THE LAWFULNESS OF ATTACKING COMPUTER NETWORKS IN ARMED CONFLICT AND IN SELF-DEFENSE IN PERIODS SHORT OF ARMED CONFLICT: WHAT ARE THE TARGETING CONSTRAINTS?

JAMES P. TERRY[1]

I. Introduction

When President Clinton signed the Fiscal Year 2000 version of the Unified Command Plan (UCP) on 29 September 1999, it marked a new era in operational planning for information warfare, to include the possible targeting of an adversary's computer networks where necessary to protect vital U.S. or allied interests.[2] The UCP provides planning guidance and requirements for the operational commands within the Department of Defense (DOD).[3] In the latest version, responsibility for maintaining and managing the Joint Information Operations Center (JIOC), located in San Antonio, Texas, was transferred to the U.S. Space Command (USSPACECOM) at Petersen Air Force Base, Colorado.[4]

The JIOC, formerly known as the Joint Command and Control Warfare Center, provides "full-spectrum" information warfare (IW) and information operations (IO) support to U.S. operational commanders worldwide. That is, the JIOC provides support in planning, coordination, and execution of all DOD IW and IO missions, as well as assistance in the development of IO doctrine, tactics and procedures.

What makes the transfer of the JIOC significant is the recent enhancement of its missions. In August 1999, the mission of the JIOC was broad-

---

1. Colonel, United States Marine Corps (Retired). S.J.D., George Washington University, 1982; LL.M., George Washington University, 1980; J.D., Mercer University, 1973; B.A., University of Virginia, 1968. Colonel Terry served as Legal Counsel to the Chairman, Joint Chiefs of Staff, from 1 July 1992 until 30 June 1995, when he retired from the U.S. Marine Corps. Upon retirement, he was appointed to the Senior Executive Service. He currently serves as Deputy Assistant Secretary of State for Regional, Global, and Functional Affairs. He is widely published in the areas of coercion control and national security law. The views expressed are the personal views of the author.

2. U.S. DEP'T OF DEFENSE, UNIFIED COMMAND PLAN (1999).

3. *Id.*

4. Press Release, U.S. Space Command News Release No. 20-99, at 1 (Oct. 1, 1999) [hereinafter News Release No. 20-99].

ened from command and control to include operations support. The enhanced operations support now required includes psychological operations, security, electronic warfare, targeting of command and control facilities, military deception, computer network defense, civil and public affairs, and, significantly, computer network attack.[5]

For the first time in the UCP, computer network attack was specifically identified in the planning requirements for unified commanders.[6] This is significant because, by implication, the planning requirements now recognize the legality of targeting critical foreign computer infrastructure when vital U.S. or allied national interests are threatened.

II. Defining the Debate

The renewed emphasis on considering critical computer infrastructure as a legitimate target arises from recent incidents where critical U.S. infrastructure has been threatened by government-sponsored intrusions or by individual hackers using sophisticated software. From these incidents, the United States has recognized that electronic or physical elimination of this threat may be necessary to protect our defense capability or to ensure the continued effective operation of other critical computer infrastructure.

Several incidents are significant. In February 1998, two California teenagers were able to breach computer systems at eleven Air Force and Navy bases, causing a series of "denials of service" and forcing defense officials to reassess the security of their networks.[7] The investigation of this incident, code named Solar Sunrise, however, pales in comparison with "Moonlight Maze," the code name for the investigation of an early 1999 electronic assault involving hackers based in Russia. In this attack, intruders accessed sensitive DOD science and technology information.[8]

---

5. *Id.*

6. UNIFIED COMMAND PLAN, *supra* note 2, para. 22(a)(12) (unclassified portion). Under the Fiscal Year 2000 UCP, USSPACECOM's responsibilities now include:

> In coordination with the Joint Staff and appropriate CINCs, serving as the military lead for computer network defense (CND) and, effective 1 October 2000, computer network attack (CNA), to include advocating the CND and CNA requirements of all CINCs, conducting CND and CNA operations, planning and developing national requirements for CND and CNA, and supporting other CINCs for CND and CNA.

7. INSIDE DEFENSE, DEFENSE INFORMATION AND ELECTRONICS REPORT 1 (22 Oct. 1999).

Computer tracing determined that the Moonlight Maze attack originated from the Russian Academy of Science, a government organization that interacts closely with the Russian military.[9] This raises the possibility of an asymmetrical attack sponsored by a nation-state.

Nor has this been the first state-sponsored intrusion into our critical computer infrastructure. In 1996, U.S. authorities detected the introduction of a program, called a "sniffer," into computers at NASA's Goddard Space Flight Center, permitting the perpetrator to download a large volume of complex telemetry information transmitted from satellites. The Deputy Attorney General reported that the "sniffer" had remained in place for a significant period of time.[10] Of equal concern, a Federal Bureau of Investigation (FBI) report completed in 1999 detailed efforts of the People's Republic of China to attack U.S. Government information systems, including the White House network.[11]

These incidents raise important issues for defense planning. How can these threats be discovered and eliminated? What is the interplay between the role of an investigating agency and that of an operational planner? It is clear that while the targeting of these threats may require a military component, the gathering of indicators of an imminent threat requires a far broader participation. It is for this reason that the Clinton Administration established the National Infrastructure Protection Center (NIPC) in February 1998.[12]

The NIPC's mission is to serve as the government's focal point for threat assessment, warning, investigation, and response to threats or attacks against our critical infrastructures. These critical infrastructures include our defense communication networks, telecommunications sys-

---

8. *Id.*

9. *Id.*

10. Honorable Jamie Gorelick, Speech Before the Corps of Cadets, U.S. Air Force Academy (29 Feb. 1996).

11. *See* William Gertz, *Chinese Hackers Raid U.S. Computers*, WASH. TIMES, May 16, 1999, at C1, C8 (providing a review of Chinese efforts to attack White House, State Department and other government computer systems).

12. Presidential Decision Directive 63, Critical Infrastructure Protection (May 1998) [hereinafter PDD 63]. The NIPC, located in the FBI's Hoover Building in Washington, D.C, brings together representatives from the FBI, DOD, other government agencies, state and local governments, and the private sector.

tems, energy grids, banking and finance organizations, water systems, government operations apparatus and emergency services organizations.[13]

The NIPC is organized with both an indication and warning arm and an operational arm. The Analysis and Warning Section (AWS) provides analytical support during computer intrusion investigations and long-term analysis of vulnerability and threat trends. The Computer Investigations and Operations Section (CIOS) is the operational arm of the NIPC. This section manages computer intrusion investigations conducted by FBI field offices throughout the country; provides subject matter experts, equipment, and technical support to investigators in federal, state, and local government agencies involved in critical infrastructure protection; and provides an emergency response capability to help resolve a cyber incident.[14]

Neither the JIOC at USSPACECOM nor the NIPC possess the capability to eliminate a hostile cyber threat. Only the operational assets assigned to the various unified commands within the Department of Defense (DOD) possess that unique capability, and they may only be employed when the strict parameters of the law of armed conflict are satisfied.

III. Legal Constraints on Attacks on Critical Infrastructure

A. United Nations Charter System

The legal regime available to authorize actions in lawful self-defense, and specifically for attacks on critical enemy infrastructure, includes the U.N. Charter system and customary international law. The basic provision restricting the threat or use of force in international relations is Article 2, paragraph 4, of the United Nations Charter. That provision states: "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any

13. *Id.* Presidential Decision Directive 63 establishes these categories as "critical infrastructure," the protection of which constitutes the defense of vital national interests. *Id.*

14. The NIPC works closely with USSPACECOM's JIOC and with the Critical Infrastructure Coordination Group, which is directed by the National Coordinator for Infrastructure Protection. *See* News Release No. 20-99, *supra* note 4.

state, or in any manner inconsistent with the Purposes of the United Nations."[15]

The underlying purpose of Article 2, paragraph 4, to regulate aggressive behavior between states, is identical to that of its precursor in the Covenant of the League of Nations. Article 12 of the Covenant stated that League members were obliged not to "resort to war."[16] This terminology, however, left unmentioned actions that, although clearly hostile, could not be considered to constitute acts of war. The drafters of the U.N. Charter wished to ensure the legal niceties of a conflict's status did not preclude cognizance by the international body. Thus, in drafting Article 2, paragraph 4, the term "war" was replaced by the phrase "threat or use of force." The wording was interpreted as prohibiting a broad range of hostile activities including not only "war" and other equally destructive conflicts, but also applications of force of a lesser intensity or magnitude.[17] This distinction may be all-important, for example, when a nation's commercial infrastructure is attacked, and actions in lawful self-defense are contemplated which include targeting critical infrastructure of the adversary, an element of which may have been used in the initial attack.

---

15. U.N. CHARTER art. 2, para. 4.

16. *See* LEAGUE OF NATIONS COVENANT art. 12. Article 12 states:

> 1. The members of the League agree that if there should arise between them any dispute likely to lead to a rupture, they will submit the matter either to arbitration or judicial settlement or to inquiry by the Council, and they agree in no case to *resort to war* until three months after the award by the arbitrators or the judicial decision or the report of the Council.
>
> 2. In any case under this Article the award of the arbitrators or judicial decision shall be made within a reasonable time, and the report of the Council shall be made within six months after the submission of the dispute.

Id.

17. MYRES MCDOUGAL & F. FELICIANO, LAW AND MINIMUM WORLD PUBLIC ORDER 142-43 (Yale ed., 1961).

B. U.N. General Assembly Resolution 2625

The United Nations General Assembly has clarified the scope of Article 2 in two important resolutions, both adopted unanimously.[18] Resolution 2625, the Declaration on Friendly Relations, describes behavior that constitutes the "unlawful threat or use of force" and enumerates standards of conduct by which states must abide.[19] Contravention of any of these standards of conduct is declared to be in violation of Article 2, paragraph 4, and would likely authorize a response in self-defense.[20]

C. U.N. General Assembly Resolution 3314

Resolution 3314, The Definition of Aggression, provides a detailed statement on the meaning of "aggression" and defines it as "the use of armed force by a State against the sovereignty, territorial integrity or political integrity or political independence of another State, or in any manner inconsistent with the Charter of the United Nations."[21] This resolution

---

18. *See* Definition of Aggression, G.A. Res. 3314, U.N. GAOR, 29th Sess., Supp. No. 31, at 142, U.N. Doc A/9631 (1974) [hereinafter U.N. Definition of Aggression]; Declaration on Principles of International Law Concerning Friendly Relations and Cooperation Among States in Accordance with the Charter of the United Nations, G.A. Res. 2625, U.N. GAOR, 25th Sess., Supp. No. 28, at 121, U.N. Doc. A/8028 (1970) [hereinafter U.N. Declaration on Friendly Relations].

19. The Declaration on Friendly Relations includes the following provisions:

> Every State has the duty to refrain from organizing, instigating, assisting or participating in acts of civil strife or terrorist acts in another State.
>
> No State or group of States has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State.
>
> No State shall organize, assist, foment, finance, incite, or tolerate subversive,
> terrorist, or armed activities directed towards . . . the regime of another State.

U.N. Declaration on Friendly Relations, *supra* note 18, at 122-23.

20. U.N. CHARTER art. 2, para. 4 "By accepting the respective texts [of the Declaration on Friendly Relations], States have acknowledged that the principles represent their interpretations of the obligations of the Charter." James Resinstock, *The Declaration of Principles of International Law Concerning Friendly Nations: A Survey*, 65 AM. J. INT'L L. 713, 715 (1971).

21. U.N. Definition of Aggression, *supra* note 18, at 142.

contains a list of acts that qualify as acts of aggression. Included in the list is "the use of any weapon by a State against the territory of another State."[22] The resolution provides that the state that commits an act of aggression violates international law as embodied in the U.N. Charter.[23] The actions of states or their surrogates—in supporting or taking part in acts of aggression, which threaten vital national interests of a state or states—clearly fall within the scope of Article 2, paragraph 4 and authorize a response sufficient to end the violence and deter future aggression.[24] This responding coercion might include, for example, disruption of military information downlinks in satellites, sabotage of vital computer networks, or infiltration of electronic commercial transmission systems, where proportional to the original attack and where necessary to preclude future aggression.

D. The Right of Self-Defense

When the U.N. Charter was drafted in 1945, the right of self-defense was the only included exception to the prohibition of the use of force.[25] Customary international law had previously accepted reprisal, retaliation, and retribution as legitimate responses as well. Reprisal allows a state to commit an act that is otherwise illegal to counter the illegal act of another state. Retaliation is the infliction on the delinquent state of the same injury that it has caused the victim. Retribution is a criminal law concept, implying vengeance, which is sometimes used loosely in the international law context as a synonym for retaliation. While debate continues as to the present status of these responses, the U.S. position has always been that actions protective of U.S. interests, rather than punitive in nature, offer the

22. *Id.* at 143.

23. A fundamental purpose of the U.N. Charter is to "maintain international peace and security." U.N. CHARTER art. 1, para. 1. Article 5, paragraph 2, of the Definition of Aggression provides: "A war of aggression is a crime against international peace. Aggression gives rise to international responsibility." Definition of Aggression, *supra* note 18, at 144.

24. *See* U.N. CHARTER art. 2, para. 4. One potential act of destructive information warfare that would certainly trigger the definition of aggression would be the use of information technology to disrupt some vital element of the U.S. economic apparatus, such as the banking system or stock exchange, such that a Juggernaut would impede U.S. commercial activity.

25. U.N. CHARTER art. 51.

greatest hope of securing a lasting, peaceful resolution of international conflict.[26]

The right of self-defense was codified in Article 51 of the U.N. Charter. That article provides: "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 . . . ."[27] The use of the word "inherent" in the text of Article 51 suggests that self-defense is broader than the immediate Charter parameters. During the drafting of the Kellogg-Briand Treaty, for example, the United States expressed its views as follows:

> There is nothing in the American draft of an anti-war treaty which restricts or impairs in any way the right of self-defense. That right is inherent in every sovereign state and is implicit in every treaty. Every nation is free at all times and regardless of treaty provisions to defend its territory from attack or invasion and it alone is competent to decide whether circumstances require recourse to war in self-defense.[28]

Because self-defense is an inherent right, its contours have been shaped by custom and are subject to customary interpretation. Although the drafters of Article 51 may not have anticipated its use in protecting states through defensive actions using technological means, international law has long recognized the need for flexible application. Former Secretary of State George Shultz emphasized this point when he said: "The U.N. Charter is not a suicide pact. The law is a weapon on our side and it is up to us to use it to its maximum extent."[29] The final clause of Article 2, paragraph 4, of the Charter supports this interpretation and forbids the threat or

---

26. *See* Steve Rovine, *Contemporary Practice of the United States Relating to International Law*, 68 AM. J. INT'L L. 720, 736 (1974).

27. U.N. CHARTER art. 51.

28. 5 MARJORIE WHITEMAN, DIGEST OF INTERNATIONAL LAW § 25, at 971-72 (1965).

29. George Shultz, *Low Intensity Warfare: The Challenge of Ambiguity*, *in* U.S. Department of State Current Policy No. 783, at 3 (Jan. 1986).

use of force "in any manner inconsistent with the Purposes of the United Nations."[30]

The late Professor Myres McDougal of Yale University placed the relationship between Article 2, paragraph 4, and Article 51 in clearer perspective.

> Article 2(4) refers to both *the threat* and use of force and commits the Members to refrain from the "threat or use of force against the territorial integrity or political independence of any state, or in any manner inconsistent with the Purposes of the United Nations;" the customary right of self-defense, as limited by the requirements of necessity and proportionality, can scarcely be regarded as inconsistent with the purpose of the United Nations, and a decent respect for balance and effectiveness would suggest that a conception of impermissible coercion, which includes threats of force, should be countered with an equally comprehensive and adequate conception of permissible or defensive coercion . . . .[31]

Significant from Professor McDougal's interpretation is our correlative recognition of the right to counter the imminent threat of violent attack with all lawful available means, to include destruction of critical infrastructure that may preclude an imminent attack. This comprehensive conception of permissible or defensive actions, honoring appropriate responses to threats of an imminent nature, is merely reflective of the customary international law. It is precisely this anticipatory element, such as the elimination of a necessary command and control system in the moments before an unlawful attack, which is critical to an effective policy to counter aggression. This does not suggest a lack of international law constraints upon the determination of necessity for preemptive action. Rather, it suggests that legitimate consideration must be given to critical computer infrastructure on target lists, where the preemptive targeting of those systems could eliminate the possibility of one or more enemy attacks.

One aspect of this contextual appraisal of necessity, especially as it relates to the converse situation of responding after the fact to destructive

---

30. U.N. CHARTER art. 2, para. 4.

31. Myres McDougal, *The Soviet-Cuban Quarantine and Self-Defense*, 57 AM. J. INT'L L. 597, 600 (1963).

acts against our sovereignty, concerns the issue of whether force, even limited force where only systems are targeted, can be considered necessary if peaceful measures are available to lessen the threat. To require a state to tolerate attacks to its security or economic well-being without resistance, on the grounds that peaceful means have not been exhausted, is absurd. Once an attack has occurred, the failure to consider a military response, whether on critical infrastructure or otherwise, would play into the hands of those governments or groups who deny the relevance of law in their actions.

The legal criteria for the proportionate use of force are established once a state or identifiable group-supported attack on the security of the nation has taken place. No state is obliged to ignore an attack as irrelevant, and the imminent threat to the national security requires consideration of a response. One such lawful response is the elimination of the very computer infrastructure that allows the enemy's weapons systems to function.

A related, but more difficult issue concerns the elapsed time between the initial attack and the identification of the state or group responsible, thus authorizing responding coercion, possibly against critical infrastructure. Admittedly, there must be some temporal relationship between a destructive act and the lawful defensive response. Nevertheless, it would be unreasonable to preclude the United States from taking appropriate action after a delay in identifying an attacker—for example, where the actions of the perpetrator of the attack on the *USS Cole* precluded their immediate identification—based upon a doctrinaire determination that the threat of further destructive attack is no longer imminent.

The requirement of proportionality is linked to necessity. Professor McDougal and Dr. Feliciano have defined the rule as follows:

> Proportionality in coercion constitutes a requirement that responding coercion be limited in intensity and magnitude to what is reasonably necessary promptly to secure the permissible objectives of self-defense. For present purposes, these objectives may be most comprehensively generalized as the conserving of important values by compelling the opposing participant to terminate the condition which necessitates responsive coercion.[32]

32. MCDOUGAL & FELICIANO, *supra* note 17, at 242.

This definition simply requires a rational relationship between the nature of the attack and the nature of the response. Although the relationship need not approach precision, a nation subjected to an isolated attack may not be entitled to launch a strike on the offender nation's most critical infrastructure. Other canons of military practice, such as conservation of resources, support the principle of restraint in defense. The United Nations has condemned as reprisals those defensive actions that greatly exceed the provocation.[33] Where there is evidence that a continuation of destructive attacks will occur beyond the triggering event, however, such attacks could threaten the very fiber of a nation's ability to defend itself. Therefore, a response beyond that related to the initial intrusion would be legally appropriate to counter the continuing threat, and one could envision that such responding coercion could properly include an attack on critical computer systems.

Because the real-time relationship between threat and threat recognition is often compressed in the case of a violent military attack, such as the attack on the *USS Cole* in the Yemeni Aden harbor, strategy development is severely limited with respect to the non-military initiatives that may be considered in response. These lesser initiatives should always be the choice where available. However, traditional means of conflict resolution, authorized by law and customary practice, are often precluded because attacks by terrorists are, by nature, covert in execution, unacknowledged by the state or group sponsor, and practiced with silent effectiveness. As part of any response considered, therefore, the use of technical means to place electronic blocks on a nation's or organization's computer systems and telecommunications network may be an important adjunct of any proportionate response in the future.

IV. Operational-Legal Considerations in the Use of National Command Authority

A. Operational Law Context Provided in Rules of Engagement (ROE)

The rules of necessity and proportionality in determining the appropriateness of attacking critical computer infrastructure are given operational significance through ROE. The ROE are directives that a government may establish to define the circumstances and limitations, including targeting limitations, under which its forces will initiate and con-

33. *See* U.N. SCOR, 36th Sess., 2285-88 mtgs., U.N. Docs. S/PV 2285-88 (1981).

tinue responsive actions to eliminate the threat posed by an attack. That response might include the complete or partial destruction, through technical or other means, of the critical communications or information infrastructure of an adversary, where proportional to the threat. For the United States, adherence to the ROE provided by the National Command Authority ensures that crisis-response guidance is provided through the Joint Chiefs of Staff (JCS) to subordinate headquarters and deployed U.S. forces both during armed conflict and in periods of crisis short of war.[34]

Rules of engagement reflect domestic law requirements and U.S. commitments to international law. They are affected by political, as well as operational considerations. For the commander concerned with responding to a threat to his force, ROE represent limitations or upper bounds on how to use defensive or responsive systems and forces, without diminishing his authority to consider the available range of critical infrastructure targets where those systems pose immediate risks to his command.[35]

B. Evolution of JCS Rules of Engagement

Violence directed against a critical U.S. interest—whether military forces, a weapons platform, or critical infrastructure—represents hostile activity that may trigger the applicable ROE. Until June 1986, the only U.S. peacetime ROE applicable worldwide were the JCS Peacetime ROE for U.S. Seaborne Forces. These ROE, which until 1986 served as the basis for all commands' peacetime ROE, were designed exclusively for the maritime environment. In June 1986, Secretary of Defense Caspar Weinberger promulgated more comprehensive ROE for sea, air, and land operations worldwide.[36] These 1986 Peacetime ROE provided the on-scene commander with the flexibility to respond to hostile intent, as well as hostile acts and unconventional threats, with the minimum necessary force to limit the scope and intensity of the threat. The strategy underlying the

---

34. *See* CHAIRMAN, JOINT CHIEFS OF STAFF INSTR. 3121.01A, STANDING RULES OF ENGAGEMENT FOR U.S. FORCES (15 Jan. 2000) [hereinafter CJCS INSTR. 3121.01A].

35. *See generally* Lieutenant Commander Dale Stephens, *Rules of Engagement and the Concept of Unit Self Defense*, 45 NAVAL L. REV. 126 (1998).

36. CHAIRMAN, JOINT CHIEFS OF STAFF, PEACETIME RULES OF ENGAGEMENT FOR U.S. FORCES (June 1986).

1986 Peacetime ROE sought to terminate violence quickly and decisively, and on terms favorable to the United States.

In October 1994, Secretary of Defense Les Aspen approved the Standing Rules of Engagement for U.S. Forces (SROE), which significantly broadened the scope of the national ROE.[37] In January 2000, Secretary of Defense William Cohen approved SROE modifications, which delineated the scope of SROE application.[38] Significantly, the SROE "apply [to U.S. forces] during 'operations, contingencies, and terrorist attacks' *outside* the United States, and during attacks against the United States."[39] The SROE establish U.S. policy that, should deterrence fail, provides commanders flexibility to respond to crises with means that are proportional to the provocation and designed to limit the scope and intensity of the conflict, to discourage escalation, and to achieve political and military objectives. The inherent right of self-defense underlies the SROE, which are intended to provide general guidance on self-defense and the use of force consistent with mission accomplishment. The SROE apply to all echelons of command.[40]

The expanded national guidance represented in the SROE has greatly assisted in providing both clarity and flexibility of action for U.S. theater commanders. The approval by the Secretary of Defense ensures consistency in the way military commanders address the unconventional threats posed by the advanced command and control infrastructure systems of our adversaries. The SROE permits U.S. forces to respond to the hostile use of such infrastructure systems, within the application limits of the SROE. Targeting these systems specifically, where possible through the electronic means of U.S forces, may now be authorized where enemy platforms carrying these systems pose a specific threat to our forces.

When and if the DOD assets are used to eliminate or destroy critical enemy infrastructure in lawful self-defense, the specific—as opposed to standing—ROE developed for the operation will be guided by Presidential Decision Directive (PDD) 62, *Combating Terrorism*, signed into law by

---

37. CHAIRMAN, JOINT CHIEFS OF STAFF INSTR. 3121.01, STANDING RULES OF ENGAGEMENT FOR U.S. FORCES (1 Oct. 1994) (superceded by CJCS INSTR. 3121.01A, *supra* note 34).

38. CJCS INSTR. 3121.01A, *supra* note 34.

39. Major W.A. Stafford, *How to Keep Military Personnel from Going to Jail for Doing the Right Thing: Jurisdiction, ROE & the Rules of Deadly Force*, ARMY LAW., Nov. 2000, at 3 (quoting CJCS INSTR. 3121.01A, *supra* note 34, para. 3). *See generally* Stafford, *supra*, at 3-6 (discussing the current SROE in some detail).

40. CJCS INSTR. 3121.01A, *supra* note 34, paras. 1, 3, 6.

President Clinton in 1998.[41] Presidential Decision Directive 62 is the successor to National Security Decision Directive (NSDD) 138, signed by President Reagan in 1984, which determined that the threat of terrorism constituted a form of aggression that justified acts in self-defense.[42] Presidential Decision Directive 62 is more expansive in its coverage than NSDD 138 and addresses a broad range of unconventional threats, to include attacks on critical infrastructure, terrorist acts, and the threat of the use of weapons of mass destruction. The aim of the PDD is to establish a more pragmatic and systems-based approach to counter-terrorism. It recognizes the legality of computer network attack (CNA) and that preparedness is the key to effective consequence management. Presidential Decision Directive 62 creates the new position of National Coordinator for Security, Infrastructure Protection and Counter-Terrorism, which will coordinate program management through the Office of the National Security Advisor.[43]

V. Evaluation of Lawful Targeting Criteria

When a vital U.S. national interest—such as one of the critical infrastructure systems defined in PDD 63, *Critical Infrastructure Protection*[44]—is threatened or attacked by electronic or other computer-driven means, the system responsible for the threat may become a legal target that can be destroyed or disabled by military assets. Such destruction may be both necessary and proportionate under the law of armed conflict to eliminate the threat perceived.[45] The law of targeting is premised upon three

41. Presidential Decision Directive 62, Combating Terrorism (May 22, 1998) [hereinafter PDD 62].

42. National Security Decision Directive 138 (Apr. 3, 1984). *See* James P. Terry, *An Appraisal of Lawful Military Response to State-Sponsored Terrorism*, NAVAL WAR C. REV., May-June 1986, at 58 (discussing NSDD 138).

43. PDD 62, *supra* note 41. Richard C. Clarke, longtime senior National Security Council staff-member, was appointed as the first National Coordinator.

44. PDD 63, *supra* note 12. The eight categories of critical infrastructure listed are banking and finance, telecommunications, power generation/distribution, transportation, water services, emergency law enforcement, continuity of government, and public services. *Id.*; *see also* W. GARY SHARP, SR., CYBERSPACE AND THE USE OF FORCE 201-04 (1999) (providing a comprehensive review of the major elements of PDD 63 and the requirements it imposed upon the government departments and the private sector).

45. The law of targeting is a subset of the law of armed conflict, and the dual requirements of necessity and proportionality, the twin pillars of that body of law, are equally applicable to target selection and approval. *See, e.g.,* Jonathan P. Tomes, *Legal Implications of Targeting for the Deep Attack,* MIL. REV., Sept. 1988, at 70-76.

fundamental principles: the means of injuring an enemy are not unlimited; it is unlawful to launch attacks against civilian populations; and distinctions must be made between combatants and non-combatants, with non-combatants spared to the extent possible.[46] These rules are complimented by other, more specific, customary notions and by international conventions.

Commonly accepted is the premise that only military objectives may be attacked.[47] Military objectives, however, embrace more than troops, weapons systems, and military equipment. Rather, they include all objects which, by their nature, purpose, use, or location, effectively contribute to the military initiative being pursued and whose destruction would constitute a "military advantage" to the force attacking the objective.[48] Instead of using language incorporating the term "military advantage," Article 52(2) of the 1977 Geneva Protocol I uses the broader phrase, "make an effective contribution to enemy action."[49] This expansive definition includes all dual-use facilities used to support military operations, such as communications networks, command and control facilities, and other critical infrastructure such as petroleum storage areas, power generation plants, and economic targets that indirectly but effectively support and sustain the aggressor's capability to continue its military operations.[50] This definition would clearly encompass computer networks, to include civilian

---

46. *See* 20th International Conference of the Red Cross, Fundamental Principles of the Red Cross: Res. XXVIII (1965); G.A. Res. 2444, U.N. GAOR, 23d Sess., Supp. No. 18, at 1(c), U.N. Doc. A/7218 (1968) (adopting Red Cross. Res. XXVIII); G.A. Res. 2675, U.N. GAOR, 25th Sess., Supp. No. 28, at 2, U.N. Doc. A/8028 (1970) (affirming the principles of G.A. Res. 2444). The United States considers these fundamental principles as customary international law. *See* Letter from General Counsel, Department of Defense, to Senator Edward Kennedy (Sept. 22, 1972), *in* 67 AM. J. INT'L L. 122 (1973).

47. This customary rule of international law was codified for the first time in 1977. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, Dec. 12, 1977, art. 57(4), 1125 U.N.T.S. 3 [hereinafter Protocol I].

48. This definition is accepted by the United States as declarative of the customary rule. *See* DEP'T OF NAVY, ANNOTATED SUPPLEMENT TO THE COMMANDER'S HANDBOOK ON THE LAW OF NAVAL OPERATIONS, NWP 1-14M, at 8.1.1 (1995) [hereinafter ANNOTATED SUPPLEMENT].

49. Protocol I, *supra* note 47, art. 52(2).

50. *See id.*

networks, supporting military operations, communications, and command and control. All such military objectives may be attacked.

While military objectives, including computer networks supporting military requirements, are properly included within target sets, civilians and civilian objects are not.[51] Civilian objects consist of all civilian property and activities other than those used to support or sustain the capability for armed aggression on the part of the attacker.[52] Thus, activities normally considered civilian in character—when conducted in support of a nation's aggression, where implemented to shield an aggressor's identification, or where employed to preclude effective and lawful response to unlawful attack—would, under these circumstances, become the lawful objects of attack. The DOD General Counsel made this point succinctly in May 1999, when she wrote:

> If the international community were persuaded that a particular computer attack or a pattern of such attacks should be considered to be an "armed attack," or equivalent to an armed attack, it would seem to follow that the victim nation would be entitled to respond in self-defense either by computer network attack or by traditional military means in order to disable the equipment and personnel that were used to mount the offending attack.[53]

Stated another way, a civilian computer system, used either to conduct an attack or to shield an aggressor's attack from discovery, becomes a valid and lawful target when: (1) aggression against critical infrastructure equating to an armed attack has occurred; and (2) the total or partial destruction, capture or neutralization of the computer system offers the United States or its allies a definite military advantage.

Computer networks are not *per se* illegal targets under traditional international law criteria. The standard law of armed conflict analysis must be applied in every instance, however. This analysis determines whether the critical computer infrastructure of an attacking state or other non-state aggressor constitutes a valid target under the circumstances. The target review must conclude that the specific computer network or other critical infrastructure system—by its nature, location, capability, purpose

---

51. *See id.* art. 51(1) (codifying this principle of customary international law).

52. *Id.* art. 52 (1) (defining civilian objects as "all objects which are not military objectives as defined in paragraph 2").

53. GENERAL COUNSEL, DEP'T OF DEFENSE, AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS 22 (1999) [hereinafter DOD GC ASSESSMENT].

or use—makes an effective contribution to the military capability of the offending state *and* that its destruction, capture or neutralization offers the United States or its allies a definite military advantage.

The fact that a computer system or other critical infrastructure is a valid target does not necessarily mean it should be attacked. In weighing the political and strategic implications, refraining from an in-kind, albeit legal, response may provide greater benefit. For example, such restraint may be appropriate to facilitate a shift in world sentiment, a movement of nations in terms of their allegiances, an opportunity for international bodies like the U.N. to become engaged, or an opportunity to open or expand previously closed political channels.

A final concern relates to collateral damage. While collateral damage does not have a different definition in a CNA context, additional steps may be required to show that reasonable precautions were taken to avoid unnecessary destruction. Obviously, the effects of a CNA are less predictable than the effects of conventional weapon systems. Lawrence G. Downs, Jr., explains a related and even more important consideration for the state using digital data warfare in lawful self-defense.

> When the U.S. Army contracted a study to determine the feasibility of developing DDW [digital data warfare] -type viruses for military use, many people had misgivings that were summed up by Gary Chapman, program director of Computer Professionals for Social Responsibility. "Unleashing this kind of thing is dangerous," he said. "Should the virus escape, the United states heads the list of vulnerable countries. Our computers are by far the most networked."[54]

These concerns make it clear that any weapon developed to provide CNA capability must be both predictable and capable of being armed and disarmed; otherwise they will unduly threaten innocent civilians in the target state *and* the user state. Downs is correct when he suggests that weaponeers should, in general, co-develop a detection and immunization program for all viruses they intend to use. [55] In this way, a DDW attack gone wrong cannot inadvertently do harm to the attacker. In short, users and

---

54. Lawrence G. Downs, Jr., *Digital Data Warfare: Using Malicious Computer Code as a Weapon*, NAT'L DEF. U. INST. FOR STRATEGIC STUD. 58 (1995).

55. *Id.*

developers of DDW need to be aware of the risks and the absolute requirement for predictability when developing DDW code.

VI. The Impact of International Agreements and Domestic Communications Law on CNA

Military planners developing a cyber-defense capability must also consider the international agreements regulating the use of space. The United States is a party to four such multilateral conventions: (1) the 1967 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies (Outer Space Treaty);[56] (2) the 1968 Agreement on the Rescue of Astronauts, Return of Astronauts, and the Return of Objects Launched in Space (Rescue and Return Agreement);[57] (3) the 1972 Convention on International Liability for Damages Caused by Space Objects (Liability Convention);[58] and (4) the 1975 Convention on Registration of Objects Launched into Outer Space (Space Objects Registration Treaty).[59]

These four conventions reiterate principles which are so widely accepted that they are viewed as reflective of customary international law, even as between non-parties. These accepted principles include the premises that: (1) access to outer space is free and open to all nations;[60] (2) each user of outer space must show due regard for the rights of others;[61] (3) states that launch space objects are liable for damage for any damage they may do in space, in the air, and on land;[62] and (4) space activities are subject to the general principles of international law.[63] Military planners).

---

56. Jan 27, 1967, 18 U.S.T. 2410, 610 U.N.T.S. 205 [hereinafter Outer Space Treaty].

57. Apr. 26, 1968, 19 U.S.T. 7570, 672 U.N.T.S. 119.

58. Mar. 29, 1972, 24 U.S.T. 2389, 961 U.N.T.S. 187 [hereinafter Liability Convention].

59. Jan. 14, 1975, 28 U.S.T. 695, 1023 U.N.T.S. 15.

60. Outer Space Treaty, *supra* note 56, art. I.

61. *Id.* art. IX.

62. The Liability Convention elaborates the general principles of international liability for damages set forth in Article VII of the Outer Space Treaty. Liability Convention, *supra* note 58, arts. Ia, II, III, VI. The Liability Convention also address joint and several liability. *Id.* arts. IV, V.

63. *See* ANNOTATED SUPPLEMENT, *supra* note 48, at 2-38 ("International law, including the United Nations Charter, applies to the outer space activities of nations.").

should heed not only the international agreements, but also these underlying principles.

Restrictions imposed by some of the preceding conventions and principles may not apply in wartime. The DOD General Counsel concluded, in her 1999 assessment of international legal issues related to information operations, that the non-interference principle—which preserves the right to use outer space—does not apply during armed conflict. She stated:

> There appears to be a strong argument that the principle of non-interference established by these agreements is inconsistent with a state of hostilities, at least where the systems concerned are of such high military value that there is a strong military imperative for the adversary to be free to interfere with them, even to the extent of destroying the satellites in the system. As indicated in the discussion of treaty law in the introduction to this paper, the outcome of this debate may depend on the circumstances in which it first arises in practice. Nevertheless, it seems most likely that these agreements will be considered to be suspended between the belligerents for the duration of any armed conflict, at least to the extent necessary for the conduct of the conflict.[64]

Underlying this statement by the DOD General Counsel is the obvious principle that the right of self-defense is in no way abrogated by other international commitments entered into by a nation.

One significant convention with apparent applicability to U.S. interdiction of foreign communications infrastructure is the International Telecommunications Convention (ITC) of 1982. In Article 35, the ITC prohibits interference by member states with the communications of other member states. The ITC has an exception for military transmissions in Article 38, however, which arguably would authorize information operations conducted by military forces.[65] The Office of Legal Counsel in the U.S. Department of Justice took this position in July 1994 when it ruled,

---

64. DOD GC ASSESSMENT, *supra* note 53, at 32.

65. The same requirements were stated previously in the International Telecommunications Convention, Malaga-Torremolinos, Oct. 25, 1973, 28 U.S.T. 2495, T.I.A.S. 8572. The Malaga-Torremolinos Convention was replaced by the International Telecommunications Convention, Nairobi, 6 Nov. 1982, 32 U.S.T. 3821; T.I.A.S. 9920 (entered into force for the United States 10 January 1986).

with respect to planned broadcasts into Haiti concerning boat operations, that the ITC did not prohibit such broadcasts.[66]

An unlikely convention to consider when discussing cyber operations is the 1907 Hague Convention on Neutrality on Land,[67] which could affect satellite relay operations. That convention does not apply to systems that generate information, but does apply to relay facilities and requires that facilities of other states not be disrupted. While Articles 8 and 9 contemplate only telegraph and telephone cable links, they would arguably apply to satellite links as well.[68] However, since most computer-based systems and certainly all that control critical infrastructure generate information as well as relay that information, the prohibition against disruption would likely not apply.

International consortia that lease satellite nodes for commercial communications raise another potential concern. These organizations include International Telecommunications Satellite, International Marine/Maritime Satellite, Arab Satellite Communications Organization, European Telecommunications Satellite, and European Organization for the Exploration of Meteorological Satellites. The contracts signed by each user, which are nearly identical in the case of each provider, state that the system must be used exclusively for peaceful purposes.[69] While the United States has leased one or more nodes from at least one of these providers in the past, it retains separate satellite capabilities should it need to defend itself through digital data warfare.[70]

Domestic communications law provides a final consideration for cyber operations. Congress passed 47 U.S.C. § 502 in 1994 to implement the ITC requirement that member states enact legislation to prohibit interference with the communications of other members.[71] During Haiti operations in October 1993, just as it would again in July 1994, the Office of Legal Counsel to the Department of Justice issued a written opinion to the effect that the § 502 does not apply to military actions by the United States.[72] Thus, domestic law would not preclude the United States from

66. *See* DOD GC ASSESSMENT, *supra* note 53, at 36-37.

67. Hague Convention No. V Respecting The Rights and Duties of Neutral Powers and Persons in Case of War on Land, Oct. 18, 1907, 36 Stat. 2310-2331; 1 BEVANS 654-668.

68. *Id.* arts. 8-9.

69. *See generally* SHARP, *supra* note 44. Where this provision is violated, however, and a satellite node is used for aggression, the inviolability of the system from attack would arguably cease.

70. *See id.*

using CNA when it is engaged in an armed conflict or in operations short of war, provided necessity and proportionality dictate the use of CNA.

VII. Conclusion

From the preceding analysis, it is clear that computer networks critical to the functioning of enemy infrastructure systems can be valid military targets under customary international law principles. Further, the use of CNA does not violate applicable international conventions. During armed conflict, military and dual-use computer infrastructure are always legitimate targets provided they make an effective contribution to the adversary's military effort and if their destruction would offer a definite military advantage. The criteria for determining military advantage include the nature, location, purpose or use of the offending computer network and whether it is used to threaten U.S. or allied interests. Similarly, under self-defense principles, these same computer networks may be attacked as lawful targets in circumstances prior to armed conflict if their partial or total destruction is a necessary and proportional response to an attack. As a corollary to this rule, simply because a particular target is valid in a military sense does not mean that it must be attacked; a nation must always analyze potential targets in light of the applicable political, tactical, and strategic implications.

In the target analysis required for CNA, as with more traditional targets, reasonable precautions must be taken to discriminate between military and civilian networks. This will be most difficult with dual-use systems such as commercial telephone exchanges that can serve both a military and civilian purpose. In this area, the political implications are

---

71. 47 U.S.C. § 502 (1994**)** provided:

> Any person who willfully and knowingly violates any rule, regulation, restriction, or condition made or imposed by the Commission under authority of this Act, or any rule, regulation, restriction, or condition made or imposed by any international radio or wire communications treaty or convention, or regulations annexed thereto, to which the United States is or may hereafter become a party, shall, in addition to any other penalties provided by law, be punished, upon conviction thereof, by a fine of not more than $500 for each and every day during which such offense occurs.

Id.

72. *See* DOD GC ASSESSMENT, *supra* note 53, at 38.

magnified and must be carefully weighed. However, it is clear that computer networks—such as those serving commercial infrastructure, government agencies, and banking and financial institutions—can constitute legitimate targets if those networks contribute to the enemy's war-sustaining capability such that their destruction would constitute a definite military advantage. Conversely, attacks on computer networks—such as those serving civilian infrastructure, food distribution systems, and water supply systems—would be prohibited if designed solely to support the civilian population.

International communications law likewise contains no direct or specific prohibition against the conduct of CNA or other information operations by military forces during armed conflict or in response to aggression. Again, the law of self-defense enjoys a superior position in the hierarchy of a nation's sovereign rights. Moreover, the practice of nations provides persuasive evidence that telecommunications treaties are regarded as suspended among belligerents during international armed conflict. Similarly, domestic communications laws, and specifically 47 U.S.C. § 502, do not prohibit military information operations. It is apparent that computer network attacks—authorized by the Fiscal Year 2000 Unified Command Plan and implemented through the JIOC and NIPC—can be employed in a manner consistent with domestic law, as well as customary and conventional international law principles.