Document created: 31 July 00
Air & Space Power Chronicles - Chronicles Online Journal

Information Operations: An Act of War?

Maj David J. DiCenso, USAF, Reserves

I. Introduction

Somewhere deep in Iraq sits a 24-year-old computer programmer, a graduate of the University of California at Berkeley. More than 60% of Berkeley's student body in technology-related subjects are foreign nationals;[1] he was among them. He learned all that he could about computers, networks, computer telecommunications protocols, and system architecture at U.S. educational institutions. Now he's a graduate, at home in Iraq. He's been hired by a foreign terrorist group to infiltrate U.S. Department of Defense (DoD) computers to gather intelligence on U.S. military operations. When his handlers noted his remarkable ability to glean precisely the information desired, he was paid to go one step further … to infiltrate DoD systems and carefully place "sniffers" (computer programs designed to collect passwords from those who log on to the system) on specific computers within the target nation's borders. After obtaining a sizable number of passwords through the use of these sniffers, he used the information to log on and gain root access to the systems; he was now considered a *Super User* by the computer system. All of the abilities and authorizations that the system administrator had on the computer network were now at his disposal.

Before long, he obtained access to both the unclassified as well as certain classified DoD communications networks. Once again impressed, his handlers directed him to delete some important DoD information, deny access to other information, and to replace some information with false data created by his handlers. This was to be timed such that it would occur in conjunction with several other key world events, all precisely choreographed to further the goals and interests of the terrorist group.

Suddenly, the U.N. forces in Bosnia received beans instead of bullets. The personnel records of all deployed U.S. forces suddenly disappeared. Instead of receiving expected e-mail traffic, in-theater leaders received strings of computer-generated obscenities and irrelevant passages from the World Book Encyclopedia. Suddenly the in-theater commanders couldn't trust any of their electronic data; even data that "sounded right" still had to be checked and double-checked for accuracy, as all data reliability was suddenly suspect. The military members whose records had been deleted were suddenly no longer on the payroll, causing individual financial difficulties to the soldiers and their families. Morale plummeted

while fear and frustration grew at an alarming rate. Telephone switchboards at the U.S. House and Senate were jammed with dependent spouses demanding relief from their financial woes, blaming the DoD for the disaster.

Confusion reigned in the field, too; command and control above the squad level was practically nonexistent. The delays, lack of information, and misinformation practically incapacitated the commanders' ground forces. Similarly distrusting their information as well as the information passed by allied ground forces, the air support elements were grounded pending resolution of the data security issues. It certainly wouldn't play well in the international media to make targeting errors that could violate the Law of Armed Conflict and drive the international opinion against the U.S. and its Bosnian involvement. Computer systems owned by the manufacturer of the F-22 "Raptor" had been broken into as well, causing the code used by the fighter system to become suspect. Nobody even dreamed of flying the aircraft in the deployed theater.[2]

All of this damage was caused by a lone foreign civilian on the payroll of a relatively unknown terrorist group. He had successfully incapacitated (at least for a time) the entire operations of the U.S. military forces involved in a coalition U.N. peacekeeping mission, and generated a great deal of international disdain for the once-proud "superpower" that had fallen to its knees in a few short hours. After the Tomahawk "anticipatory self-defense" action by the U.S. in Sudan, several other terrorist organizations suddenly felt at risk, and quickly became interested in retaliatory and preemptive computer attacks upon the United States. The young Berkeley graduate soon found his services in high demand.

Although it sounds far-fetched, it's not completely unforeseeable. Technology has expanded at an astronomical rate over the past several years, making logarithmic leaps in both complexity and utility. As technology has dramatically increased, so has our dependency upon it. As we have discovered the efficiency of these technological advances, we are slowly weaning ourselves of the once-predominant "low-tech" ways to perform these same functions. For this reason, an effective computer intrusion followed by additional adverse information operations (such as data "theft," corruption, denial, or delay) could be more devastating than we realize.

If these types of operations could be launched against the U.S. (and its computer networks), it makes sense for us to explore the applicability of this technology to similar operations. Are we doing so?

> The full extent of U.S. offensive capabilities is among the most tightly held national security secrets. According to various accounts, the government has explored ways of planting computer viruses or "logic bombs" in foreign networks to sow confusion and disruption. It has considered manipulating cyberspace to disable an enemy air defense network without firing a shot, shut off power and phone service in major cities, feed false information about troop locations into an adversary's computers and morph video images onto foreign television stations.[3]

Although there is practically no unclassified information available regarding U.S. offensive information

warfare capabilities or programs, George J. Tenet, the director of central intelligence, has commented "we're not asleep at the switch in this regard."[4] The available technology provides many new applications that far exceed the ethical limitations on such use, according to one high-ranking DoD official.[5] We can assume that every technologically modern country is aggressively pursuing a "cyberwar" program, including both info-protect and info-attack types of operations.

II. Issues

How should a computer network intrusion be viewed by the affected "victim" state? Is some level of intrusion acceptable? When does a computer intrusion "go too far?" How should the victim of the attack respond? When does an information operation become information warfare? When does an information operation become an act of war? As of July of 1998, there has been no Presidential Directive or plan to respond to definitional and operational difficulties that these issues raise. There has been no public Congressional discussion regarding these issues, nor have they promulgated any guidelines for use of offensive Information Operations (IO) capabilities.[6] In 1997, the DoD created the joint Information Operations Technology Center at the National Security Agency (NSA). The NSA is a "black world" organization responsible for spying on foreign communications, including computer networks,[7] but the overarching policy that would drive decisions surrounding the limits of peacetime IO is notably absent, at least in the unclassified world. This report is an attempt to respond to some of these difficult issues.

III. International Law

Some general guidance on these perplexing issues may be found in the history of the use of force, the Law of Armed Conflict (LOAC), and the Charter of the United Nations. Although these sources do not provide definitive answers, the guidance they provide is instructive at least, and may help set some parameters for future development of the law in this area.

a. Historical Context of the Use of Force

Up until the early twentieth century, there was no effective prohibition upon a nation's ability to resort to war as a political tool. Either nation involved could freely resort to the use of arms, force, and war to resolve conflict as that nation saw fit. A theory that "just" wars were supportable and morally defensible seemed to be the prevailing thought. The logic of the day was that "[c]ontemporary public international law does not know of any rules about when it is permissible to wage war. If a state so decides, it may resort to war at any time. Force is thus permitted in the relations between states without any conditions."[8] Although nations could freely enter into war at will, later developments curtailed the unrestricted right of a nation to wage war.

b. The Law of Armed Conflict

Under the Law of Armed Conflict (LOAC), the determination of whether an Information Operation (IO)

activity is an "act of war" is determined by the nature of the activity itself. The Hague Convention and subsequent Protocols were created in the days of weapons that provided blast, heat, and fragmentation damage. It is clear that these types of kinetic weapons were exclusively present in the minds of the drafters. They could not have foreseen the importance of computers and network security tools as a means of waging war. Although it's true that IOs have been deemed critical at least as far back as Sun Tzu,[9] the modern computer network instrumentality for undertaking the information operation was not readily foreseeable. Thus, the LOAC defines war as warfare by a belligerent nation involving actual arms … weapons that deploy kinetic energy to cause the enemy some form of physical damage. Unfortunately, electrons and binary digits floating through computer networks and into another computer is *not* the equivalent of armored divisions rolling across a national border.[10]

Thus, the LOAC is founded upon notions of armed conflict in purely kinetic terms, while the conventions and protocols are silent on the utilization of a modern ***Electronic Network Information Operation*** (ENIO) as an instrument of international conflict.[11] Despite the myriad times U.S. military members have engaged in some type of armed conflict in the recent past, the last time the United States actually declared war was at the onset of World War II. A substantial amount of "war fighting" has been done by the United States while not technically "at war." It would seem that the analysis of whether an ENIO is an "an act of war" under the LOAC is unnecessary and irrelevant. If the LOAC will not provide helpful guidance in determining how far we can go with ENIO, where else might we seek an answer?

c. The United Nations Charter

The Charter of the United Nations may be a better source of modern authority that could provide us with some instructive, practical guidance. Under the U.N. Charter, the old concept of an "Act of War" becomes practically obsolete. The Charter is founded in several bedrock principles, articulated in Article 1, paragraphs 1 through 4:

> 1. To maintain international peace and security, and to that end: to take effective collective measures for the prevention and removal of threats to the peace, and for the suppression of acts of aggression or other breaches of the peace, and to bring about by peaceful means, and in conformity with the principles of justice and international law, adjustment or settlement of international disputes or situations which might lead to a breach of the peace;
>
> 2. To develop friendly relations among nations based on respect for the principle of equal rights and self-determination of peoples, and to take other appropriate measures to strengthen universal peace;
>
> 3. To achieve international co-operation in solving international problems of an economic, social, cultural, or humanitarian character, and in promoting and encouraging respect for human rights and for fundamental freedoms for all without distinction as to race, sex, language, or religion; and

> 4. To be a centre for harmonizing the actions of nations in the attainment of these common ends. [12]

Article 1 of the UN Charter articulates the principles of the organization, including the prevention of acts of aggression and breaches of the peace. Interestingly, Article 1 recognizes the concept of "peace over justice".[13] Justice was not incorporated into the primary operative mandate of Article 1.[14] The Article lists peace and security as the primary goals to be maintained and only mentions that they may be preserved or secured in conformity with the principles of justice and international law. This clearly makes "justice" subordinate to "peace and security." The preamble also echoes that concept.[15] Article 1 also refers to the prevention of breaches of the peace. Interestingly, this phrase is not defined anywhere in the Charter. The Charter indicates only that the organization is to suppress "acts of aggression or other breaches of the peace."

Article 2 of the Charter recognizes the principle of sovereign equality of all members,[16] and that all members agree to settle their international disputes by peaceful means,[17] refraining from the threat (or use) of force against the territorial integrity or political independence of any state.[18] Even if the peaceful settlement of disputes was not included in the Charter, the basic, fundamental concept is already firmly imbedded in the body of international law as a matter of custom.[19]

The evaluation of how ENIOs conform with the Charter is much more helpful than attempting to define an "act of war," and the implications are much more practical. Additionally, a discussion of whether an IO conforms with the provisions of the Charter and how the Security Council would view the ENIO is useful as well. Should a member country violate the Charter, the U.N. Security Council will determine the existence of any threat to the peace, breach of the peace, or whether an act of aggression had occurred.[20] The Security Council may also decide whether remedial measures are necessary, up to (and including) armed intervention.[21] These remedial measures may include traditional armed force as well as a lesser degree of intervention that expressly excludes armed force. "These may include complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations."[22]

It is important to understand the provisions of Article 41 of the Charter (quoted above). Interruption of telegraphic, radio, and "other means of communication" are listed as specific measures that do ***not*** involve the use of armed force. Clearly, "other means of communications" fairly encompasses computer communications and communication over computer networks. We could, therefore, undertake the ENIO equivalent of broadcasting radio interference to interrupt radio communications. Could we instead transmit false information to interrupt communications without severing them? Denying information or sending misinformation has long been an accepted subterfuge by countries in time of peace as well as in times of war.[23] Logical progression leads us to conclude that sending fabricated *computer-generated* messages falls within this same category. Intercepting information from a foreign country, altering the meaning of the information, then re-transmitting the information to the originally intended recipient would also logically fall within this category. It seems that Article 41 permits countries to deprive

another nation of its communications, as well as interrupting communications by manipulation of the target country's data such that it is corrupt and untrustworthy, altering the data to render it useless for that nation's purpose, and actually altering the data such that it achieves an intended purpose for the aggressor nation. Although this sounds like *carte blanche* for operators to engage in ENIO, the provisions of Article 41 still require the Security Council to decide what measures are to be employed under that article, including force and actions that do not include armed force.[24]

The provisions of Article 51 of the Charter are not directly related to Electronic Network Information Operations, but becomes relevant as it provides member states with the opportunity to act in self-defense. "Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken the measures necessary to maintain international peace and security."[25] This demonstrates that the long-standing tenet of international law that justifies unilateral action by a member state is upheld, even under the restrictions of the U.N. Charter, at least until the Security Council can act. Determining how a "target" country will react, or may legally react, under the Charter may help us plot our strategy in ENIOs, as will be discussed later in this paper.

The power of the Security Council is very broad. The Security Council is composed of fifteen members. Among these fifteen members are several "permanent members."[26] The permanent members are the "Republic of China, France, The Union of Soviet Socialist Republics, the United Kingdom of Great Britain and Northern Ireland, and the United States of America."[27] The General Assembly of the U.N. elects ten other members of the U.N. to be non-permanent members of the Security Council.[28] Decisions regarding procedural matters are made by an affirmative vote of nine members of the fifteen member Security Council. Decisions on all other matters are made by an affirmative vote of nine members as well, however, the permanent members must all concur.[29] Thus, a single permanent member of the Security Council could frustrate the intentions of a member nation or of the remainder of the Council.

d. Interplay Between LOAC and the U.N. Charter

If the U.N. Charter seems to categorize ENIO as "measures not involving the use of armed force," has the LOAC become an irrelevant relic or a vestige of ancient protocol? Not by any means. The tenets and doctrines of the LOAC are still very relevant to international relations and the conduct of information operations. Although the *letter* of the LOAC may not seem wholly applicable, the *principles* of the LOAC certainly are. "The Armed Forces of the United States will comply with the law of war during the conduct of all military operations and related activities in armed conflict, however such conflicts are characterized and unless otherwise directed by higher competent authorities, will apply law of war principles during all operations that are categorized as Military Operations Other Than War."[30] Any action contemplated, whether achieved through traditional kinetic means or ENIO, must conform to the principles that have evolved as the Law of Armed Conflict. For example, destroying a communications hub with traditional bombs requires war-fighters to balance the risk of collateral damage against the tactical or strategic benefit gained before firing.[31] Why should an information operation require any less? If we can shut down communications by infiltration of a computer network to do the same job,

shouldn't we also perform the same balancing test to ensure that we do not violate the same LOAC principle?

The Law of Armed Conflict is based upon specific prohibitions as well as a few basic principles: humanity, military necessity, proportionality, and chivalry. Where the facts are not covered by a specific prohibition, the fundamental principles should govern the conduct of state actors.[32] Humanity requires that we mitigate human suffering, and that any wounds suffered heal as painlessly as possible while we conduct ourselves within the dictates of the public conscience.[33] Military necessity permits us to apply any amount and kind of force to cause the complete submission of the enemy while minimizing the expenditure of time, life, and money; a reasonable connection must exist between the destruction caused and overcoming the enemy's resistance.[34] Proportionality requires us to balance the loss of life and damage against the value of the military objective to be gained. If the potential value of the objective does not outweigh the loss of life and damage, then the action violates the rule of proportionality.[35] Although the LOAC does not answer the burning, specific questions regarding ENIO, it still provides overarching fundamental principles that should guide our actions, regardless of the path we take to realize our tactical, operational, or strategic goals.

IV. What CAN We Legitimately Do?

The law always lags behind technology. Although this is not particularly convenient, it is generally necessary. Technological advances arise and new, innovative applications are found for those technologies. Military members are all familiar with the advent of submarine warfare and aerial warfare and the fact that there were few rules that applied to those arenas of conflict. Over time, rules emerged to govern these new technologies in their use against other states. This, too, is how it must happen with computer network technology. Although some may condemn the legal community for their perceived failure to be forward-looking, one must understand the role of law in international relations; it is traditionally a method to resolve disputes and one must patiently await the time when a dispute arises or all parties readily foresee a dispute arising in the near future. Only then will the states involved be ready and willing to act.

As described hereinabove, the U.N. Charter and the LOAC seem to set some parameters upon the use of ENIO. The inchoate nature of the law in this area has caused a great deal of confusion for operators. Operators simply want a pragmatic answer to the question, "what can we legitimately ***do***?" The law is being shaped and formed slowly to respond to the new technology. If we could predict what shape the law in this area is likely to take in the future, we may better plan for operations in that environment. Although it is a new (largely uncharted) area of law, we are not without clues as to what might occur. We have current law and custom upon which we may rely to provide analogies that can be extrapolated into the information operations environment. As the application of rules for aerial bombardment arose through analogy with naval bombardment, so may analogies assist us in shaping our understanding of the law as it applies to ENIO.

a. Analogies

If an IO included simple monitoring of open communication systems that are available to the general public, one would be hard-pressed to argue that eavesdropping upon these communications violates any tenet of law. This would be similar to a U.S. agent simply walking down the street and overhearing a loud conversation made in a public place. There is no recourse for the government who failed to communicate in a more secure fashion. There is no legitimate argument that the government agent who overheard the conversation did anything untoward. This would certainly not be an incident where the subsequent use of force by the "victim" state would be warranted.

The next step is the Trojan Horse. This idea presumes that we create a malignant virus, but we do not send it anywhere or do anything immediately offensive with it. Instead, we choose a computer program or file in one of our systems that a foreign government would like to have, and load the file with our own active executable program, much like the Trojan Horse being loaded with soldiers. We foresee that a foreign actor would want to "steal" that information - and we want him to download more than he bargained for! We place this program or file in the system where a snooping electronic intruder would likely find it. When he "steals" it, the malicious virus is then released and replicated on his system, thus causing damage and potentially devastating effects within his own computer system. One obvious problem with this tactic is the potential that the virus could become uncontrollable.[36] Although a virus may attack a single system, a mutating virus or a worm would introduce complications. Once released, we could not control what systems a worm or mutating virus would eventually attack or damage. In an interconnected world, a worm or mutating virus such as this could easily run amok on the network of networks that comprise the World Wide Web and eventually cause damage and destruction to our own systems. We cannot forget the LOAC's rule of proportionality, either. As you recall from our earlier discussion of the LOAC, we should refrain from any indiscriminate attack or any attack where the incidental loss or damage to nonmilitary targets outweighs the military advantage to be gained from the attack. Here, if a Trojan Horse were used and we were unable to control how, when, or where it replicates, the damage to civilian networks would likely outweigh any military advantage; particularly if the Trojan virus were left simply as an electronic minefield to attract intruders and subsequently "teach them a lesson," even though we don't know who "they" are. It would simply be unjustified. There may be some similar computer programs which would not violate the principles of the LOAC. If there were a software application used only by the military community in another nation, and the virus were of a variety that would only affect that specific software application, the analysis might be different. In the case presented, however, the likelihood of collateral damage to inappropriate targets would likely be too great to warrant the Trojan Horse approach. The problems presented by this tactic are magnified if one considers an otherwise benign domestic hacker who, while snooping around in the system motivated by a simple pursuit of entertainment, stumbles upon - and detonates - the Trojan Horse. This could potentially damage our own infrastructure and result in the very information corruption or denial of service that we feared in the first place.

What if the ENIO includes an actual penetration into the target nation’s computer system by United States operators? This necessarily entails involvement greater than simple monitoring of "public view" conversations or putting a minefield in your own system. This presumes that a DoD computer operator actually enters, electronically, the target’s systems and does *something* while there. Whether it was

merely accessing the system through use of human intelligence (HUMINT), communications intelligence (COMINT), or by simply guessing passwords, the U.S. operator transmits some commands or otherwise passes bits and bytes of information into the target system. Suddenly the activity is no longer passive. Actual penetration of the target nation's computer system would be tantamount to a U.S. agent breaking into another nation's embassy. Such an embassy intrusion wouldn't be taken lightly, and neither would the computer intrusion. Whether that U.S. agent undertakes a physical "break-in" or an electronic one, it is still intrusive. Although this could be treated as a violation of Article 2 of the U.N. Charter,[37] it could also be addressed under the criminal law paradigm, and the issues of "spying" would be resolved through the State Department. If the intrusion released information absolutely critical to national defense, it could elicit an "armed force" response under Article 51 (the self-defense provision) of the U.N. Charter. Note, however, that the argument for "self-defense" is considerably weakened after the act has occurred - responding AFTER the attack is more akin to a parting shot than "self-defense." Furthermore, Article 41 seems to indicate that an ENIO is *not* use of armed force; thus Article 51's provisions regarding self-defense are not implicated and the target country could not respond with a kinetic strike in response to the ENIO intrusion. It would likely be a "breach of the peace," and the Security Council could act, but the victim nation is prohibited from an armed response to the electronic attack. There is an argument that a nation may act in "anticipatory self-defense,"[38] but this is a convoluted area of law and is well beyond the purview of this paper. For legal analogy purposes, there should be no substantive difference between an electronic intrusion or a physical intrusion into a nation's sovereignty.

Let us consider a case that goes one step further. Assume that the ENIO includes not only intrusion, but also some type of activity that causes no immediate or discernible damage, but somehow leaves a potential for future damage that lingers after the intrusion has ostensibly ended. For some time hackers have had the capability to enter a system and leave behind a "back door" to ease future reentry into that very same system if a future need to do so should arise.[39] Once the hacker has gained access to the system, he or she can secretly leave a reentry mechanism such as this "back door" behind for use when necessary at some indeterminate future time. The technology currently exists that would permit a system infiltrator to enter a computer or networked communications system and leave a "logic bomb" that would detonate at a later date or upon later command of the state that placed the "bomb."[40] This takes us a step higher on the conflict spectrum because we not only have an intrusion to contend with, but also a real impact upon another nation's computer infrastructure system and, arguably, their sovereignty in violation of the spirit of Article 1 of the Charter. Again, without actual damage (other than observation or a "taking" of data), it would be difficult to characterize the infiltration itself as an activity that would justify an armed response (like self-defense). It would also be very difficult to establish the identity of the intruder, or determine whether it is the action of a foreign state, a terrorist, or a lone hacker with no political motivations. If the attacker could be identified, the conflict would, most likely, remain a battle of electrons within the confines of Article 41 until the Security Council could act. Surely the Security Council would deem this electronic duel as a "breach of the peace" under Article 39 and would take remedial measures. It would certainly become a hot topic of debate between heads of the states involved and likely the Security Council and/or the General Assembly of the United Nations if the intrusion was followed by the evidence of a logic bomb or other malicious code. The political morass would be exacerbated if a Security Council permanent member vetoed any remedial action by the Council.

One step higher in the conflict spectrum is the situation where a government agent actually denied services, corrupted data, or placed alternate data in the target country's computer system, resulting in a shutdown of that country's infrastructure assets (loss of power, utilities, air traffic control, etc.) potentially causing chaos and death in the target nation. We have now undoubtedly entered the arena of offensive Information Warfare (IW). Although no bombs or missiles have been dropped or launched, the target country has suffered actual, tangible damage. It would be difficult, indeed, to convince the targeted country that they were not under attack. Most likely, the "victim" state would believe that they had the authority (and perhaps a "duty") to defend themselves under the authority of Article 51 of the U. N. Charter. Surely most victim countries would perceive this as an "act of war," "use of force," or "act of aggression," or whatever terminology they decided would best serve to justify their retaliatory action. Academic debate of semantics would abruptly end when news programs could broadcast images of the tangible results such as aircraft wreckage, starving city dwellers, hospital intensive care units without power, riots, *et cetera*, and negative attention would turn toward the aggressor state.

Could the U.S. become sanguine as a permanent member of the Security Council and engage in ENIO with impunity, knowing full well that it can veto any adverse action the Council contemplates? Does this mean that the U.S. is the "big dog" in the neighborhood and that it can do whatever it pleases? Not by a long shot! The power and authority of the United States in the global community is based upon respect and trust. Should the technical operation of the U.N. be twisted to the United States' advantage to achieve some short-term goal, the long-term repercussions may be dramatic. Further, inaction or inappropriate action by the Security Council and the role of the U.S. therein may cause the General Assembly to sit as a united body to censure the Security Council and the United States. To believe that the Security Council veto power is an "escape clause" for anything the U.S. feels like doing is to ignore the international political realities of a globally interdependent community. The Court of International Opinion is substantially more important and relevant than any codified rule or law that exists under the language of the U.N. Charter.

As previously mentioned, the U.S. is a permanent member of the Security Council with veto power. It is unlikely that the U.S. would ever vote to censure itself or vote to take remedial action against itself. However, should the facts and circumstances arise involving nations who are not permanent members, the precedent for resolving the issue may be "written in stone" long before the U.S. becomes involved as a party to the dispute. Normally, if the U.S. were an interested party, it would be appropriate for it to simply abstain from voting.[41] Otherwise, the U.S. must consider future repercussions to the nation in addition to the current dispute under examination. If the issues are not resolved favorably for U.S. future interests, the rights and responsibilities of the parties may evolve into an operational, legal, and political morass that is ultimately contrary to U.S. interests and security.

b. Terminology

The value of attempting any legal definition for terms such as "act of war," "use of force," and "act of aggression" is suspect at best. There is simply no value in expending any time, energy, or effort to

determine precisely how to define these phrases. Article 41 tells us what a use of force is not, and those acts would thus not warrant a kinetic self-defense strike under Article 51. Thus, for purposes of ENIO, the definitions are practically extraneous.

Similarly, the old-fashioned "act of war" analysis seems inapplicable. The U.N. Charter provides no guidance for defining an "act of war," but it clearly proscribes violence without the involvement of the UN Security Council.[42] The Charter does not use the "act of war" language, but it does contain the phrases "use of force,"[43] "armed attack,"[44] "armed force,"[45] and "acts of aggression."[46] From the perspective of the Security Council's authorization and ability to take action, these terms become less important. Article 39 permits the Security Council to take action based only upon a finding that a mere "breach of the peace" has occurred. When a nation undertakes an operation that may be deemed a "breach of the peace" by the Security Council, they have exposed themselves to international scrutiny and potential sanctions by the United Nations.

V. A Pragmatic Approach

Suppose a country is spoiling for a fight. Suppose also that another country has engaged in ENIO against that country; no death or destruction has yet occurred. The target country is eager to creatively interpret this vague "armed attack" phrase found in Article 51 of the Charter, as they'd like to launch a kinetic response. Would their argument succeed? Probably not. The Charter seems to indicate that information operations are not tantamount to the "use of force." Article 41 sets out activities that the Security Council may undertake to give effect to its decisions and specifically articulates several activities which are deemed "***not*** involving the use of armed force" (emphasis added) which fairly encompass ENIO.[47] Therein lies the rub for the targeted nation. If they feel that their sovereignty has somehow been compromised, it would seem that a response in-kind would be authorized. Should they undertake a kinetic response, they would likely be deemed to be the aggressor and the *target nation* could respond in self-defense under Article 51.

The largest danger occurs when a country adept at ENIO targets a nation without similar technological capability in the electronic environment. ENIO in such an environment could precipitate derogation of relations to the point where the disadvantaged nation resorts to a kinetic attack, driven by a different view of the applicable international law, of technology, or by wholehearted belief in some religious doctrine that demands a *jihad* when an assault upon its sovereignty has occurred. If backed into an electronic corner, the lesser-advanced country may respond with the only weapons it has available (regardless of what the U.N. Charter would deem appropriate). At this point, the political (and practical) considerations far outweigh the legal ramifications of an ENIO. There is a good argument that the determination of whether an IO activity becomes an "act of war," "act of aggression," or "use of force" depends upon the damage that occurs.

Where a country obtains information by non-intrusive measures, there would be no issue. Where some clearly offensive weapon were to be employed such as an ElectroMagnetic Pulse (EMP) weapon or High Energy Radio Frequency (HERF) gun,[48] it would be easy to make the analogy to conventional weapons.

Where the damage was done using ENIO, the conclusion that an "armed attack" had occurred would be more difficult to reach. Whether the targeted nation is likely to respond as though it were an "armed attack" would depend upon whether its infrastructure were badly damaged, whether they suffered high casualties, or if threats to their national defense had occurred.[49] As discussed earlier, law is generally reactive; some world event or foreseeable problem precipitates a rule, law, or treaty to prevent an incident from occurring or recurring. Law also generally parallels common sense. Thus, a practical, pragmatic analysis may represent the most logical approach to the issue, regardless of the technical language of the U.N. Charter and governing international law and custom. If a targeted nation experiences casualties and dramatic loss, the leadership (and people in non-belligerent nations) would likely view the electronic activity as an attack. In such a case, the targeted country may well respond with ENIO (if they don't feel the international community is sympathetic enough with their plight) or kinetic measures (if they believe they can portray themselves as the victims of an "armed attack"). The political and policy considerations of the ENIO far outweigh any legal considerations. Having a solid argument for the offensive ENIO under the technical language of the Charter is good, but it becomes unpersuasive when the sentiment of the world is against us. To "legally" win is pragmatically unimportant when we have been tried and convicted in the court of international public opinion.

VI. Conclusion

Policy considerations are paramount before any nation even considers use of ENIO in anything other than a purely non-intrusive manner. The U.S. is by far the most technologically advanced nation with dependency upon practically every aspect of electronic and computer technology.[50] Computer information assurance contemplates risk management principles; we quickly recognize that we cannot completely protect our systems in the dynamic environment of cyberspace.[51] Our computer security only begins to approach the level it should attain before we can feel confident that we are relatively free from enemy strategic or tactical intrusion. The U.S. military is highly dependent upon its civilian infrastructure, particularly for telecommunications services.[52] Additionally, the U.S. financial giant is heavily dependent upon computer technology. No one could plausibly argue that the United States' financial strength is not an integral element of its national security,[53] for without economic might, our political and military might is diminished as well. Understanding that the U.S. is the world's heaviest technology and computer user (and most likely has the greatest vulnerability to ENIO), does the U.S. really want to begin a new era of cyberoperations as a unilateral activity and flex its understanding of international law to the point where it can arguably justify its actions by wordsmithing arguments to the international community? Does the U.S. really want to play cyber-cowboy and push the limits of the uncertain law, even though it recognizes that it has more to ***lose*** than any other nation on earth?

The question of whether an ENIO is an "act of war" is an obsolete notion, and a question that has become irrelevant due to the increasingly global nature of the United States' influence and the "fuzzy" nature of the U.N. Charter. What ***is*** relevant is determining what constitutes a "breach of the peace" that would enable the U.N. Security Council to act. Obviously, this is more of a political issue than a legal one. The United States' leadership in the U.N. is relevant too. If the U.S. wishes to retain its status as a true world power, it must nurture the respect that other countries have for it, and act to preserve and

expand its authority within the U.N. This necessarily entails compliance with the U.N. Charter, whether the U.S. likes it or not. Although the Charter seems to treat IO as though it were not the use of "armed force," an intrusion into another country's electronic infrastructure is nonetheless a potential breach of that country's sovereignty and the Security Council would likely become involved. Thus, the resolution of any ENIO issues would probably occur at the U.N. and the heads of state level, not by any subordinate military or civilian organization. These are monumental issues of international policy.

The onus is now upon the United States. The U.S. has long been a leader in the development and expansion of international law. It has been a powerful member of the United Nations. It must continue to exercise its leadership and foresight to ensure that the legal landscape crafted to deal with this area of law conforms to its national interests and does not undermine its strength. We clearly foresee ENIO problems looming on the horizon. The analysis presented in this paper seems to resolve many questions, but it leaves many of them unanswered as well. An extrapolation of existing law and custom may help define the parameters of the problem, but do not offer a definite approach. There is obviously some remaining "wiggle room" for a country to exploit. There is room for meaningful expansion of these rules and it would benefit the international community to clarify precisely how ENIOs should be handled when they occur. Although the U.N. Charter, international custom, and LOAC are all applicable, it seems that this area of law is ripe for advancement and must evolve to a greater level of sophistication to effectively deal with these issues in the future. The U.S. understands the import of these issues and the problems that could occur if some internationally acceptable guidelines are not promulgated. The United States needs to focus attention on this issue immediately and accelerate its efforts to officially and explicitly resolve these issues on an international political level in the best interests of international policy and national security.

End Notes

1. Foreign national student statistics gathered via telephone interview with official source at the University of California, Berkeley.

2. There are in excess of 1.2 million lines of code in the systems of the Raptor F-22 fighter platform. Obviously, testing such a mammoth program presents complex problems, especially if the data itself were suddenly deemed "untrustworthy." One can easily imagine the manpower and time required to "de-bug" such a complex system under wartime conditions, potentially resulting in the failure of the mission or restructure of the mission to employ alternate platforms. (The "1.2 million lines of code" comes from a personal conversation on 6 Oct 98 with Capt Anne Clark, Department of Electrical Engineering, USAF Academy, and former Mission Software Engineer and Mission Software Integrated Product Team Lead at the F-22 Systems Program Office.)

3. Bradley Graham, "Authorities Struggle with Cyberwar Rules," Washington Post, 8 July 98, p. A1. Also found at http://www.washingtonpost.com/wp-srv/frompost/july98/cyberwar8.htm.

4. *Id.*

5. *Id.* (citing an unnamed official who requested anonymity).

6. *Id.*, generally.

7. *Id.*

8. Bruno Simma *et al.*, "The Charter of the United Nations: A Commentary," Oxford University Press (1995), 109.

9. Sun Tzu: "All warfare is based upon deception" and "[t]o subdue an enemy without fighting is the acme of skill." Samuel B. Griffith, "Sun Tzu: The Art of War," Oxford University Press (1971), 66 and 77, respectively.

10. FM 27-10, "The Law of Land Warfare" (July 1956), Chapter 1, Section 8 (p.6), indicates that war is defined as a "legal condition of *armed* hostility between States" (emphasis added). Armed conflict without "war" is contemplated in accordance with the provisions of the UN Charter. It continues, in Chapter 2, section 20 (p. 15), that "hostilities... may not commence without previous and explicit warning, in the form either of a reasoned declaration of war or of an ultimatum with a conditional declaration of war." The context and background of the Laws of War (and the LOAC) clearly indicate that the drafters envisioned traditional weapons violating geographical borders to trigger the provisions of the governing law.

11. Information Operations and Information Warfare do not adequately describe the operations discussed here. Many view the phrase "information operations" to include traditional psychological operations (PSYOPS) and the utilization of techniques that are not the subject of this discussion. Similarly, the phrase "information warfare" seems to jump to the conclusion that we are waging war, when clearly we do not intend to specify an extreme level of conflict when we strive to contemplate and discuss a full range of electronic network operations. I have used the phrase "electronic network information operations" or "ENIO" to better describe exactly what we are contemplating: the use of computers and network technology to affect or exploit information or communications of a target computer or computer network.

12. U.N. Charter, art. 1, ¶¶ 1-4.

13. *See* Cmdr. James N. Bond, JAGC, U.S. Navy, "Peacetime Foreign Data Manipulation as One Aspect of Offensive Information Warfare: Questions of Legality under the United Nations Charter Article 2(4)," 14 June 1996, p. 16.

14. *Id.* at 16-17.

15. *Id.*

16. U.N. Charter, art. 2, ¶ 1.

17. *Id.*, ¶ 3.

18. *Id.*, ¶ 4.

19. *Nicaragua v. United States* (1986), ICJ pp. 14 *et seq.* at 145. *See also* Yoram Dornstein, War, Aggression, and Self-Defense, (Cambridge: Grotius Publications Limited, 1988), 91-94.

20. U.N. Charter, art. 39.

21. *Id.*, arts. 39, 41, 42, and 46.

22. *Id.*, art. 41.

23. *See e.g.*, FM 27-10 "The Law of Land Warfare" (July 1956), Chapter 2, Section V, ¶ 51 (p.22).

24. U.N. Charter, arts. 23 and 39.

25. *Id.*, art. 51.

26. *Id.* art. 23 ¶ 1.

27. *Id.*

28. *Id.*, art. 27.

29. *Id.*

30. Chairman, Joint Chiefs of Staff Instruction 5810.01, Implementation of the DoD Law of War Program (12 August 1996), ¶ 4(a).

31. This reflects the well-understood principle of proportionality. *See e.g.*, F. Kalshoven, "Constraints on the Waging of War" (1987).

32. *See, generally*, Maura McGowan, "Means and Methods of Waging War" (unpublished - on file at HQ USAFA/DFL).

33. J. Pictet, Humanitarian Law and the Protection of War Victims, 28-29 (1975).

34. Military necessity was defined by Francis Lieber's Code, General Order 100, Instructions for the Government of Armies of the United States in the Field, Article 14 (1863); *U.S. v. List et al*., XI Law Reports of Trial of War Criminals 1253-55 (1950) (The Nuremburg trials). *See, generally* McGowan, *supra* note 32.

35. FM 27-10, ¶ 41(c1); AFP 110-31, ¶ 5-3(2)(b). *See also* McGowan, *supra* note 32.

36. *See, generally*, Mark W. Eichin and Jon A. Rochlis, "With Microscope and Tweezers: An Analysis of the Virus of November 1988." M.I.T. 1988, submitted at 1989 IEEE symposium on Information Security and Privacy, Oakland California.

37. U.N. Charter, Article 2, articulates the principles of the charter. These include sovereign equality and an agreement to settle international disputes by peaceful means.

38. Anticipatory self-defense is beyond the purview of this paper, but a good discussion may be found in Dornstein, *supra* note 19.

39. Simpson Garfinkle and Gene Spafford, "Practical Unix & Internet Security," O'Reilly & Associates (1996), 329. This text also gives a good introduction to virus programs, back door programs, worms, and rabbits.

40. *Id.* at 328-32. *See infra* note 42.

41. A permanent member of the Security Council does not have to abstain except under Chapter VI; abstention is not required under Chapter VII, where the arguments over self-defense and ENIO under Article 41 are likely to occur.

42. U.N. Charter, art. 39.

43. *Id.*, art. 2, ¶ 4.

44. *Id.*, art. 51.

45. *Id.*, art. 41.

46. *Id.*, art. 39.

47. *Id.*, art. 41.

48. Winn Schwartau, "Information Warfare" (1st edition), Thunder Mountain Press (1995), 184.

49. Commentary of Colonel Phil Johnson (position) at the National Defense University Intermediate Information Warfare Course, 15 July 1998.

50. Ira Winkler, "Corporate Espionage," Prima Publishing (1997), 16.

51. *Id.*

52. According to the Staff Statement of the U.S. Permanent Subcommittee on Investigations (Minority Staff) Hearings, on Security in Cyberspace, 5 June 1996, 95% of military communications travel over the public communications switch network (see section I.B. of the report for further details).

53. John Fialka, "War by Other Means," W.W.Norton & Company (1997), 7.

Disclaimer

The conclusions and opinions expressed in this document are those of the author cultivated in the freedom of expression, academic environment of Air University. They do not reflect the official position of the U.S. Government, Department of Defense, the United States Air Force or the Air University.

This article has undergone security and policy content review and has been approved for public release IAW AFI 35-101.

[*Air & Space Power Chronicles* Home Page | Feedback? Email the Editor]