of severity, and that the criterion of severity in effect is just another way of articulating the observation that, for an event of CNA to be considered a type of force under Article 2(4), it must produce (or at least threaten to produce) personal injury or property damage similar to that caused by military weapons. Review of the proposed criteria, it is submitted, substantiates this proposition.

*Immediacy*: CNA ordinarily occurs with great immediacy, once its destructive potential is triggered. While malicious software may be designed to lie dormant for an extended period until some triggering event occurs, once it becomes active, the disruption of the targeted computer or computer network can be expected to be immediate, as well as immediately perceptible in result, even if the owner of the computer does not recognize that CNA is the cause of its degradation or destruction. (It is hard to imagine circumstances in which a slow, imperceptible deterioration of the targeted computer would be advantageous to the

author of the attack.) Thus, there seems to be little difference between CNA and ordinary armed force.

*Directness*: Compared to economic or political coercion, many applications of CNA are as direct as traditional armed force. The consequences generally flow directly from the act of attack itself and do not depend on intervening or contributory factors in order to have a harmful effect. Directness might become an issue if the only harmful effect were property damage and any effect on human beings was reactive. Thus, there could be a significant difference between CNA that caused a dam's floodgates to open and kill people, and CNA that merely inconvenienced the target population (e.g., by disrupting financial markets) to such a degree that rioting ensued. On the other hand, the path even from the latter form of CNA to the reprobated result of physical injury and tangible property damage is no more (or less) indirect than similar consequences, such as starvation or health disasters, arising from a military blockade. Yet a military blockade is undeniably a use of force. To the extent that the directness criterion is useful, it really seems to do no more than restate the proposition that to constitute force an event of CNA must directly cause physical injury or property damage and not operate solely in the economic or political realm.

*Invasiveness:* At least at the level of electrons, the act causing the harm in a CNA attack usually crosses into the target State, whether it be by importation of a corrupted item of hardware or software, the actions of an agent of the hostile State (a cyber saboteur), or cross-border data transmission over the telephone network. There appears to be no difference, in this regard, between CNA and traditional armed force.

*Measurability*: There seems no reason to assume that the consequences of an event of CNA would be any harder to measure than the negative consequences of armed coercion.

*Presumptive legitimacy*: Many States already have enacted laws outlawing CNA when perpetrated by private parties within the territory. As more and more States become aware of the threat, it is likely that this technique, at least when used by non-State actors, will be viewed in most States as presumptively illegal,[47] thus eliminating any distinction between CNA and what traditionally has been regarded as armed force.

Factoring out those of the criteria that do not appear reliably to distinguish CNA from armed coercion, all that is left is *severity*. Moreover, severity, as defined for this purpose, seems applicable only to physical injury and property damage, compelling the conclusion that CNA will be considered within the force category only if its foreseeable consequence is to cause physical injury or property damage and, even then, only if the severity of those foreseeable

consequences resembles the consequences that are associated with armed coercion. In short, what seems at first blush to be a nuanced way of analyzing incidents of CNA in practice may in fact turn out to do no more than identify the cases that would be clear without applying a criterion any more formal than was suggested in the preliminary conclusions above: CNA will be considered as force when it causes physical injury or property damage that is recognizably similar to that produced by instruments generally identified as weapons.

The limitations of the proposed factors are demonstrated by Schmitt's own comparison of two hypothetical uses of CNA.[48] In the first, CNA is used to disable an air traffic control system, causing airplanes to crash. According to Schmitt, this meets the criteria and is force. In the second example, the attacker destroys a university computer network for purposes of disrupting military research being conducted on campus. This does not meet the test and is not force. Schmitt suggests that there should be a different result in the attack on the university because the desired outcome, diminished capacity on the battlefield, is too remote from the event of CNA and too dependent on indeterminate factors. But this is not persuasive; the question of remoteness depends on how the outcome is defined. The immediate objective of the hypothetical CNA is to degrade the functioning of the targeted computer network, and the nexus between the act and that outcome is immediate. (One could as well argue that dropping filaments on Serbian electric power facilities to produce temporary power outages is remote from the ultimate objective, impairing Serbia's ability to maintain military operations. Yet few would gainsay that the NATO bombing raids in which these devices were dropped constituted force under Article 2(4).) Thus, except for this purported difference in directness, Schmitt's two examples are remarkably similar with respect to the proposed factors. In reality, it is submitted, the only tenable reason, and the real underlying explanation, for the difference in the posited outcome is that in the first case there is physical injury and significant property damage and in the second there is not.

That severity does not reliably predict the legal outcome unless it is confined to the severity of physical injury and/or property damage is shown by considering another hypothetical use of CNA, disruption of the target State's financial system through interference with the computers through which securities are traded, money moves, and financial transactions are recorded and settled. If successfully used against the United States or many other Western countries, the resulting social and economic disruption and monetary losses would be staggering. For each of Schmitt's factors, this event of CNA seems comparable to disabling an air traffic control system, except for the fact that it does not directly and foreseeably result in physical injury or property damage. In terms of severity,

more broadly construed, can there be any doubt that the impact of such an attack would be orders of magnitude more serious than if a hostile State, through a missile attack that caused no loss of life, obliterated a military warehouse full of uniforms—an incident that no one would hesitate to describe as within the scope of Article 2(4)? Yet, applying the existing legal framework for analyzing Article 2(4), this hypothetical attack on the country's financial infrastructure probably would be considered to fall outside the Article 2(4) force category, because it much more closely resembles economic coercion than traditional armed force.

## Conclusion: The Unsatisfactory Reality

There is no legal authority directly applicable to the status of CNA under Article 2(4). The most significant interpretive issue under Article 2(4) that might support extending it to a broad range of types of CNA is whether force includes economic or political coercion, and the weight of prevailing opinion is that it does not. Against this background, two approaches recently have been suggested in the literature. The first, destructiveness as the criterion, is relatively simple to apply (or could be made so with a few clarifications) and might be an appealing rule in a legislative context. The problem is that it is not founded in sufficient legal authority to engender confidence as a correct predictive statement of international law under Article 2(4). The second recognizes the limitations imposed by prevailing interpretations of Article 2(4) and tries to remain faithful to them, while positing criteria by which one can recognize those uses of CNA that fall in the force category. The exercise turns out to be somewhat illusory, however. At bottom, it leads to a conclusion that probably can be reached by reference to only one criterion: whether the foreseeable consequence of a particular manifestation of CNA is physical injury or property damage comparable to that resulting from military weapons. If so, the CNA will be held to fall within the force category. Otherwise it will not.[49]

What we are left with, it is submitted, is a situation in which general agreement probably can be reached on the proposition that there are some kinds of CNA that so resemble armed force that, like other manifestations of non-military physical force that have been suggested as falling within Article 2(4) (e.g., diverting a river in the hostile State so as to cause flooding in the target State), they will be held to fall within the scope of Article 2(4). It is likely that these forms of CNA will be recognized widely as Article 2(4) force if and when they occur, but it is difficult to articulate the precise bases on which recognition will rest. The one basis that seems most reliable is that physical injury or property damage must arise as a direct and foreseeable consequence of the CNA and must

resemble the injury or damage associated with what, at the time, are generally recognized as military weapons.

This conclusion appears highly unsatisfactory, leaving the law in a state of uncertainty, but does it really matter that much? First, it is clear that, whether or not they violate Article 2(4), most significant uses of CNA probably will violate other rules of international law, such as the prohibition against intervention in the affairs of other States, which the ICJ has held to be a principle of customary international law.[50] Various specific techniques used in carrying out CNA are likely to violate other international treaties, such as those relating to telecommunications. Thus, responsible decision-makers concerned about determining the legality of proposed uses of CNA are not bereft of legal principles to guide them.

Second, at least from the target State's perspective, the key issue is whether an incident of CNA gives rise to a right to take counteraction in self-defense. For that right to arise under the Charter, there must be an armed attack within the meaning of Article 51, a standard that goes beyond the existence of force under Article 2(4). It is difficult to say whether an event of CNA that caused significant physical injury and/or property damage, standing alone, ever could be considered an armed attack. In all likelihood, however, a State's use of CNA of such magnitude would not occur in isolation; instead it probably would form part of a coordinated offensive, other elements of which undeniably would constitute armed attack. In such a context, the legal status of the CNA element in isolation probably would be of little importance.

Third, worrying about the status of CNA under Article 2(4) may be fiddling while Rome burns. The notion that the Charter represents the sole legal structure under which coercive force can be exerted by one State against another largely has been discredited—both by the failure of the Security Council mechanism to function as envisioned by the Charter's framers and by the practice of States in ignoring recourse to the Security Council in favor of unilateral (including alliance-based) interventionism. The recent NATO humanitarian intervention in Serbia, which was given the fig leaf of a Security Council resolution only after its military aims were achieved, may be a step on the road to a better and more moral system of international law, but it was only the most recent in a series of events that, over the decades, have dealt a heavy blow to the system supposedly established by the Charter.[51] These events sustain the view that, while Article 2(4) represents an aspiration, (perhaps, like another form of prohibition, a failed "noble experiment"), the reality of international law on the use of force lies in the development of a "nuanced code for appraising the lawfulness of individual unilateral uses of force"[52] that is different from Article 2(4). If so, it can be

expected that over time a set of understandings as to the lawfulness of CNA will evolve outside the Charter framework.

This patient approach will not satisfy many, especially those who view CNA as a dangerous phenomenon. Enormous benefits to humankind, both actual and potential, derive from the use of computers. Advanced societies are moving towards pervasive dependence on the interplay of computer networks and advanced communications technologies. While not all consequences necessarily are welcome (loss of privacy, for example, is a significant concern), technologically sophisticated countries like the United States are experiencing enormous benefits in terms of increased productivity and enhancement of many aspects of the quality of life. These are benefits to which the rest of the world appears to aspire.

Yet technological sophistication engenders a degree of vulnerability that would have been unimaginable in earlier generations. (Who would have imagined a few decades ago that significant numbers of people would fear the end of a millennium not for religious reasons but because of a computer programming issue?) Human well-being throughout the world increasingly will depend on the inviolability of computer networks and the communications links that connect them. The world, it can be argued, should not have to rely for protection on unclear and debatable interpretations of the Charter or on principles of customary international law, such as non-intervention, that are honored in the breach and carry no ready enforcement mechanism. Nor should civilian populations be exposed to the risk that a code of rules on the use of CNA will evolve only after devastating examples of its use have pointed the way.

Thus, it is suggested (and this is an explicit expression of a policy preference, not a statement about the law as it is), efforts should be made towards the adoption of an international convention that would bind the parties not to use CNA for any military or hostile use. This should be accompanied by enhanced efforts, whether in the context of the same convention or separately, to achieve global legal cooperation in fighting CNA perpetrated by non-State actors, by making such action criminal under domestic laws regardless of purported justification, and by allowing prosecution of the perpetrators wherever apprehended or their extradition to the country in which the target computer or computer network was located.

## Notes

1. *Hackers Hit More Federal Web Sites*, WASHINGTON POST, June 5, 1999, at A5.

2. *See, e.g.*, Bruce D. Berkowitz, *Operation Backfire: Covert Action Against Milosevic is Neither Secret nor Smart*, WASHINGTON POST, July 18, 1999, at B1; Philip Sherwell, Sasa Nikolic & Julius

Strauss, *Kosovo: After the War: Clinton Orders "Cyber-sabotage" to Oust Serb Leader*, SUNDAY TELEGRAPH, July, 4, 1999, at 27; Gregory L. Vistica, *Cyberwar and Sabotage*, NEWSWEEK, May 31, 1999, at 38.

3. John Markoff, *Cyberwarfare Breaks the Rules of Military Engagement*, NEW YORK TIMES, October 17, 1999, News In Review, at 5.

4. Bradley Graham, *Military Grappling with Guidelines for Cyberwar*, WASHINGTON POST, November 8, 1999, at A1.

5. *See* Office of 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.

6. Article 2(4) is one of the basic principles in accordance with which members of the United Nations are obligated to act. It provides that "[a]ll Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations." UN Charter, art. 2, para.4.

7. It generally is accepted that "force" under Article 2(4) is not necessarily always an "armed attack" under Article 51. The present discussion leaves to others the attempt to define the circumstances in which the use of CNA would rise to the level of an armed attack or would be a legitimate measure of self-defense under Article 51. UN Charter, art. 51.

8. W. Michael Reisman, *Allocating Competences to Use Coercion in the Post-Cold War World: Practices, Conditions and Prospects, in* LAW AND FORCE IN THE NEW INTERNATIONAL ORDER 26, at 28 (Lori Damrosch Fisler & David J. Scheffer eds., 1991).

9. That the law is unclear and possibly lacking should be no surprise. There can be little argument that Article 2(4) is not well adapted to rapidly evolving technologies. Nor would many be heard to contend that the Charter framework, including Article 2(4), is a perfect and effective instrument for controlling undesirable hostile activities directed by one State against another (not to speak of failing adequately to address the growing threat of hostile activities by non-State actors).

10. Chairman of the Joint Chiefs of Staff, Joint Publication 3-13, Joint Doctrine for Information Operations (1998).

11. Whether that use of force violates international law will depend on the circumstances, including, *inter alia*, the nature of the target (military or civilian), whether the event occurred in war or in peacetime and, in the latter case, whether the operation fell within an exception to the Article 2(4) prohibition (e.g., an exercise of the right of self-defense under Article 51).

12. *See* President's Commission on Critical Infrastructure Protection, Critical Foundations: Protecting America's Infrastructures, at A-48 (1997), *cited in* Michael 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 (1999).

13. For example, the manipulation of a hospital's computer-controlled life-support systems to cause them to malfunction. *See* Lawrence G. Downs, Jr., *Digital Data Warfare: Using Malicious Computer Code as a Weapon, in* ESSAYS ON NATIONAL STRATEGY XIII 43, 54 (Mary A. Sommerville ed., 1996).

14. Downs reports that unidentified persons are studying "psycho-electronics" by which a virus introduced into a computer system causes the video screen to flicker, inducing headaches in users of the video display, such as radar operators. *Id.*

15. The range of potential CNA activities perhaps could be more accurately captured, without destroying the alliterative symmetry of the Joint Chiefs' current definition, by amending it to include "operations to disrupt, deny, degrade, destroy or deleteriously deploy information resident in computers and computer networks, or the computers and networks themselves."

16. *See, e.g.*, Downs, *supra* note 13.

17. *Id.* at 44.

18. *Id.* at 45.

19. *Id.* at 49–50.

20. As noted above, press reports suggest that some form of CNA may have been approved for use by NATO forces in operations against Serbia. *See, e.g.*, William Drozdiak, *Allies Target Computer, Phone Links*, WASHINGTON POST, May 27, 1999, at A1. It appears, however, that what really was involved was the targeting of the public telecommunications system. While degradation of the public switched network almost certainly will cause substantial collateral effects on computer networks, it is questionable whether general attacks on telecommunications or electric power infrastructures, both of which can massively affect computer networks, usefully can be considered a form of CNA. In the case of Serbia, in any event, the question is of little interest in the present context, since NATO's bombing attacks indubitably constituted a use of force. In any event, the United States now appears intent on disavowing any such uses of CNA in the Kosova conflict. *See supra* note 4.

21. *See, e.g.*, General Accounting Office, Information Security: Computer Attacks at Department of Defense Pose Increasing Risks, AIMD-96-84 (May 22, 1996).

22. Ellen Joan Pollack & Andrea Peterson, *Serbs Take Offensive In The First Cyberwar, Bombing America*, WALL STREET JOURNAL, April 8, 1999, at A1.

23. Downs, *supra* note 13, at 49.

24. *See, e.g.*, YORAM DINSTEIN, WAR, AGGRESSION AND SELF-DEFENSE 18 (2d ed. 1994); Albrecht Randelzhofer, *Article 2(4), in* THE CHARTER OF THE UNITED NATIONS: A COMMENTARY 112 (Bruno Simma ed., 1994).

25. WALTER GARY SHARP, SR., CYBERSPACE AND THE USE OF FORCE 88–91 (1999).

26. Schmitt, *supra* note 12, at 908.

27. *Id.*

28. *See generally*, Edward Gordon, *Article 2(4) in Historical Context*, 10 YALE JOURNAL OF INTERNATIONAL LAW (1985).

29. Declaration on Principles of International Law Concerning Friendly Relations and Cooperation Among States in Accordance with the Charter of the United Nations, G.A. Res. 2625 (XXV), UN GAOR, 25th Sess., Supp. No. 28, UN Doc. A/8082 (1970).

30. G.A. Res. 42/22, UN GAOR, 42d Sess., 73d plen. mtg., Agenda Item 131, annex (1988).

31. *See* Schmitt, *supra* note 12, at 905–908, for a discussion of this history.

32. Military and Paramilitary Activities (*Nicaragua v. United States*) 1986 I.C.J. 4 (June 27).

33. *Id.* at 119.

34. *See generally, e.g.*, Schmitt, *supra* note 12, at 904–908.

35. Randelzhofer, *supra* note 24, at 113.

36. Military and Paramilitary Activities, *supra* note 32, at 108, 109–110, 126–127.

37. *NATO Warplanes Jolt Yugoslav Power Grid*, WASHINGTON POST, May 25, 1999, at A1.

38. SHARP, *supra* note 25, at 140. Essentially the same conclusion is reached by a law student author of a case note on information warfare. *See* Todd A. Morth, *Considering Our Position: Viewing Information Warfare as a Use of Force Prohibited by Article 2(4) of the U.N. Charter*, 30 CASE WESTERN RESERVE JOURNAL OF INTERNATIONAL LAW 567 (1998).

39. SHARP, *supra* note 25, at 90–91. The author suggests that CNA having purely economic consequences could even rise to the level of an armed attack, citing the example of a "complete and long-term crash of the New York Stock Exchange." *Id.* at 117. This conclusion appears highly debatable.

40. *Id.* at 101, *citing* IAN BROWNLIE, INTERNATIONAL LAW AND THE USE OF FORCE BY STATES at 113 (1963).

41. SHARP, *supra* note 25.

42. *Id.* at 102.

43. Schmitt, *supra* note 12, at 911.

44. *Id.* at 914.

45. *Id.*

46. *Id.* at 915.

47. One could question the utility of this criterion, since it may well apply as much to economic or political coercion as it does to other forms of CNA and to traditional armed force. While some instruments for exercising such coercion are presumptively legal under both domestic and international law (such as cutting off financial aid to the target State or imposing trade sanctions), others (such as creating economic pressure by massive fraud or theft or destabilizing the target State's political process by corrupt payments to government officials) are presumptively illegal under domestic law and may well violate norms of international law other than Article 2(4), such as the principle of non-intervention.

48. Schmitt, *supra* note 12, at 916–917.

49. Schmitt seems to imply, at least in theory, that there might be a form of CNA that does not cause physical injury or property damage but which causes consequences which approximate the nature of those involving armed force and thus comes within the scope of Article 2(4), but no example is given.

50. Military and Paramilitary Activities, *supra* note 32, at 106.

51. To this effect, see, for example, Michael Glennon, *The New Interventionism*, FOREIGN AFFAIRS, May/June 1999, at 2.

52. W. Michael Reisman, *Criteria for the Lawful Use of Force in International Law*, 10 YALE JOURNAL OF INTERNATIONAL LAW 297, at 280 (Spring 1985).