



---

---

# Responding to Attacks on Critical Computer Infrastructure

## What Targets? What Rules of Engagement?

---

---

James P. Terry

### Introduction

In 1997, in an exercise emphasizing infrastructure security, the National Security Agency exposed the United States' vulnerability to the disruption of computer operations at our major military commands at the hands of a hostile State or an organization with hostile intent.<sup>1</sup> A year earlier, US authorities had detected the introduction of a program, called a "sniffer," into computers at NASA's Goddard Space Flight Center, that permitted 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.<sup>2</sup> Of equal concern, an FBI report in 1999 detailed Chinese efforts to attack US Government information systems, including the White House network.<sup>3</sup> These actual and projected interstate intrusions into Government computer networks once thought secure raise important questions concerning what, if any, rights in self-defense are triggered by such attacks. More importantly, they pose the issue of how the right of self-defense, if

an attack impacts a vital national security interest, would be translated into effective rules of engagement, specifically, legally defensible targeting decisions.

### **Understanding the Threat**

The world of information operations represents an environment created by the confluence of cooperative networks of computers, information systems, and telecommunication infrastructures. The concern addressed here relates to the threat posed to these systems when operations are unlawfully disrupted, denied, or degraded, or when secure information that is stored in computers or computer networks is destroyed, compromised, or altered in such a way that it has a destructive effect on the national security interests of a nation. Computer espionage and computer network attacks, as well as the subversion of political, economic, and/or non-military information bearing on a nation's capabilities and vulnerabilities, may well constitute an unlawful use of force warranting a military response under traditional international law principles.

The threshold issues which emerge are: (1) which peacetime interstate activities within the telecommunications highway constitute a threat or use of force; (2) when does such a threat constitute an attack under the international law such that a right to use force in self-defense exists; and (3) what is an appropriate response. To respond to these issues, we must understand the military applications of information technology. This requires an understanding of the Internet. The Internet was originally a network of computers linked by telecommunications infrastructure and managed by the Department of Defense (DoD) in the 1970s. The internal computer networks of universities and private research facilities were merged through the development of hypertext, created in 1989 as the primary platform of the Internet. It (hypertext) translates diverse computer protocols into standard format.

This hypertext process, while extremely beneficial to both the military and civilian sectors, has created vulnerabilities. The World Wide Web, the full implementation of the Internet, which is at once the heart of the Defense Reform Initiative and key to the reengineering and streamlining of our business practices, can provide adversaries with a potent instrument to obtain, correlate, evaluate, and *adversely affect* an unprecedented volume of aggregated information critical to proper management of DoD and US infrastructure capabilities.

This chapter responds to these attacks on US infrastructure. Even though international law could not have anticipated specific information warfare concerns when the Hague Conventions of 1899, addressing means and methods of

warfare, were negotiated, the drafters thereof did anticipate technological change. The “Martens Clause,” included within both Hague Convention II 1899, and Hague Convention IV 1907, provides that even in cases not explicitly covered by specific agreements, civilians and combatants remain under the protection and authority of principles of international law derived from established custom, principles of humanity, and the dictates of public conscience, and therefore are not left to the arbitrary judgment of military commanders.<sup>4</sup> This provision was considered necessary to prevent future unnecessary and/or disproportionate destruction from weapons systems not yet developed. The drafters had just witnessed unimaginable carnage in the Crimean War and the American Civil War resulting from advanced rifling techniques and other innovations, and were cognizant that warfare was rapidly changing. As Greenberg, *et al.*, so accurately state, as a result of the Martens Clause, “attacks will be judged largely by their effects, rather than by their methods.”<sup>5</sup>

## The Legal Parameters for Response

### UN Charter System

The existing legal regime available to deter destructive actions through computer technology includes the United Nations 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 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 state, or in any manner inconsistent with the Purposes of the United Nations.”<sup>6</sup>

The underlying purpose of Article 2(4), to regulate aggressive behavior between States, is identical to that of its precursor, the Covenant of the League of Nations. Article 12 of the Covenant stated that League members were obliged not to “resort to war.”<sup>7</sup> This terminology, however, left unmentioned actions which, although clearly hostile, could not be considered to constitute acts of war. The drafters of the UN Charter wished to ensure that the legal niceties of a conflict’s status did not preclude cognizance by the international body. Thus, in drafting Article 2(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.<sup>8</sup>

## UN General Assembly Resolution 2625

The United Nations General Assembly has clarified the scope of Article 2 in two important resolutions, both adopted unanimously.<sup>9</sup> Resolution 2625, the Declaration on Friendly Relations, describes behavior which constitutes the “unlawful threat or use of force” and enumerates standards of conduct by which States must abide.<sup>10</sup> Contravention of any of these standards of conduct is declared to be in violation of Article 2(4).<sup>11</sup>

## UN 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.”<sup>12</sup> This resolution contains a list of acts which qualify as acts of aggression. Included in the list is “the use of any weapon by a State against the territory of another State.”<sup>13</sup> The resolution provides that the State which commits an act of aggression violates international law as embodied in the Charter.<sup>14</sup>

The actions of States or their surrogates in supporting or taking part in acts of aggression through information technology that threaten vital national interests of a State or States, whether through disruption of military information downlinks in satellites, sabotage of vital computer networks, or infiltration of electronic commercial transmission systems, clearly fall within the scope of Article 2(4).<sup>15</sup>

## The Relationship Between Customary International Law and the Charter

When the UN Charter was drafted in 1945, the right of self-defense was the only included exception to the prohibition of the use of force. 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, that 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 US position has always been that actions protective of US interests, rather than being punitive in

nature, offer the greatest hope of securing a lasting, peaceful resolution of international conflict.<sup>16</sup>

The right of self-defense was codified in Article 51 of the 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. . . ." <sup>17</sup> 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.<sup>18</sup>

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 from destructive actions perpetrated through technological means, international law has long recognized the need for flexible application. Former Secretary of State George Shultz emphasized this point when he stated that: "The UN 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."<sup>19</sup> The final clause of Article 2(4) supports this interpretation and forbids the threat or use of force "in any manner inconsistent with the Purposes of the United Nations."<sup>20</sup>

The late Professor Myres McDougal, of Yale Law School, has placed the relationship between Articles 2(4) and 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 . . . .<sup>21</sup>

Significant from Professor McDougal's interpretation is our correlative recognition of the right to counter the imminent threat of techno-violence as well as actual destructive acts of information warfare. This comprehensive conception of permissible or defensive actions, honoring appropriate response to threats of an imminent nature, is merely reflective of the customary international law. It is precisely this anticipatory element that is critical to an effective policy to counter destructive acts against critical information systems. This does not suggest the lack of international law restraints upon the determination of necessity for preemptive action. Rather, it suggests that legitimate considerations for effective response to evidence of imminent destructive acts against critical communications infrastructure must be appraised in the total context in which they occur. One aspect of this contextual appraisal of necessity, especially as it relates to responding after the fact to destructive acts against our critical information systems, concerns the issue of whether force can be considered necessary if peaceful measures are available to lessen the threat. To require a State to tolerate attacks on infrastructure critical to its security and/or economic well-being without resistance, on the grounds that peaceful means have not been exhausted, is absurd. Once an attack on critical infrastructure has occurred, the failure to consider a military response 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 is established once a State or identifiable group-supported attack on technical infrastructure critical to 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.

A related, but more difficult, issue concerns the elapsed time between the attack on critical infrastructure and the identification of the State or group responsible. Admittedly, there must be some temporal relationship between a destructive act and the lawful defensive response. Nevertheless, it would be unreasonable to preclude the victim of techno-violence from redress, based upon a doctrinaire determination that the threat of further destructive intrusions into a critical system is no longer imminent, when the perpetrator's own actions have precluded immediate identification.

The requirement of proportionality is linked to necessity. Professor McDougal and Dr. Feliciano define 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.<sup>22</sup>

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 intrusion and disruption of an important computer system may not be entitled to launch a strike on the offender nation. 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 exceeded the provocation.<sup>23</sup> Where there is evidence that a continuation of destructive electronic sabotage will occur, beyond the triggering event, that could threaten the very fiber of a nation's ability to defend itself, however, a response beyond that related to the initial intrusion would be legally appropriate to counter the continuing threat.

Because the real-time relationship between threat and threat recognition is often compressed in the techno-violence arena, strategy development is severely limited with respect to the non-military initiatives that may be considered in response to cyber-attack, although they are always the options of choice where available. Traditional means of conflict resolution, authorized by law and customary practice, are often precluded because attacks on computer systems are, by nature, covert in execution, unacknowledged by the State or group sponsor, and practiced with silent effectiveness.

It must be noted, however, that non-coercive efforts to avoid attacks on computer systems and telecommunication networks are also important. Diplomatic action, alone or in concert with allies or international organizations with conceivable successful impact upon a State or group considering such a cyber initiative, should be considered and employed whenever possible. In 1998, for example, the UN General Assembly passed Resolution 53/70,<sup>24</sup> an initiative of the Russian Federation, that called upon Member States "to promote at multilateral levels the consideration of existing and potential threats in the field of information security."<sup>25</sup> The United States supported this resolution with the following pertinent comments:

The General Assembly's adoption of the resolution in plenary will launch the international community on a complex enterprise encompassing many interrelated factors which delegates . . . do not ordinarily address. For example, the topic includes technical aspects that relate to global communications—as well as non-technical issues associated with economic cooperation and trade, intellectual property rights, law enforcement, anti-terrorist cooperation, and

other issues that are considered in the Second and Sixth Committees. Further, the actions and programs of governments are by no means the only appropriate focus, for the initiative also involves important concerns of individuals, associations, enterprises, and other organizations that are active in the private sector.<sup>26</sup>

Despite such international initiatives focusing upon multilateral cooperation, the opportunity to look to outside assistance in protecting secure transmissions and critical systems in circumstances where our national security is threatened, is likely illusory. That responsibility will most certainly remain exclusively within the National Command Authorities.

### **Operational-Legal Considerations in Addressing Techno-Violence**

#### **Operational Law Context Provided in Rules of Engagement**

The rules of necessity and proportionality in the information warfare scenario are given operational significance through rules of engagement (ROE). ROE are directives that a government may establish to define the circumstances and limitations under which its forces will initiate and continue responsive actions to eliminate the threat posed by an attack through technical or other means on critical communications/information infrastructure. In the US context, this ensures that the National Command Authorities' guidance for handling crisis responses to techno-violence and other threats is provided, through the Joint Chiefs of Staff (JCS), to subordinate headquarters and deployed US forces both during armed conflict and in periods of crisis short of war.

ROE reflect domestic law requirements and US commitments to international law. They are impacted by political, as well as operational considerations. For the commander concerned with responding to a threat to his communications/command and control infrastructure, ROE represent limitations or upper bounds on how to utilize defensive and/or responsive systems and forces, without diminishing the authority to effectively protect his own critical infrastructure from attack.

#### **Evolution of JCS Rules of Engagement**

Techno-violence against a critical US computer system, whether information, communications, or command and control-related, represents hostile activity which may trigger the applicable ROE. Until June 1986, the only US peacetime ROE applicable worldwide were the JCS Peacetime ROE for US

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 Weinberger promulgated more comprehensive ROE for sea, air, and land operations worldwide.<sup>27</sup> The 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 minimum necessary force, and to limit the scope and intensity of the threat. The strategy underlying the 1986 ROE sought to terminate violence quickly and decisively on terms favorable to the United States. In October 1994, Secretary of Defense Aspin approved the Standing Rules of Engagement for US Forces (SROE), which significantly broadened the scope of US national ROE.<sup>28</sup> As established in the SROE, US policy, should deterrence fail, provides flexibility to respond to crises with options that are both proportional to the provocation and designed to limit the scope and intensity of the conflict, discourage escalation, and achieve political and military objectives. The inherent right of self-defense establishes the policy framework for the SROE. These SROE are intended to provide general guidelines on self-defense and are applicable worldwide to all echelons of command. Providing guidance governing the use of force consistent with mission accomplishment, they are to be used, absent superseding guidance, in operations other than war, during transition from peacetime to armed conflict or war, and during armed conflict.

The expanded national guidance represented in the 1994 SROE, as further refined in the 2000 SROE, has greatly assisted in providing both clarity and flexibility of action for our theater commanders. The approval by the Secretary of Defense has ensured consistency in the way all military commanders, wherever assigned, address unconventional threats such as those posed to our advanced command and control infrastructure systems when these systems or computer networks are destroyed, compromised, or altered so as to have a destructive effect on the national security interests of the nation.

### **Targeting Considerations**

The SROE, as they relate to information warfare, are implemented through the law of targeting, a subset of the law of armed conflict. The law of targeting is based upon three fundamental principles. These are:

- The right of States to adopt means of injuring the enemy is not unlimited.
- The launching of attacks against the civilian population as such is prohibited.

- Distinctions must be made between combatants and noncombatants, to the effect that noncombatants are spared to the extent possible.<sup>29</sup>

Because the law of armed conflict is an eminently practical law which takes into account military efficiency, these basic principles are also consistent with the response authorized for non-violent but equally destructive forms of coercive activity, such as sabotage of critical defense computer systems. Moreover, targeting theory is premised upon practical considerations that serve the purpose of defining the objects of legitimate and proportional response to each variant of aggression, whether it be an armed attack on US facilities or an equally debilitating computer-assisted attack, and of providing functional targeting criterion to the responsible official, whether civilian or military.

### *Executive Order 13010*

The key, then, to an effective response to the threat posed by States or groups engaging in attacks against US critical infrastructure must be the commitment to address the attacks they sponsor within the scope of the law of armed conflict. We must think of cyber aggression as a variant of terrorist activity. This is precisely the approach taken by the Clinton Administration. When President Clinton signed Executive Order (EO) 13010 on July 15, 1996, thereby establishing the President's Commission on Critical Infrastructure Protection (CCIP), he declared that certain designated "national infrastructures are so vital that their incapacity or destruction . . . would have a debilitating impact on the defense or economic security of the United States." The eight categories of critical infrastructure designated in the EO as requiring the development of a national strategy for protection include: continuity of government; telecommunications; transportation; electric power systems; banking and finance; water supply systems; gas and oil storage and transportation; and emergency services (medical, police, fire and rescue). Chaired by Robert T. Marsh, a retired Air Force General, the CCIP was tasked with developing a comprehensive national strategy for protecting critical infrastructures from electronic and physical threats. On October 13, 1997, the CCIP issued the unclassified version of its report, entitled "Critical Foundations: Protecting America's Infrastructure." In addition to determining the challenge of adapting to a changing culture, the report found the existing legal framework inadequate to deal with threats to critical infrastructure. The centerpiece of the CCIP's national strategy, then, is the domestic and international legal regime required to protect against threats to critical infrastructure. Although the report itself provides few specifics, on May 22, 1998, the Administration issued Presidential Decision Directives (PDD) 62 and 63 in implementation of its policy framework.

### *Presidential Decision Directive 62*

PDD 62, Combatting Terrorism, is the successor to National Security Decision Directive (NSDD) 138, signed by President Reagan on April 3, 1984, which determined that the threat of terrorism constitutes a form of aggression and justifies acts in self-defense.<sup>30</sup> PDD 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 protection of critical infrastructure and counter-terrorism, with preparedness the key to effective consequence management. PDD 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.<sup>31</sup>

### *Presidential Decision Directive 63*

PDD 63, Critical Infrastructure Protection, mandates that the National Coordinator, established in PDD 62, initiate immediate action between the public and private sectors to assure the continuity and viability of critical infrastructures. The goal established within PDD 63 is to establish a reliable interconnected and secure information system infrastructure by the year 2003. A National Plan Coordination Staff is tasked with integrating the plans developed by the various departments of government serving as lead agencies within their respective areas of responsibility into a comprehensive National Infrastructure Assurance Plan, overseen by the National Infrastructure Assurance Council. The Council includes representation from both the public and private sectors. Under the PDD, the Federal Bureau of Investigation's National Infrastructure Protection Center, established in February 1998, will continue to provide a control and crisis management point for gathering information on threats to critical infrastructure and for coordinating the federal government's response.<sup>32</sup>

### Targeting in the Context of PDD 62 and PDD 63

The issue remains, however, should the Critical Infrastructure Plan fail, what legal remedy can be applied under the law of armed conflict. If a response is justified, what targets in a perpetrator country are proportional to the threat posed by destruction or compromise of critical infrastructure. Again, our experience in addressing terrorism must be reviewed. The reason this is necessary is that the flexibility of the law of armed conflict in addressing unconventional threats provides far more salient options than domestic law or intelligence law in cases

where the very fiber of our national security is placed at risk. For example, as W. Gary Sharp correctly points out, an unlawful entry into and/or compromise of a critical national security system by an individual or individuals can be viewed as criminal activity under the jurisdiction of the federal and state law enforcement officials. The same intrusion by the same individual or individuals representing a State or international entity could be viewed as lawful espionage or intelligence gathering practiced by all States. If, however, that intrusion and the debilitating effect it has on national security can appropriately be characterized as an attack on vital US national interests, the range of options is greatly enhanced.<sup>33</sup>

This is important because the State or group attempting to compromise US national security through the calculated sabotage of critical infrastructure *is attacking the nation*, not with bombs or bullets, but with the intent of destroying equally critical elements of national well-being and sovereignty. The loss of a power grid or of a US telecommunications network through computer generated viruses for an extended period of time would have the capacity of placing more Americans at risk than a significant military threat.

The United States was jolted into an awareness of the changing character of aggression when its embassy in Tehran was seized on November 4, 1979, by Iranian militants who enjoyed the support of Ayatollah Khomeini's revolutionary government.<sup>34</sup> In August 1998, US Embassies in Nairobi and Dar-es-Salaam were the subjects of unconventional warfare attacks, resulting in the significant loss of life in Nairobi. In the attacks, a US response was only possible because of the linkage established between Osama bin Laden's organization and the assaults on American interests. The thrust of the new US strategy, outlined in PDD 62, must be to reclaim the initiative lost while the United States pursued a reactive policy toward unconventional threats, especially those to its critical infrastructure.

An examination of authorized responses (and the selection of appropriate targets) to techno-violence requires an understanding that cyberterrorism is a strategy that does not follow any of the traditional military patterns. In fact, a fundamental characteristic of attacks on critical infrastructure is its violation of the established norm of information security. The only norm for cyberterrorism is effectiveness. While traditional international law requires discrimination among those affected by an attack and proportion in its intensity, the nature of information warfare and cyberterrorism is such that success is measured by the extent and duration of destructiveness to the systems targeted, with no concern for those affected. In the contemporary language of defense economics, they wage countervalue rather than counterforce warfare.

Why is this important? It is important because the only credible response to attacks on critical infrastructure is deterrence. There must be an assured,

effective reaction that imposes unacceptable costs on the perpetrators and those who make possible their activities. For domestic intruders, the criminal law may suffice. For those operating outside the United States, the US reaction must counter the cyber-terrorist's strategy within the parameters of international law and PDD 62. Those who suggest otherwise neither understand the inherent flexibility of international law nor the cost of violating that law.

In this regard, a case for a response in self-defense is not persuasive either on the political or legal level unless a reasonable basis of necessity is perceived. Those to whom a justification is addressed (that is, other governments or the public) will consider whether it is well founded; they will not regard the use of force as a purely discretionary act. An important dimension of this question concerns the separate issue of when does action become necessary; that is, when is the use of force necessary to enforce adherence to the norm of information security. As Professor Lauterpacht has pointed out, every State judges "for itself, in the first instance, whether a case of necessity in self-defense has arisen," but that "it is obvious that the question of the legality of action taken in self-preservation is suitable for determination and must ultimately be determined by a judicial authority or political body . . . ." <sup>35</sup> The United States has long taken the position that each nation is free to defend itself and is the "judge of what constitutes the right of self-defense and the necessity . . . of same." <sup>36</sup> Similarly, more than a half-century ago, Secretary of State Frank Kellogg noted that when a State has resorted to the use of force, "if it has a good case, the world will applaud and not condemn its actions." <sup>37</sup>

### **A Pro-Active Response to Threats to Critical Infrastructure is Authorized under International Law**

The decision to respond with force against techno-violence must be as closely tied to a clear objective as in the case where planning is conducted at the higher end of the coercion spectrum. Because the relationship between objective and threat is often unclear in the low intensity conflict arena, a strategy to fight cyberterrorism must always focus on the underlying political purpose of the State or group attempting to degrade or destroy an element of critical US infrastructure, whether that element be commercial, communications, intelligence, or defense-related. That purpose is unquestionably the degradation of our critical systems such that we are unable to defend ourselves militarily or protect ourselves from serious political or financial overreaching on the part of our adversaries. How do we counter this purpose, this objective? Former Secretary of State Shultz was correct when he stated that US policy

“must be unambiguous. It must be clearly and unequivocally the policy of the United States to fight back—to resist challenges, to defend our interests . . . .”<sup>38</sup> Implementation of this pro-active policy requires that we make the fullest use of all the weapons in our arsenal. These should include not only those defensive and protective measures which reduce US systems-vulnerability, but also new legal tools and agreements on international sanctions, as well as the collaboration of other concerned governments. While we should use our military power only as a last resort and where lesser means are not available, there will be instances where the use of force is the only alternative available to eliminate the threat to critical civil or military infrastructure.

Closely related to the legal question is the political question of linkage. When clear linkage to a supporting State exists, we must publicize that relationship and respond with discrimination in a manner calculated both to eliminate the current threat while deterring the offending State from further destabilizing actions. The “center of gravity” in the offending State must always be that target or capability which most significantly undermines that State’s will to continue to destabilize our critical infrastructure. Since cyberterrorism is a lesser form of international conflict and is bound by its rules, lawful response is properly limited to those targets which do not enjoy civilian immunity. Military targets may be preferable for two other reasons. First, the selection of military targets, while our adversaries are attacking our civil infrastructure in violation of international law, should not raise concerns on the part of other States. Additionally, selection of military targets would refocus attention on the fact that cyberterrorism and techno-violence are, in fact, forms of armed conflict.

The thrust of this new strategy, outlined in PDDs 62 and 63, must be to reclaim the initiative lost while the United States pursued a reactive policy to incidents of information warfare which neither deterred cyber-terrorists nor encouraged successful response. The key to an effective, coordinated policy to address the threat posed by those willing to target our critical infrastructure is the commitment to hold those accountable responsible under the law of armed conflict. Full implementation of the two PDDs should lead to increased planning for protective and defensive measures to address this challenge to US national security, and, where deterrence fails, to respond in a manner which eliminates the threat, rather than treating each incident after the fact as a singular crisis provoked by international criminals. By treating cyber-terrorists as participants in international coercion where clear linkage can be tied to a State actor, the right of self-defense against their sponsor is triggered, and responding coercion (political, economic, or military) may be the only proportional response to the threat.

This pro-active strategy to the threat posed by attacks on our critical infrastructure embraces the use of protective, defensive, non-military, and military measures. It attempts, for the first time, to define acts designed to destabilize our eight most important infrastructure systems in terms of “aggression,” with the concomitant right of self-defense available as a lawful and effective response. The use of international law and, more specifically, the law of armed conflict, will not only complement the current criminal law approaches, but give pause to those who would target vital US interests.

---

## NOTES

1. See Bradley Graham, *US Studies New Threat: Cyber Attack*, WASHINGTON POST, May 24, 1998, at A-1. The author describes Operation Eligible Receiver, conducted by the NSA and other government agencies.

2. Speech of the Hon. Jamie Gorelick before the Corps of Cadets, US Air Force Academy, February 29, 1996.

3. See William Gertz, *Chinese Hackers Raid US Computers*, WASHINGTON TIMES, May 16, 1999 at C1, C8, for a troubling review of Chinese efforts to attack White House, State Department and other government computer systems.

4. Convention (II) with Respect to the Laws and Customs of War on Land, July 29, 1899, 1 AMERICAN JOURNAL OF INTERNATIONAL LAW (Supp.) 129 (1907); Convention (IV) Respecting the Laws and Customs of War on Land, Oct. 18, 1907, 2 AMERICAN JOURNAL OF INTERNATIONAL LAW (Supp.) 90 (1908), ADAM ROBERTS AND RICHARD GUELFF, DOCUMENTS ON THE LAWS OF WAR 59 (3rd ed. 2000); Protocol I Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, June 8, 1977, 16 INTERNATIONAL LEGAL MATERIALS 1391 (1977), ROBERTS AND GUELFF, *supra*, at 420. Most treaties relevant to the law of armed conflict are available on the International Committee of the Red Cross website at [www.icrc.org/ihl/](http://www.icrc.org/ihl/).

5. LAWRENCE T. GREENBERG, SEYMOUR E. GOODMAN, AND KEVIN J. SOO HOO, INFORMATION WARFARE AND INTERNATIONAL LAW 32 (1997).

6. UN CHARTER, art. 2, para. 4.

7. See LEAGUE OF NATIONS COVENANT, art. 12.

8. MYRES MCDUGAL AND FLORENTINO FELICIANO, LAW AND MINIMUM WORLD PUBLIC ORDER 142-143 (1961).

9. See Definition of Aggression, G.A. Res. 3314, 29 UN GAOR Supp. (No. 31) at 142, UN Doc. A/9631 (1974) [hereinafter 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, 25 UN GAOR Supp. (No. 28) at 121, UN Doc. A/8028 (1970) [hereinafter Declaration on Friendly Relations].

10. 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.

Declaration on Friendly Relations, *supra* note 9, at 122–23.

11. “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.” Robert Rosenstock, *The Declaration of Principles of International Law Concerning Friendly Nations: A Survey*, 65 AMERICAN JOURNAL OF INTERNATIONAL LAW 713, 715 (1971).

12. Definition of Aggression, *supra* note 9, at 142.

13. *Id.* at 143.

14. A fundamental purpose of the UN Charter is to “maintain international peace and security.” UN 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 9, at 144.

15. 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 US economic apparatus (banking system, Stock Exchange, etc.) such that a juggernaut was placed on US commercial activity.

16. 68 AMERICAN JOURNAL OF INTERNATIONAL LAW 720, 736 (1974) (Statement of Acting Secretary of State Dean Rusk).

17. UN CHARTER, art. 51.

18. 5 MARJORIE WHITEMAN, DIGEST OF INTERNATIONAL LAW § 25, at 971–72 (1965).

19. George Shultz, Low Intensity Warfare: The Challenge of Ambiguity, US Department of State Current Policy No. 783, at 3 (Jan. 1986).

20. UN CHARTER, art. 2, para. 4.

21. Myres McDougal, *The Soviet-Cuban Quarantine and Self-Defense*, 57 AMERICAN JOURNAL OF INTERNATIONAL LAW 597, 600 (1963).

22. MCDOUGAL AND FELICIANO, *supra* note 8, at 242.

23. See the Security Council’s discussion in 36 UN SCOR.(2285–2288 mtgs.), UN Docs. S/PV 2285–88 (1981).

24. G.A. Res. 53/70, UN GAOR, 53rd Sess., UN Doc. A/RES/53/70 (1998).

25. *Id.*

26. United States Explanation of Vote After the Vote, re: G.A. Res. 53/70 (1998), *reprinted in* W. GARY SHARP, SR., CYBERSPACE AND THE USE OF FORCE 189 (1999).

27. Joint Chiefs of Staff Peacetime Rules of Engagement for U.S. Forces (June 1986).

28. Chairman of the Joint Chiefs of Staff Instruction 3121.01, Standing Rules of Engagement for US Forces, Oct. 1, 1994, as amended Dec. 22, 1994. (The current version of the SROE was promulgated on Jan. 15, 2000, as CJCS Instruction 3121.01A.)

29. US NAVY, The Commander’s Handbook on the Law of Naval Operations (NWP 9), para. 8.1., (1987).

30. Classified document described by Robert C. McFarlane in “Terrorism and the Future of a Free Society,” (Speech delivered at the National Strategic Information Center, Defense Strategy Forum, Washington, D.C.: 25 March 1985). See discussion in James Terry, *An Appraisal of Lawful Military Response to State-Sponsored Terrorism*, NAVAL WAR COLLEGE REVIEW, May–June 1986, at 58.

31. Presidential Decision Directive 62, Combatting Terrorism, May 22, 1998. Richard C. Clarke, longtime senior National Security Council staff-member, was appointed as the first National Security Coordinator.

32. Presidential Decision Directive 63, Critical Infrastructure Protection, May 22, 1998. See SHARP, *supra* note 26, at 201–204, for a comprehensive review of the major elements of PDD 63 and the requirements imposed upon the various departments of government and the private sector under this directive.

33. *Id.* at 205–206.

34. See James Terry, *The Iranian Hostage Crisis: International Law and US Policy*, JAG JOURNAL 31-79 (Summer 1982).

35. ROBERT OPPENHEIM, INTERNATIONAL LAW 299 (8th ed. 1955).

36. Ian Brownlie, *The Use of Force in Self-Defense*, BRITISH YEARBOOK OF INTERNATIONAL LAW 183, 207 (1961).

37. Address by Secretary of State Kellogg before the American Society of International Law, April 28, 1928, PROCEEDINGS OF THE AMERICAN SOCIETY OF INTERNATIONAL LAW 141, 143 (1928).

38. George Shultz, Address before the Low Intensity Warfare Conference, National Defense University, Washington, D.C., Jan. 15, 1986.