Chapter LI
The U.S. Military Response to Cyber Warfare

Richard J. Kilroy, Jr.
Virginia Military Institute, USA

ABSTRACT

The United States military has taken a number of steps to confront the threat of cyber warfare. These include organizational, operational, and personnel changes by all the armed services, as well as the joint commands, which conduct operational warfare. Many of these changes began before the terrorist attacks of 9/11 as military planners recognized the vulnerabilities the nation faced to asymmetrical warfare conducted in cyberspace, as well as the military's dependency on key critical infrastructures within the United States that were vulnerable to cyber warfare. Although many changes have taken place, to include training new classes of military officers and enlisted specialists in career fields and military doctrine related to cyber warfare (both offensive and defensive), the military continues to remain vulnerable to an adversary's ability to control the informational battlefield. Thus, a key strategic goal of the U.S. military leadership is to achieve information superiority over its current and potential adversaries.

INTRODUCTION

In the mid-1990s, the U.S. military recognized a growing threat to its informational architecture as well as the nation's critical infrastructure from *cyber warfare*. Since Department of Defense (DoD) installations in the United States were dependent on civilian infrastructure for communications, transportation, energy, water, and the full range of logistical support, the DoD recognized that a threat to any of these critical systems would directly impact the military's ability to deploy forces overseas against foreign threats and actors. This chapter will address the U.S. military response to the threat of cyber warfare, to include organizational and doctrinal changes made to confront the threat, as well as cultural and career force changes that have impacted forces structures, resources, and the war-fighting capability of the armed forces.

In 1995, the chairman of the Joint Chiefs of Staff, Army Gen. John Shalikashvili, released an unclassified document, *Joint Vision 2010*, that laid out his strategic goals for the military for the next 25 years. The document identified four key operational concepts that the chairman viewed as essential for the ability of the

U.S. military to fight as a joint force in an uncertain future. "This vision of future warfighting embodies the improved intelligence and command and control available in the information age and goes on to develop four operational concepts: dominant maneuver, precision engagement, full dimensional protection, and focused logistics" (Shalikashvili, 1995, p. 1).

To achieve such operational success in any future battlefield, military planners realized that their ability to maneuver forces, engage adversaries, protect the force, and even deploy the force to any future conflict was completely dependent on a complex civilian infrastructure, which the DoD had little control over. Critical infrastructures, such as transportation networks, telecommunications, power generation, and even health care and financial resources, were outside of federal oversight when it came to assessing national security and the potential threats to those infrastructures. To make matters worse for military planners, the "operational environment" for these infrastructures was not a series of buildings or "hard sites" that could be secured with concertina wire and a guard force. Rather, these infrastructures were comprised of complex information systems, which presented a whole new set of challenges for security planners who were now faced with the difficult question of how to defend critical infrastructures "over here" in order to even begin to get military forces deployed "over there" for the next conflict.

Recognizing these new challenges, the DoD began a series of training exercises aimed at testing the vulnerabilities of our nation's critical infrastructures and the information systems on which they depended. The first operational-level exercise conducted in June 1997 was called Eligible Receiver. The exercise involved using National Security Agency (NSA) "hackers," operating as an adversary (red-team), to attack defense and other government information systems, while also conducting simulated attacks on civilian infrastructure (Robinson, 2002). The lessons learned from the exercise showed serious problems with defending critical information systems and infrastructures, on which the DoD (and the nation) depended, against cyber attacks by adversaries using asymmetrical means to defeat (or simply neutralize) our nation's military strength indirectly. The U.S. Atlantic (later Joint Forces) Command in Norfolk, VA, also ran an exercise labeled Evident Surprise, which continued to explore vulnerabilities to cyber warfare in DoD information systems. One example involved a simulated attack on the DoD's electronic medical records that track blood supplies.

If Evident Surprise and Eligible Receiver were not enough to convince defense planners that cyber warfare was a real threat to military operations, a series of incidents in early 1998 provided additional proof. Termed *Solar Sunrise,* an investigation into intrusions into DoD information systems, which appeared to be originating from a Middle Eastern country, coincided with operational planning for Dessert Fox, a series of military attacks against Iraq in February 1998. The cyber intrusions impacted multiple service components and DoD agencies; such that investigators believed they were deliberate attacks being perpetrated by a foreign government. Further criminal investigations later turned up two California teenagers being mentored by an Israeli man, Ehud Tannenbaum, as being behind the attacks (Robinson, 2002). Although no real security breeches of critical DoD information systems occurred, the incidents did further identify significant vulnerabilities, which, if exploited, could have had a significant impact on operational planning and execution utilizing the military's integrated command, control, communications, computers, and intelligence (C4I) architecture.

In December 1998, the DoD took the initiative to stand up an operational unit to specifically deal with the threat toward DoD information systems posed by cyber warfare. The Joint Task Force – Computer Network Defense (JTF-CND) was formed as a field operating agency, based in Arlington, VA, at the Defense Information Systems Agency (DISA). The JTF-CND would later move to operational control of U.S. Space Command (SPACECOM) in Colorado Springs, CO, as a result of changes to the DoD's Unified Command Plan which took effect on Oct. 1, 2000 (Verton, 1999). The JTF-CND originally focused only on the defensive aspects of what would be called