by Colonel Charles J. Dunlap, Jr., USAF

"The markets were deliberately taken down by a systematic and highly skillful attack" said George Winston, a character in Tom Clancy's recent novel *Debt of Honor*. The "attack," however, was not one of bombs or bullets, it was much more subtle: a computer virus corrupts the New York Stock Exchange's electronic records and millions of transactions are wiped out. But as in every Clancy novel, clever people devise ingenious ways to counteract the assault. Of course the good guys win in the end.

Life can and does imitate art from time to time but often without the happy ending. American commerce and government is dependent upon millions of computers, most of which are vulnerable to cybersubversion.

With computers internationally linked by a bewildering number of cross-connections, tracking down a computer-attacker can be a profoundly difficult task. Suppose, however, that the source of the techno-assault against the Stock Exchange is definitively identified as emanating from the headquarters of the intelligence service of a hostile foreign government. Moreover, suppose the hostile government claims responsibility and threatens further cyber-assaults if its demands are not met. Can the U.S., consonant with the United Nations Charter, launch a bevy of smart bombs or cruise missiles against the offending facility?

The answer is hardly a resounding "yes," and more likely a qualified "no." The adoption of the UN Charter in 1945 had the effect of rendering obsolete traditional notions of "acts of war." The Charter was designed to eliminate the threat or use of force from international affairs. For example, under Article 2(3) of the Charter the signatories have agreed to settle their disputes — including many that might have once been considered "acts of war" — by "peaceful means." Similarly, Article 2(4) requires all members to "refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state...."

The Charter does, however, allow signatories to use force in certain limited circumstances. In addition to actions specifically authorized by the Security Council, unilateral use of armed force is permitted in self-defense. Specifically, Article 51 of the Charter allows force to be used in self-defense "if an *armed* attack occurs against a Member of the United Nations...." [Emphasis added.] The issue then is whether the use of a computer virus equate to an "armed" attack within the meaning of Article 51.

This is a good illustration of where technology is, perhaps, ahead of international law. Although computer viruses can wreak havoc on advanced societies like that of the United States, such "attacks" — at least the economically-oriented one described in this scenario — do not as yet equate to an "armed" attack within the meaning of the UN Charter. As a general rule, "armed" attacks justifying an Article 51 response are largely limited to a significant assault using traditional kinds of weapons.

In the 1986 decision in *Nicaragua v. United States*, for example, the International Court of Justice concluded that Nicaragua's support for rebels in various Central American countries did not justify the "armed" response (i.e., mining Nicaraguan harbors and other covert actions) by the United States.

Further support for the proposition that an "armed" attack warranting an Article 51 response does not include cyberassaults can be found by examining the Charter as a whole. In its outline of actions to be taken against recalcitrant nations, it seems to distinguish between acts constituting "armed" operations and lesser coercive maneuvers. Article 41, for example, discusses "measures *not* involving the use of armed force" and cites as examples the "complete or partial interruption of *economic relations* and of rail, sea, air, postal, telegraphic, radio, and *other means of communication*...." [Emphasis added.]

Analogizing such tactics to a computer virus assault that causes a "complete" or "partial interruption" of the electronic communication of economic information is not difficult. Thus, it appears that the use of a computer virus probably does not *per se* constitute an "armed" attack under the Charter and Article 51 would not justify the proposed military strikes. Indeed, such military action, notwithstanding the virus invasion, might constitute "aggression" — a serious allegation in the post-Nuremberg world.

Some scholars argue, however, that the true meaning of "armed attack" under Article 51 relates to the "intensity of the coercion" imposed. Thus, it might be argued that where the economic damage caused by the electronic attack is of sufficient scale and scope, then the coercion equates to "armed attack" justifying an Article 51 response.

This argument is somewhat stronger, however, if the nature of the cyberattack was different, e.g., if a computer virus let loose by the hostile nation infected all kinds of computer systems, not just economic ones like the stock exchange. If, for example, a virus destroyed the computer controlling the power grid or the telephone system serving a major urban area, hundreds if not thousands of innocent civilians could die (e.g., elderly people could freeze to death, emergency 911 calls would be blocked, etc.).

Under such circumstances, clear evidence of reasonably foreseeable deaths directly attributable to the "attack," it *might* be possible to equate a computer virus assault with an "armed" attack as used in Article 51. Indeed, most experts would agree that where data manipulation directly results in significant destructive effects that are indistinguishable in any meaningful way from those caused by traditional (kinetic) weapons, such assaults constitute "armed attacks" for purposes of Article 51.

Even if the particular action does not warrant a military response under Article 51, this does not mean that the United States would be without recourse. Domestic criminal law may apply, and the U.S. could take the matter to the Security Council or other international fora for resolution. The Security Council could authorize military force against offending state even in the absence of an "armed attack." The requirement for an "armed attack" applies only to the authority to engage in self-defense pursuant to Article 51.

Furthermore, just because a particular cyberassault does not authorize a military strike does not mean it is legal under international law. A whole range of international agreements may be violated. The doctrine of state responsibility holds that every breach of international law creates a duty to pay for any loss or damage that results.

Moreover, an important new study by Commander James N. Bond of the Naval War College asserts that victims of an unlawful cyberattack that does not amount to a use of force may take proportional countermeasures that also do not amount to a use of "force." He maintains that one such response might be a "tit-for-tat" data manipulation.

All of this suggests a need to establish an international consensus as to the meaning and consequences of cyberattacks. One obvious method of qualifying cyberassaults as "armed attacks" is to simply define electronic methodologies as "weapons." In this respect a 1974 UN resolution defined the "use of *any* weapons by a State against the territory of another State" as "aggression." The United States, however, should approach such proposals with caution. They may result in unintended limitations when applied to the range of emerging new technologies. While the U.S. has many vulnerabilities to cyberassault, it also has great potential capability.

Nevertheless, as the world becomes more cybernetically dependent, real lives become at risk in the 'virtual' environment. Moreover, corrupting the vast databases of industry the Federal government can easily do as much damage as the physical destruction that dozens of enemy bombers could wreak. The United States needs to be able to deter the specter of such assaults by all means at its disposal — including traditional military strikes.

❖End❖

Colonel Dunlap is Staff Judge Advocate of United States Strategic Command. He has a B.A. from St. Joseph's University (PA) and a J.D. from Villanovoa University School of Law. He is a Distinguished Graduate of the National War College. All views and opinions he expresses are his alone and not necessarily those of the Department of Defense or any of its components.