



---

---

## Is It Time for a Treaty on Information Warfare?

---

---

Phillip A. Johnson

### Introduction

Several participants in the conference on computer network attack held at the Naval War College in Newport, Rhode Island, in June 1999 addressed the issue of whether serious consideration should be given in the near future to negotiating international agreements to regulate information warfare. The consensus appeared to be that it would be useful to expand current efforts to improve international cooperation in investigating and prosecuting computer crimes and “cyber-terrorism,” but that it would be premature anytime in the near future to attempt any further prohibition or regulation of State action in the broad area of information warfare. I generally share those views. This chapter will discuss a number of possibilities for international agreements on information warfare, indicate the extent of declared support for negotiations intended to produce such agreements, and venture an opinion on their potential utility.

Some observers have said that the few calls already heard for a treaty banning information warfare come primarily from “have-not” nations that fervently desire to keep the “haves” from reaping any advantage from the information warfare capabilities they have developed by their effort and investment. Others say that new agreements are necessary to enhance the international cooperation that

is essential to effective suppression of malicious interference with information systems that are essential to development, prosperity, international peace and security, and human health and safety. Still others say that new information technologies raise novel international legal issues that would be better resolved by negotiating a definitive international agreement than through the slow and uncertain process by which customary international law develops. Others reply that we are not yet smart enough to sit down and create international law on these new issues, and that the gradual accumulation of practice and precedent offers the best process for applying existing international law to these new issues in cyberspace. I boldly take the position that each of these views is correct—in part and on some subjects.

For the purposes of this chapter, I intend to set aside discussion of a number of military missions that are often considered to be elements of information warfare. These are the physical destruction of information systems by traditional military means, electronic warfare (e.g., “jamming” of radio and radar signals), military deception, and operations security. These traditional military missions have been conducted for a long time over a wide spectrum of military operations from peace to war, and the application of international law to them is reasonably well settled. I also intend to set aside discussion of directed energy weapons such as high-energy radio, microwave, and electro-magnetic pulse devices. The technology of these devices is relatively new, but their employment and effects are likely to be so similar to those of traditional weapons that established principles of international law concerning the use of force and the law of armed conflict can be applied to them with great confidence.

Psychological operations have also been a traditional military mission, but new technologies such as the broadcasting of radio and television signals from aircraft and satellites, worldwide access to the Internet, and greatly improved capabilities to create false images and messages give “psyops” unprecedented reach and power. As we shall see, there already have been a few isolated calls for new international controls over these new capabilities for spreading “propaganda.”

The newest element of information warfare, and the one currently drawing the most attention, is computer network attack, or CNA. CNA is conducted by sending electronic messages from one computer to another through some connecting medium or network, such as radio or the Internet, or by direct input by a user of the target computer system. The most common forms of CNA are: (1) overloading an adversary’s web pages or e-mail systems with so much input that they cannot function properly; (2) tricking an authorized user into inputting malicious logic, as by sending an e-mail message with a virus or a worm in an attached file; and (3) obtaining unauthorized access to an adversary’s computer

system. Unauthorized access may be obtained by exploiting a security weakness in the target's operating system, by unauthorized use of a genuine user identification and password, or by other means. Even if an intruder does no apparent harm, the mere fact that an intruder has gained unauthorized access renders the system and its contents suspect, since an intruder could have altered stored data, changed the operating system, or introduced malicious logic such as a virus, worm, or logic bomb. An intruder may even damage the system to the point where it becomes unusable. The remainder of this chapter will focus primarily on the question of whether it would be desirable to negotiate international agreements to prohibit or regulate CNA.

At this point in history, there are a number of "revealed truths" concerning CNA that make it different from prior methods and means of conducting hostilities. I list them here as common points of departure; the reader can find a fuller discussion of them in the other contributions to this volume:

- The more a nation relies on sophisticated information systems, the more vulnerable it is to interference with them;
- Geography has ceased to be relevant to the security of information systems that are connected to the Internet or that are accessible by radio;
- The worldwide use of comparable equipment, operating systems, and software greatly facilitates CNA;
- Information technologies change rapidly;
- Most advances in information technology are developed by individuals or companies for commercial purposes;
- Developing at least some capability to interfere with other nations' information systems is relatively cheap and easy, compared to other modern weapons systems, and the necessary expertise and equipment are widely available;
- CNA "offense" currently seems to be dominant over CNA "defense," but the balance between them might change quickly and dramatically;
- In most cases it is difficult to locate and identify computer intruders, to discover their motive and intent, and to determine whether their acts are attributable to State sponsors; and
- Because many "dual-use" information infrastructures whose support to military operations makes them legitimate military targets are also used for noncombatant purposes, interference with them may endanger the safety of persons and property protected by the law of war from deliberate attack and from disproportionate collateral damage.

## **Calls For International Agreements**

Public calls by governments for new international agreements on information warfare consist primarily of: (1) initiatives by the United States and by certain European and other American nations to promote better international cooperation in investigating and prosecuting computer crimes and terrorism; and (2) a campaign by Russia in United Nations channels for multilateral arms control negotiations to protect international "information security."

International cooperation in investigating and prosecuting computer crimes has sometimes proven to be quite effective even in the absence of new agreements and working arrangements specifically tailored to this new category of offenses. For example, in 1987 West German authorities relied on the authority provided by existing German law to trace the origin of over 200 intrusions into US government computers to four German nationals who turned out to be working for the KGB.<sup>1</sup> In far too many cases, however, effective international cooperation in investigating computer offenses has been frustrated by the unwillingness of the requested State to cooperate, its lack of domestic legal authority to investigate and punish computer offenses, the absence of established procedures and points of contact, and problems arising from extradition treaties.

In an effort to address such problems, in December 1997 the United States Attorney General hosted a meeting of the Group of Eight (G-8) Justice and Interior Ministers to discuss international cooperation in the investigation and prosecution of computer intrusions and other high-tech crimes.<sup>2</sup> Since this meeting, a number of international working groups have devoted considerable effort to modernizing the G-8 nations' domestic criminal laws and to improving international agreements and arrangements providing for mutual legal assistance and extradition in cases involving computer offenses. This work has also generated a project in the Council of Europe, which the United States has assisted, to draft an international convention on "cyber-crime." The United States has also undertaken similar initiatives in the Organization of American States and at the United Nations. Significant progress has been made, but there is still an enormous amount of work to be done in this area. For example, while several European nations have made significant reforms in their domestic computer crime laws and the state of procedures for international assistance in investigating computer offenses has greatly improved between various nations, Russia has essentially stonewalled all requests for cooperation in investigating several thousand intrusions into US military computer systems in early 1999 that apparently originated in Russian territory.<sup>3</sup>

In addition, these efforts have focused on computer offenses committed by individuals that can be characterized as crimes or terrorism. They are not directly

relevant to State action. Somewhat ironically, the only nation that has made a prominent effort to address the use of computer network attack by States against other States has been Russia. In October 1998, Russian Federation Ambassador Vasily Sidorov made a statement before the UN General Assembly's Committee on Disarmament and International Security to the effect that Russia is alarmed by the serious threats to international peace and security raised by developments in information technology, and that it is urgent to take preventive measures by establishing international principles on the use of information technology and possibly an international monitoring and control regime.<sup>4</sup> Russia also tabled a resolution that called for Member States to express their views on the creation of "international legal regimes to prohibit the development, production or use of particularly dangerous forms of information weapons" and the establishment of "an international system (centre) for monitoring threats pertaining to the security of global information and telecommunications systems."<sup>5</sup>

No significant support was expressed by other nations for the Russian proposal. Instead, on December 4, 1998, the General Assembly adopted without a vote a greatly watered-down resolution that called on Member States to "promote at multilateral levels the consideration of existing and potential threats in the field of information security," invited all Member States to inform the Secretary General of their views on the subject, requested the Secretary-General to submit a report to the General Assembly in its 1999 session, and included in the provisional agenda for its next session the topic, "Developments in the field of information and telecommunications in the context of international security."<sup>6</sup>

Undeterred, Russia has continued to pursue its proposal for an "international legal regime" on "information weapons." In its submission of views to the Secretary General as invited by the General Assembly resolution, Russia declared that "information weapons" can have "devastating consequences comparable to the effect of weapons of mass destruction," called for the General Assembly to pass "resolutions on the question of information security with a view to reducing the threat of the use of information for terrorist, criminal or military purposes," and proposed the development of a code of conduct for States concerning international information security that would ultimately be incorporated into a multilateral international legal instrument.<sup>7</sup>

The United States also submitted its views, which generally were that the international community should give priority to developing measures to deal with criminal or terrorist misuse of information technology, and that "it would be premature to try to formulate overarching principles pertaining to information security in all its aspects."<sup>8</sup>

Only eight other nations—Australia, Belarus, Brunei, Cuba, Oman, Qatar, Saudi Arabia, and the United Kingdom—submitted written views to the Secretary General. Of these, only Belarus and Cuba expressed support for negotiations to restrict information warfare. The Secretary General offered no opinion.

In August 1999, the United Nations Department of Disarmament Affairs and the United Nations Institute for Disarmament Research (UNIDIR) hosted a conference in Geneva, Switzerland on the topic: “Developments in the Field of Information and Telecommunications and Their Impact on International Security.” Russia used the forum to promote its proposals for international legal restrictions on information warfare, but it was unable to garner significant support for doing more than continuing to study the problem.<sup>9</sup>

Nevertheless, the current paucity of enthusiasm for negotiating an international agreement restricting information warfare may not last forever. In the past twenty years, the international community has negotiated multilateral treaties restricting such weapons as chemical weapons, blinding lasers, incendiaries, weapons designed to wound with undetectable fragments, and antipersonnel landmines.<sup>10</sup> It might take only a few spectacular incidents involving CNA to provoke serious interest in placing international legal restrictions upon “information weapons.”

### **Subjects For Possible Agreements**

#### **Treaties to suppress private misconduct.**

1. *Suppression of “cyber-crime.”* As indicated above, efforts are already under way in the G-8, the Council of Europe, the Organization of American States, and the United Nations to improve domestic criminal legislation, international cooperation in investigations and prosecutions, and extradition treaties in order to more effectively investigate and punish cross-border computer crimes. The US and British submissions of views mentioned above recommended that the United Nations give this area top priority in its activities concerning information security.

ASSESSMENT: This topic is a logical candidate for priority consideration, since both the nature of the problem of cross-border computer crime and the required remedial steps are reasonably well understood, and since national security issues are not directly implicated. (It should be noted, however, that effective international cooperation in tracing computer network attacks to their origin would also greatly expedite attribution of State-sponsored CNA.) That is not to say that the negotiation of the necessary international agreements will be easy,

given the major differences that exist among domestic legal systems and the encroachment on traditional sovereignty principles that will be inescapable in creating legally binding obligations to assist with criminal investigations and prosecutions, not to mention the proposals that are under consideration for reciprocal authorization of cross-border electronic tracing and monitoring.

2. *Suppression of "cyber-terrorism."* A "cyber-terrorism" agreement might well adopt the common features of the existing multilateral treaties intended to combat such terrorist acts as the hijacking and sabotage of aircraft, hostage taking, attacks on diplomats, terrorist bombing, and the seizure of ships on the high seas.<sup>11</sup> These common features are a recognition of universal or quasi-universal jurisdiction over individuals committing specified acts, an obligation upon each Party to put into place severe domestic criminal penalties for such acts, and an obligation to prosecute or extradite any person suspected of such acts who is found in the territory of a Party.

ASSESSMENT: It may prove to be difficult to generate much interest in negotiating such an agreement until the international community experiences incidents in which "cyber-terrorism" causes death and destruction on the scale experienced as the result of more traditional forms of terrorism. To date, the most common form of cross-border CNA motivated by political reasons has consisted of individuals defacing the target nation's websites, which is likely to strike most people more as vandalism than as terrorism. Even the theft of large amounts of money or the crippling of expensive information systems is unlikely to provoke the same kind of fear and loathing created by more traditional terrorist acts that directly threaten innocent human lives. It would probably take an incident in which planes crash, trains collide, floods cause death and devastation, or a nuclear accident spreads radiation over the countryside before CNA would be taken seriously as "cyber-terrorism." Another major problem would be reaching agreement on definitions of the acts to be suppressed. It is certainly worth exploring the possibilities here, but rapid progress—or even moving the international community at large to devote serious effort to negotiation of a "cyber-terrorism" treaty—seems unlikely in the near future. It may turn out that the most effective legal mechanism for suppression of "cyber-terrorists" will be "cyber-crime" agreements, as discussed above, that would put into effect domestic computer crime laws and facilitate cross-border investigations and prosecutions.

### Treaties to restrict state action.

1. *Declarations of general legal principles.* Perhaps the simplest approach to advancing the development of international law on information security would be

to negotiate a multilateral treaty that declares broad relevant principles of international law. An example of such a document is the 1967 Outer Space Treaty,<sup>12</sup> which declares, *inter alia*, that space is not subject to national appropriation or territorial claims, that nations are obligated not to interfere with the space activities of other nations, that space objects remain under the jurisdiction and control of their nation of registry, that nations bear international responsibility for their space activities, and that established principles of international law, including the UN Charter, apply to space activities. Some candidate principles for a similar declaration of principles on information activities might be that nations must not damage/disrupt/interfere with the information systems of other nations; that such acts violate the sovereignty of the victim nation and threaten international peace and security; and perhaps even that interference with information systems causing death, injury, widespread property damage, or serious damage to communications, public utilities, economic institutions, emergency services, or national security systems will be considered to be equivalent to an armed attack, thereby authorizing the victim nation to employ the remedies provided under international law to the victims of traditional armed attacks, including the use of force in individual or collective self-defense.

**ASSESSMENT:** It will take some time for most nations to determine what international legal principles concerning information warfare are likely to best serve their long-term national interests. Even nations that already possess sophisticated information systems have little confidence at this point that they can reliably forecast near-term technical developments that may drastically affect the balance of information warfare capabilities and vulnerabilities. Those nations that have even a minimum of capabilities to engage in information operations must make a judgment as to whether their interests would be best served by keeping open their options to interfere with other nation's information systems, especially when they are engaged in an international armed conflict, or whether their national interests would be best served by creating an international legal regime that broadly prohibits such interference.

The current domestic and international debate over "space control" may present a useful analogy. As indicated above, the Outer Space Treaty declares the general principle that nations will not interfere with the space activities of other nations. However, its provisions recognizing that nations must conduct their space activities in compliance with international law, including the UN Charter, bring to bear the international law principles that force can be used in self-defense and to execute mandates of the Security Council. Accordingly, these widely-recognized legal authorizations for the use of force apply to space activities in the same manner as they do in the air, at sea, and on land.

Furthermore, since the Outer Space Treaty is silent as to its application during an international armed conflict, we are left to rely on the general principles of international law to determine the extent to which its obligations may apply in wartime.<sup>13</sup> In these circumstances, there has been considerable activity in the UN General Assembly and in the Conference on Disarmament devoted to drafting a multilateral agreement to prevent an “arms race in space.” To date, however, this activity has produced virtually nothing in the way of concrete results.<sup>14</sup>

The continuing impasse over attempts to develop international legal measures to prevent an “arms race in space” might be seen as a confrontation of the “haves” versus the “have-nots,” which might also be seen as the dynamic at work in the impasse over proposals for complete nuclear disarmament. On the other hand, the impasse might also be seen as reflecting the reluctance of at least some of the thirty or so space-capable nations to participate in formulating international legal principles concerning space control when they have yet to reach their own judgments concerning where their own long-term national interests lie.

The analogy between space control and information warfare is less than exact, for several reasons. One is the fact that it is many orders of magnitude easier for a nation to develop a significant information warfare capability than it is to develop space control capabilities. This is clearly demonstrated by the computer network attacks that have already been reported in connection with such conflicts as Kosovo and Chechnya, and in the continuing tensions between Taiwan and mainland China.<sup>15</sup> The converse is also true—virtually every nation employs at least some automated information systems, making them vulnerable to CNA, while only about thirty nations conduct space activities. In these circumstances, it seems unlikely that very many nations will regard themselves as “non-players” in information warfare. It seems equally unlikely that many of them will come to firm conclusions anytime soon about how their own long-term national interests might be affected by restricting CNA or other information warfare activities. Accordingly, even a declaration of general legal principles concerning information warfare is likely to be beyond the grasp of the international community for the foreseeable future.

2. *Arms Control Agreements.* Another approach would be to negotiate agreements under which the parties would commit themselves not to develop, possess, or transfer certain information warfare capabilities, or to use them in a manner that is destabilizing to other arms control regimes or to crisis management systems.

ASSESSMENT: This approach is subject to the same caveat stated above, which is that not many nations—if any—have figured out where their long-term national interest lies in relation to information warfare. It also suffers from the great difficulty of defining exactly what capabilities the parties would

agree not to develop, possess, or transfer; from the apparent impossibility of verification; from the fact that governments have no monopoly over the development or use of CNA capabilities; and from the fact that CNA capabilities and vulnerabilities change rapidly. The development of "hacking" tools is a worldwide cottage industry, unlike nuclear weapons, tanks, artillery, submarines, ballistic missiles, or warplanes. Powerful hacker tools are posted on the Internet for use by all comers.<sup>16</sup> Furthermore, many highly capable computer network attack capabilities spring directly from techniques and programs developed for legitimate purposes.<sup>17</sup> For these reasons, it is difficult to envisage how an arms control-style agreement could be negotiated anytime in the near future. In addition, any proposal for a nonproliferation agreement might well raise suspicions among the developing nations that the "have" nations are engaged in a conspiracy to deny the developing nations the benefits of highly capable information systems.

Strategic arms control agreements often contain provisions to preserve or expand transparency, such as obligations not to interfere with other parties' national technical means of verification. It may not be necessary to negotiate separate agreements in order to extend the reach of such agreements to ban electronic means of interference with national technical means of verification. At most, an agreed interpretation by the parties should suffice. Another similar extension of arms control principles that might prove to be both useful and attainable would be an agreement that the parties will not employ information warfare techniques in a manner that would interfere with each others' command and control of strategic weapons or disrupt missile attack warning systems.

Another theme of arms control agreements has been to create new confidence-building procedures, as in the Open Skies Agreement.<sup>18</sup> However, it is difficult to imagine how a confidence-building agreement could be devised for computer network attack capabilities, since such an agreement would entail widespread access by each party to the national computer systems of other parties that would be exceptionally intrusive without holding out much promise of effectiveness.

In 1989, the United States and the Soviet Union agreed not to conduct dangerous military activities in peacetime in proximity to the military forces of the other party.<sup>19</sup> One of the activities in which the parties agreed not to engage is interference with command and control networks in a manner which could cause harm to personnel or damage to equipment of the other party. Since electronic interference was already the primary mechanism causing interference with command and control networks, it would appear that this agreement can be applied to CNA without change. Whether circumstances will make it appropriate to enter into similar agreements with other nations remains to be seen.

3. *Law of War Agreements.* Existing law of war treaties ban the use in international armed conflicts of weapons such as expanding bullets, barbed weapons, and projectiles filled with glass on the basis that, used as intended, they are likely to cause unnecessary suffering.<sup>20</sup> The methods and means of information warfare do not generally raise such considerations, since few information warfare techniques cause any direct personal injury or impairment to health. An odd and isolated exception is a report by Russian authorities that they have discovered a computer virus called “666” that displays certain light patterns on a computer screen that cause the operator to lapse into a coma. Fifty computer operators are reported to have died as a result of exposure to the “666” virus.<sup>21</sup> With this bizarre exception, information warfare “weapons” are not generally understood to cause unnecessary suffering in the same way as do weapons that have been banned for this reason.

The law of war also bans the use in international armed conflict of weapons that are indiscriminate, i.e., they cannot be controlled and directed only against authorized military targets. Poison gas and non-self-destructing/non-self-disabling antipersonnel landmines are examples of weapons that have been banned for this reason.<sup>22</sup> We have already seen self-propagating computer “viruses” and “worms” that clearly foreshadow the issue of malicious logic that runs amok through military and civilian computer systems. Again, however, malicious computer logic is unlikely to directly cause injury and death. Furthermore, any attempt at drafting an international agreement that would ban indiscriminate information warfare “weapons” is likely to founder on the difficulty of defining them. It seems unlikely that any resulting agreement would advance international law beyond the principle that “information weapons,” like all weapons, must be discriminate.

Law of war agreements have also taken the tack of banning or restricting attacks on certain targets, such as medical facilities, prisoner of war camps, and cultural property.<sup>23</sup> These existing agreements already protect these facilities from attack by any means, including information warfare techniques. It might be argued that infrastructures that are heavily relied upon for the health and safety of the civilian populations and that are particularly vulnerable to CNA should be specifically protected from such attack by international agreement. Examples might be public utilities, transportation, communications, financial networks, emergency services, and universities. The problem is that such systems may in certain circumstances be legitimate targets of attack. This may be the case when the system is being used to provide direct support to military operations, as when a single electric power net is used both for military and civilian purposes. It may also be the case, in a long and protracted conflict,

that a belligerent's transportation, utilities, financial system, and research and development systems become valid military targets because disrupting them would significantly undermine its military strength. Accordingly, it seems unlikely that the nations would agree to bestow blanket immunity on such systems, or that an international agreement could be negotiated that would advance law of war principles on the targeting of dual-use infrastructures beyond their current state. Furthermore, it would be highly counterproductive to ban CNA against such infrastructures while leaving them open to attack by traditional military weapons, which would in most cases create a much greater danger of collateral damage.

Finally, one theme of the Russian initiative for a ban on "especially dangerous information weapons" has been a push for limitations on psychological warfare. The Russian statement submitted to the Secretary General in June 1999 referred to the threat of "(u)se of information with a view to undermining a State's political and social system; psychological manipulation of a population for the purpose of destabilizing society."<sup>24</sup> The Cuban submission also addressed this issue: "The misuse of information and telecommunications systems and information resources, especially when such systems and resources are used by some States to carry out their policies of interference in the affairs of other States, is an infringement of the sovereignty and independence of the affected States and creates centres of tension that may pose a serious threat to international security."<sup>25</sup> From past experience, it seems highly unlikely that the international community will be eager to create broad restrictions on propaganda, even as it has been empowered by new and more powerful information technologies. Russia, Cuba, and other States stung in the past by the Voice of America, Radio Marti, and other "voices of freedom" will no doubt continue to beat this drum. It seems particularly unlikely that any of the Western democracies will support such calls to impose international legal restraints on the criticism of other societies or governments. As the authors of a recent article in *Foreign Affairs* concluded, "Their societies are familiar with the free exchange of information, and their institutions of governance are not threatened by it."<sup>26</sup>

### **Forms Of Possible Agreements**

**A. Multilateral Conventions.** Multilateral conventions, especially those to which substantially all nations become parties, carry the greatest weight of authority in establishing new international law. It seems extremely unlikely, however, that a multilateral convention restricting State action relating to information warfare will be adopted anytime soon. As stated above, few nations

have expressed any interest in negotiating such an agreement, chiefly because few nations understand information warfare capabilities and vulnerabilities well enough to determine what principles of international law would best serve their long-term national interests.

In addition, the fundamental unhappiness felt by many nations as the result of recent experiences in diplomatic conferences is likely to generate significant procedural controversies that would have to be settled before negotiating new multilateral conventions. There are essentially two procedural approaches to the negotiation of a multilateral convention, whether through UN channels or in a special diplomatic conference. The first is a consensus procedure, which is used in such fora as the Conference on Disarmament. This procedure requires achieving general acceptance of a negotiating text, usually by a process of tough bargaining and compromise.

A recent alternative approach to negotiating multilateral conventions has been the use of majority-rule procedures, which were in essence the procedures used in the negotiations in Oslo that produced the Ottawa Convention banning antipersonnel landmines and in the Rome Conference that produced the draft Statute of the International Criminal Court. The great practical advantage and also the worst defect of such procedures is that they allow the majority of participating nations to approve a treaty text to which minority nations have fundamental objections. Such a result affords the organizers of the negotiations and the members of the majority immediate gratification, but it produces a treaty that will probably not be accepted by the dissenting States. In the case of the Ottawa Convention, this process generated a treaty which is almost meaningless because it apparently will not be ratified by a number of countries whose military forces and operations are most important to world affairs, including the United States, Russia, and China. The same is true to a somewhat lesser extent for the draft Statute of the International Criminal Court. Ironically, there were opportunities in the negotiations that produced both of these conventions to arrive at compromises that would have made them more widely acceptable. In both cases, however, the "like-minded" groups were not required to agree to these compromises to produce an agreement, and in both they chose ideological purity over wider acceptance. With these recent debacles in mind, it seems unlikely that there will be much enthusiasm in the near future for convening any major new international law-making diplomatic conferences on any subject.

**B. Bilateral Agreements.** Bilateral agreements, or agreements among a small number of nations, are most useful when only a few governments are directly

involved in the issues to be addressed. This may be because the issues are limited to one geographic area, or because only a few nations are capable of engaging in the activities in question. Good examples of the latter group are strategic nuclear arms control agreements and agreements to limit anti-ballistic and theater missile defense systems. Agreements to promote better suppression of cybercrime and cyberterrorism could be negotiated either multilaterally or bilaterally. The results of the current efforts described above in the G-8, the Council of Europe, and the Organization of American States are likely to be a combination of both, with regional agreements arrived at on some issues, and bilateral approaches taken to others. Negotiation of a global multilateral convention on these issues is unlikely until the problems of cybercrime and cyberterrorism are more broadly experienced and more broadly understood.

**C. General Assembly Resolutions.** The United Nations General Assembly has displayed great enthusiasm for passing resolutions on a broad range of subjects calling on Member States to adhere to certain principles. When such resolutions enjoy broad support they may persuasively influence the policies of member governments and international institutions, but such resolutions do not generally have the force of international law. On the other hand, there are occasional General Assembly resolutions that are expressly intended to declare certain principles of customary international law. When such resolutions are supported by all or substantially all Members, they may be given great weight as evidence of customary international law. An example of such a resolution recognized as “law-declarative” by the United States is the 1970 Declaration on Principles of International Law Concerning Friendly Relations and Cooperation among States in Accordance with the Charter of the United Nations.<sup>27</sup> Judging from the lack of interest generated by the Russian initiatives on “information security” in the General Assembly, it seems unlikely that there will be enough support to pass any kind of resolution calling on Member States to observe any set of principles concerning information warfare. Given the novelty of the international legal issues involved, it seems even more unlikely that the General Assembly will pass a “law-declarative” resolution on information warfare in the next several decades.

**D. “Codification” of Existing Customary International Law.** Several participants in the Newport conference recalled the work of the round-tables of governmental and academic experts that met periodically from 1988 to 1994, hosted by the International Institute of Humanitarian Law, which ultimately produced the *San Remo Manual on International Law Applicable to Armed Conflicts at*

*Sea.* The San Remo Manual is widely recognized as an authoritative restatement of the consensus understanding among the world's leading governmental and academic experts in this branch of international law, and it will no doubt be accorded great weight as evidence of the interpretation of applicable treaties and the state of customary international law. However, there would appear to be little potential in the foreseeable future for successfully employing an "experts conference" to authoritatively record the customary international law governing information warfare. At present there is no such law, which can only accumulate from State practice in reaction to events as they unfold over time. Accordingly, there are no "experts" either, since there is no accumulation of State practice that learned commentators could analyze and restate.

### Conclusions

The next few years are likely to produce a number of regional and bilateral agreements designed to improve international cooperation in battling cybercrime and cyberterrorism. If dramatic events occur involving cyberterrorism, or if the international community feels the necessity to do *something* in the area of computer network attacks, a multilateral convention on suppression of cyberterrorism may result. The parties to strategic arms control treaties may find it useful to state their common understanding concerning how their provisions apply to CNA directed against national technical means of verification, command and control systems, and attack warning systems.

However, there seems to be little or no prospect of negotiating international agreements that would broadly prohibit or regulate state action involving information warfare techniques because: (1) the issues involved are not yet well understood; (2) traditional arms control and law of war mechanisms are not well suited for application to CNA; and (3) the nations—including the United States—do not yet have a clear understanding of what kind of international legal regime relating to information warfare would best serve their long-term national interests. For the foreseeable future, the development of international law concerning information warfare is most likely to consist of the incremental accumulation of customary international law resulting from the actions and statements of nations in response to events as they unfold. Considering the circumstances, that is probably the best available process. During this formative period, statesmen and their advisers will have a heavy responsibility to bear in mind that their acts and statements will play a major role in the development of international law concerning information warfare.

## Notes

1. CLIFF STOLL, *THE COOKOO'S EGG* (1989).
2. U.S. Dep't Justice Press Release, Statement by Attorney General Janet Reno on the Meeting of Justice and Interior Ministers of the Group of Eight, Dec. 10, 1997. The members of the G-8 are Canada, France, Germany, Italy, Japan, Russia, the United Kingdom, and the United States.
3. Jim Wolf, *Moscow Said to Withhold Full Help on Cyber-Blitz*, REUTERS, Nov. 5, 1999.
4. Daniel Verton, *DoD Faces Infowar Controls*, FEDERAL COMPUTER WEEK, Jan. 11, 1999.
5. Russian Federation, draft resolution, Developments in the field of information and telecommunications in the context of international security, U.N. Doc. A/C.1/53/L.17 (1999).
6. G.A. Res. 53/70, U.N. GAOR, 53rd Sess., U.N. Doc. A/53/70 (1999).
7. Report of the Secretary General on developments in the field of information and telecommunications in the context of international security, U.N. Doc. A/54/213 (1999), at 8.
8. *Id.* at 11.
9. Discussion Summary, Developments in the Field of Information and Telecommunications in the Context of International Security (Private Discussion Meeting Hosted by the Department of Disarmament Affairs and the UN Institute for Disarmament Research, Geneva, Aug. 25-26, 1999).
10. Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons which may be Deemed to be Excessively Injurious or to have Indiscriminate Effects, Oct. 10, 1980, S. TREATY DOC. NO. 103-25 (1993) [hereinafter Conventional Weapons Convention]; Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction, Jan. 13, 1993, S. TREATY DOC. NO. 103-21 (1993) [hereinafter Chemical Weapons Convention]; Convention on the Prohibition of the Use, Stockpiling, Production, and Transfer of Anti-Personnel Mines and on their Destruction, Sept. 18, 1997, 36 I.L.M. 1507 (1997) [This agreement has not been signed by the United States].
11. Convention on Offenses and Certain Other Acts Committed on Board Aircraft, Sept. 14, 1963, 20 U.S.T. 2941, 704 U.N.T.S. 219; Convention for the Suppression of Unlawful Seizure of Aircraft, Dec. 16, 1970, 22 U.S.T. 1641, 860 U.N.T.S. 105; Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation, Sept. 23, 1971, 24 U.S.T. 564; Convention to Prevent and Punish the Acts of Terrorism Taking the Form of Crimes against Persons and Related Extortion that are of International Significance, Oct. 16, 1973, 27 U.S.T. 3949; Convention on the Prevention and Punishment of Crimes Against Internationally Protected Persons, Including Diplomatic Agents, Dec. 14, 1973, 28 U.S.T. 1974, 1035 U.N.T.S. 167; Convention on the Physical Protection of Nuclear Materials, Oct. 26, 1979, T.I.A.S. 11080; International Convention Against the Taking of Hostages, Dec. 17, 1979, T.I.A.S. 11081; Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, Feb. 24, 1988, S. TREATY DOC. NO. 100-19 (1988); Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation, Mar. 10, 1988, 27 I.L.M. 668 (1988); Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf, Mar. 10, 1988, 27 I.L.M. 685 (1988); International Convention for the Suppression of Terrorist Bombing, Nov. 25, 1997, 37 I.L.M. 249 (1998).
12. Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and other Celestial Bodies, Jan. 27, 1967, 18 U.S.T. 2410, 610 U.N.T.S. 205.

13. See Office Of General Counsel, Department of Defense, *An Assessment Of International Legal Issues In Information Operations*, sect. I.B (Nov. 1999) [hereinafter DoD/GC Paper]. This paper is appended to this volume as the appendix.

14. *Id.*

15. See, e.g., *Nerd World War*, *ECONOMIST*, Oct. 30, 1999 (LEXIS); Robyn Dixon, *Chechyns Use Net in Publicity War with Russia*, *LOS ANGELES TIMES*, Oct. 8, 1999, at A-4; David A. Fulghum, *Telecom Links Provide Cyber-Attack Route*, *AVIATION WEEK & SPACE TECHNOLOGY*, Nov. 8, 1999, at 81; Bob Brewin, *Kosovo Ushered in Cyberwar*, *FEDERAL COMPUTER WEEK*, Sept. 27, 1999.

16. Michael E. Ruane, *New Computer Technology Makes Hacking a Snap*, *WASHINGTON POST*, Mar. 10, 1999, at 1.

17. Donn Parker, *Automated Security*, *INFORMATION SECURITY*, Oct. 1999, at 32.

18. Treaty on Open Skies, Mar. 24, 1992, S. TREATY DOC NO. 102-37 (1992). The United States has ratified this agreement but it has not come into force.

19. Agreement on the Prevention of Dangerous Military Activities, June 12, 1989, 28 I.L.M. 877 (1989).

20. Hague Convention IV, Respecting the Laws and Customs of War on Land, Oct. 18, 1907, 36 Stat. 2277; Conventional Weapons Convention, *supra* note 10.

21. Timothy L. Thomas, *Dialectical Versus Empirical Thinking: Ten Key Elements of the Russian Understanding of Information Operations*, *JOURNAL OF SLAVIC MILITARY STUDIES*, Mar. 1998, at 51.

22. Geneva Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous, or Other Gases, and of Bacteriological Methods of Warfare, June 17, 1925, 26 U.S.T. 571, 94 U.N.T.S. 65; Chemical Weapons Convention, *supra* note 10, Conventional Weapons Convention, *supra* note 10.

23. Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Aug. 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31; Convention for the Protection of Cultural Property in the Event of Armed Conflict, May 14, 1954, 249 U.N.T.S. 240. The United States has signed but has not ratified this agreement.

24. Secretary General's Report, *supra* note 7, at 9.

25. *Id.* at 5.

26. Robert O. Keohane and Joseph S. Nye, Jr., *Power and Interdependence in the Information Age*, *FOREIGN AFFAIRS*, Sept.–Oct. 1998, at 93.

27. G.A. Res. 2625, U.N. GAOR, 25<sup>th</sup> Sess., U.N. Doc. A/8082 (1970). See DoD/GC Paper, sect. III. A, *supra* note 13.