TOWARD DETERRENCE IN THE CYBER DIMENSION

Report to the
President's Commission
on Critical Infrastructure Protection

1997

This report was prepared for the President's Commission on Critical Infrastructure Protection. The report represents the opinions and conclusions solely of its developers. The Commission has not made a judgment on, nor should the publication of this document be taken to represent an endorsement by the Commission for the content of the material contained herein.

Preface

While the Commission did not produce a recommendation to pursue a cyber-deterrence policy, we did investigate this concept and believe it has merit for further discussion—especially when technological developments yield the capability to identify attackers of any sort, and reply in kind. The discussion presented here helps to illuminate the issue for further consideration.

Acknowledgments

The Commission gratefully acknowledges the leadership and important contributions to this document by several individuals. Commissioners David V. Keyes, and Susan V. Simens provided important insights into understanding key policy aspects of terrorism, the cyber threats which the Commission examined, and Federal law enforcement responses to terrorism. Chief of Staff James H. Kurtz laid out the historical premises underlying the traditional nuclear deterrence of the past half-century, and showed how many of the same principles can be applied to a cyber deterrence strategy for the 21st century. Finally, Stephen T. York, Senior Analyst, provided important research and analytical support to this effort and distilling many complex issues into the essential elements of discussion.

Toward Deterrence in the Cyber Dimension

After World War II and in the early days of the Cold War, when the United States enjoyed a nuclear monopoly, our defense policy was one of Massive Retaliation. We publicly stated our intent to use nuclear weapons in the event of an attack by numerically superior Soviet forces against North Atlantic Treaty Organization (NATO) forces in Western Europe. This declaratory policy deterred Soviet aggression, but when the Soviet Union developed nuclear weapons of its own, and long-range bombers capable of delivering them against the continental United States, the policy of Massive Retaliation gave way to Mutual Assured Destruction.[1] We invested heavily in a system of overlapping radar systems to give us early warning of any Soviet "first strike" attempt to destroy our retaliatory capabilities. The North American Air Defense Command (NORAD) maintained constant surveillance against flight paths from the Soviet Union to Canada and the United States, and commanded interceptor forces whose mission was to defend against an attack by Soviet long-range bombers. When the Soviets developed Intercontinental Ballistic Missiles (ICBMs) and, later, Submarine-Launched Ballistic Missiles (SLBMs) able to reach targets in the United States, we developed overhead sensors—first manned high-altitude aircraft and then satellites—and ocean and other surveillance and sensor capabilities that enabled us to keep watch on Soviet missile sites and detect a launch. The early warning (EW) thus obtained provided sufficient time to launch our own missiles before Soviet ICBMs and SLBMs could take them out—ensuring the continued credibility of our deterrent policy of Mutual Assured Destruction.

In the cyber world, however, US leadership cannot count on any advance warning time to dissuade a potential adversary or take preemptive action to thwart a cyber attack. Nor is there currently any capability or policy that serves as a credible deterrent to potential attackers.

[1] "*US Defense Policies Since World War II*," AUSA Background Brief No. 70, Association of the US Army, March 1996.

Deterrence

The President's *National Security Strategy* says that:

> *Our ability to deter potential adversaries in peacetime rests on several factors, particularly our demonstrated will and ability to uphold our security commitments when they are challenged. We have earned this reputation through both our declaratory policy, which clearly communicates costs to potential adversaries, and the credibility of our conventional warfighting capability …*[2]

The National Security Strategy itself conveys a general US declaratory policy. It defines our ***vital interests*** as those that are of broad, overriding importance to the survival, safety and vitality of our nation. It declares that we will do whatever it takes to defend these interests, including—when necessary—using our military might unilaterally and decisively. Finally, the Strategy specifies that among these ***vital interests*** are the physical security of our territory and that of our allies, the safety of our citizens, and our economic well-being.[3] The ***physical*** security of our territory is a declared vital interest—one we would defend with military force if necessary. US declaratory policy is thus far silent concerning our ***cyber*** security.

On the other hand, the US has made public declarations concerning our own cyber capabilities. The Quadrennial Defense Review says that offensive actions to disrupt our adversary's access to information are part of US military capabilities, and that such capabilities will be increased in the future to ensure that the United States maintains information superiority during a conflict.[4] The report further states that Department of Defense (DoD) has directed a share of its planning and resourcing efforts in this area toward developing US information operation capabilities for use in ***peacetime engagement activities***, smaller-scale contingencies, and major theater wars.[5] DoD is evidently not alone in possessing the capability to conduct information operations or the willingness to employ that capability, as evidenced by recent newspaper coverage of Central Intelligence Agency operations:

> *Reflecting new threats that face US policymakers, major covert actions are now being aimed at disrupting terrorist plans, stopping narcotic shipments or fouling up financial statements of missile makers. … For instance, computer hacker technology has been used to disrupt international money transfers and other financial activities of Arab businessmen who support suspected terrorists.*[6]

---

[2] *A National Security Strategy for a New Century*, the White House, May 1997, page 8.
[3] Ibid., page 9.
[4] Ibid., page 51.
[5] *Report of the Quadrennial Defense Review*, Washington, DC, May 1997, page 50 – *emphasis added.*
[6] *"CIA Turns to Boutique Operations, Covert Action Against Terrorism, Drugs, Arms,"* Washington Post, September 14, 1997, page A6.

While sophisticated technological EW solutions are being pursued, there may be other actions which contribute to deterring cyber attacks against US infrastructures. One model might be the role of deterrence in dealing with another seemingly intractable problem: international terrorism. In the late 1970s and early 80s, the United States struggled to find an effective policy for combating terrorist attacks against Americans and American interests abroad. Murders of citizens, attacks on US embassies and officials, and hijackings of US air carriers were carried out on a regular basis in the full glare of international media attention. The responsible individuals, groups and even state sponsors often did not conceal their identities in the belief that the United States could do little, if anything, against them.

Confronted with this unacceptable situation, an aggressive interagency collaboration was undertaken to find solutions. First a number of steps were taken to reduce the vulnerability to terrorism of US citizens, companies and facilities abroad. Second, a number of credible and effective response options were developed. As vulnerabilities were successfully reduced and effective response options were implemented, their combined deterrent impact was evidenced by a dramatic change in the nature of international terrorism.

The three steps taken to reduce vulnerability to terrorism are presented below, along with thoughts on how they might be applied to the cyber world.

Step 1: Declare a Policy and Build International Consensus

From the very first international terrorist actions against US interests, the US has publicly, clearly and forcefully declared its policies concerning terrorism, those who engage in terrorism, and the groups or nations that sponsor terrorism. We then expended tremendous energy to build a broad international consensus against terrorism. Every appropriate international forum and organization was used for that purpose. International agreements were successfully concluded, the combined effect of which was to deny sanctuary to known terrorists and isolate their state sponsors as international pariahs.

While the US government as a whole has not yet framed a declaratory policy concerning cyber attacks and cyber attackers, public statements from individual government agencies avow US intent to pursue a peacetime program of offensive information operations. This apparent disconnect needs to be addressed. To deter cyber activities against the United States, the US government, not individual agencies, must declare its policy toward cyber intrusions, and then begin the work of forging an international consensus in support of that policy.

Denial of sanctuary is perhaps a greater challenge in the cyber world, where physical location and international borders present no impediment to a cyber attacker. Cyber investigators, on the other hand, do have physical borders to consider and are confronted by a confusing mosaic of time-consuming legal processes and structures and jurisdictional and pursuit issues. In some countries, cyber intrusions are categorized as petty crimes or not viewed as criminal activity at all. As a result of such legal complexities, certain foreign governments may have neither the authority to investigate intrusions nor the capability to locate and seize supporting evidence.

Even electronic "trap and trace" capabilities may be legally proscribed or not technically feasible. The result is that cyber attackers can enjoy actual or virtual safe havens—the latter because attacks looping through certain countries can be traced only as far those countries, but not beyond, because local authorities cannot or will not cooperate. As with international terrorism, an international consensus proscribing unacceptable cyber activities is necessary. The most recent National Security Strategy notes that "Placing terrorism at the top of the diplomatic agenda has increased international information sharing and law enforcement efforts." A similar high-priority effort is needed to shape the international environment in ways favorable to US interests and global cyber security.

Step 2: Harden Targets and Deny Access

Another aspect of early counterterrorism programs involved hardening potential targets and impeding or denying terrorist access to them. Through the Omnibus Diplomatic Security Act of 1994 and subsequent legislation, extensive improvements were made to the security of US embassies. Additional security measures were made available to official personnel abroad. Improvements were made, and still continue, in screening processes to prevent air piracy and enhance aviation security. These and similar actions had the cumulative result of making terrorism far harder, and much riskier for the terrorist or terrorists. Terrorists realized, too, that these new protective measures made it much likelier they would lose their protective anonymity.

The cyber equivalent of target hardening and denial involves the research and development investments discussed in the Commission's report, Critical Foundations. As with counterterrorism, however, target hardening and denial are ***processes***, not end states. One of the most important issues to overcome is the anonymity cyber attackers enjoy. When the cyber EW technology process begins in earnest, the sense of assured anonymity will begin to erode and the deterrent impact of the technology investment will begin even prior to its operational deployment.

Step 3: Share Information, Conduct Analysis, and Issue Warning Notices

Early in the counterterrorism policy evolution, a primary objective was to make potential targets more aware of terrorist risks and methods. To support this objective (among others), an improved government counterterrorism analytical process was put in place. Additionally, a new process was put in place for sharing government information with US companies, both domestically and abroad. These information-sharing channels were later expanded to include threat and warning information about potential international terrorism targets. The combined impact of these efforts was to substantially improve the counterterrorism awareness of potential government and non-government victims, enabling them to take appropriate steps to protect themselves from being victimized.

This process needs to be paralleled in the cyber dimension, and coupled with education and awareness efforts to enhance understanding of intrusion techniques, targets, and effective defenses.

In addition to the above terrorism vulnerability reduction measures, the interagency policy development process created five potential response options. The United States has declared and demonstrated its willingness to apply these options singly or in combination. In many respects, all five could be applicable to the cyber world.

The first four response options involve the use of more-or-less established capabilities. They are:

- aggressive diplomacy to isolate terrorists and their sponsors;
- use of economic sanctions against states that support terrorism;
- covert action against terrorists, terrorist groups or terrorist states; and
- military action, when appropriate.

The fifth response option, law enforcement action, was, at the time, a more revolutionary approach. For terrorist acts outside the United States, Congress created extraterritorial criminal jurisdiction for terrorist acts against Americans or American facilities abroad (such as 18 USC 1203 and 2331). In 1996, the Computer Fraud and Abuse Act (18 USC 1030) was amended by the National Information Infrastructure Protection Act of 1996. This statute expanded US jurisdiction concerning certain classes of cyber attacks, and includes extraterritorial jurisdiction.

The Computer Crime and Intellectual Property Section of the Department of Justice, in coordination with the Department of State, is presently engaged with the Council of Europe, the Organization of Economically Developed Countries (OECD), and "The Eight" to define mutual interests and options for closer legal collaboration involving computer intrusion matters across international borders. These and similar venues could be used to advance the deterrent impact that will result from more uniform international approaches to cyber attacks and the resultant reduction in actual or virtual safe haven options.

Until the necessary defensive technologies are in place, the primary deterrent to potential cyber attackers may be the certain knowledge that the US is committed to an aggressive policy of responding to cyber attacks. A national policy of cyber deterrence should formally define the penalties for nation states and other entities that attempt to deny or disrupt infrastructure services essential to our national security, economic competitiveness, and quality of life.

This policy of deterrence should consist of several components, including the development of a robust offensive information warfare capability to deliver an overwhelming response in kind; a defensive system for surveillance, assessment and warning of a cyber attack; and a physical strike capability to be used as a retaliatory mechanism, perhaps for those instances wherein an act of deliberate information warfare resulted in loss of life or significant property destruction. The foundations for these three components of a US cyber deterrence policy are already in place.

First, our possession of offensive information warfare activities was first demonstrated during DESERT STORM, when our military forces successfully took out computerized networks essential to Iraq. This success led to the recognition of our superiority in this area and the continued development and public promulgation of these capabilities should be a critical component of our deterrence policy.

The second component of deterrence should be a defensive system for surveillance, assessment, and warning of a cyber attack. Development of such a system is essential for providing near real-time notice of an attack in order to protect our own offensive capabilities for a retaliation in kind and to accurately identify the origin of the hostile attack on our infrastructures. However, as electronic communication transport systems allow data streams to flow easily without regard for geographical and political boundaries, technological means alone may not allow the origin of the attack to be identified with sufficient certainty to decide on a counterattack.

Tracing an attack may involve multiple nations and jurisdictions, most of which are not directly affected by the incident. Efforts should therefore be directed toward negotiating treaties to ensure mutual cooperation at critical times. Some nation states, whose foreign policies are inimical to US interests, would likely reject our requests for assistance in these matters. Therefore, our deterrence policy should clearly articulate that any perceived hesitation or refusal to assist tracing attempts may result in a determination that a particular entity is aiding and abetting an information warfare attack against our critical infrastructures, and that such a determination may result in a US counterstrike being targeted against such an entity for the purpose of mitigating the consequences of a contemporaneous or recently-concluded attack.

Finally, the third component of an effective cyber deterrence policy should be a declaration that any act of deliberate information warfare resulting in loss of life or significant destruction of property will be met with a devastating response. Our precision strike capabilities and our willingness to use them are well established.

A policy developed along the lines suggested here will clearly establish our intent to use any means at our disposal to protect the security of the nation—its people, territory and way of life.