

CHAPTER 19  
**Cyber Terrorism: Menace or Myth?**  
*Irving Lachow*

CYBER TERRORISM is often portrayed as a major threat to the United States. Articles, books, and reports discussing the subject conjure images of infrastructure failures, massive economic losses, and even large-scale loss of life.<sup>1</sup> Fortunately, the hype surrounding this issue outpaces the magnitude of the risk. Terrorists use the Internet extensively, but not to launch massive cyber attacks. In fact, while there is clear evidence that terrorists have used the Internet to gather intelligence and coordinate efforts to launch physical attacks against various infrastructure targets, there has not been a single documented incidence of cyber terrorism against the U.S. Government.<sup>2</sup> Why is that? Is it just a matter of time until terrorists launch a massive cyber attack against the United States, or are current trends likely to continue? If terrorists are not using the Internet to attack us, what are they using it for? This chapter addresses these questions.

The chapter begins by providing a framework for assessing the risks of cyber terrorism. It uses this framework to develop a good understanding of the factors that terrorists must consider when deciding whether to pursue cyber-based attacks. It also facilitates a general assessment of the overall risks posed by cyber terrorists, today and in the next few years.

Terrorist use of the Internet is common, even though cyber terrorism is rare. The Internet provides an almost perfect tool for enabling the goals of many terrorist organizations. The second part of this chapter examines how terrorists are using the Internet to thrive in the modern world. The chapter closes with a series of recommendations for responding to these two aspects of the threat.<sup>3</sup>

***What is Cyber Terrorism?***

The Department of Defense (DOD) defines *terrorism* as “the calculated use of unlawful violence or threat of unlawful violence to inculcate fear, intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological.”<sup>4</sup> Definitions from the Federal Bureau of Investigation (FBI) and State Department are similarly worded. Thus, there is general agreement within the U.S. Government that terrorism is focused on obtaining desired political or social outcomes through the use of tactics that instill fear and horror in target populations. By extension, *cyber terrorism* can be defined as:

a computer based attack or threat of attack intended to intimidate or coerce governments or societies in pursuit of goals that are political, religious, or ideological. The attack should be sufficiently destructive or disruptive to generate fear comparable to that from physical acts of terrorism. Attacks that lead to death or bodily injury, extended power outages, plane crashes, water contamination, or major economic losses would be examples. . . . *Attacks that disrupt nonessential services or that are mainly a costly nuisance would not [be cyber terrorism].*<sup>5</sup>

Some experts have extended the definition of cyber terrorism to include physical attacks on information technology (IT) systems.<sup>6</sup> This author does not consider such attacks to be cyber terrorism. Cyber terrorism refers to the *means* used to carry out the attacks, not to the

nature of the *targets* of a “classical” terrorist attack. Otherwise, the term *cyber terrorism* loses all value, and analyses of cyber terror threats become diffuse and lacking in rigor. This leads to a larger point: one of the reasons that cyber terrorism is often perceived to be such a threat is that the term is frequently applied (or rather misapplied) to a wide range of activities. A typical example is in a *USA Today* article, “Cyberterror Impact, Defense Under Scrutiny,” which begins: “A terrorist threat is out there—and not just against physical infrastructure.”<sup>7</sup> However, a few paragraphs later, the article acknowledges that “Al-Qaeda doesn’t see cyber terrorism as achieving significant military goals.” Declaring that other groups and nations are looking at using cyber terrorism to damage the United States, it quotes a senior government official: “There are a large number of threats: hackers, cyber criminals, other countries.” Reading this article, it is not clear exactly what the term *cyber terrorism* refers to. It seems to say that hackers, criminals, and nation-states are engaging in cyber terrorism, while terrorist groups are not.

There are many other examples of this confusion in terminology. To cite just one more: an article on the Council on Foreign Relations Web site describes the cyber attacks conducted against Estonia in 2007 as a case of “cyber espionage;” however, the attacks were clearly focused on shutting down systems rather than stealing information (more on this later).<sup>8</sup>

In order to clarify terminology for this chapter, table 19–1 illustrates the similarities and differences between six types of cyber threats: cyber terrorism, hacktivism, hacking, cyber crime, cyber espionage, and state-level information warfare.

Table 19-1 Cyber Threats: Defining Terms

	<b>Motivation</b>	<b>Target</b>	<b>Method</b>
<b>Cyber Terror</b>	Political or social change	Innocent victims	Computer-based violence or destruction
<b>Hacktivism</b>	Political or social change	Decisionmakers or innocent victims	Protest via web page defacements or distributed denial of service (DDOS)
<b>Black Hat Hacking</b>	Ego, personal enmity	Individuals, companies, governments	Malware, viruses, worms, and hacking scripts
<b>Cyber Crime</b>	Economic gain	Individuals, companies	Malware for fraud, identity theft; DDOS for blackmail
<b>Cyber Espionage</b>	Economic and political gain	Individuals, companies, governments	Range of techniques to obtain information
<b>Information War</b>	Political or military gain	Infrastructures, information technology systems and data (private or public)	Range of techniques for attack or influence operations

*Hacktivism* is usually understood as the manipulation of digital information to promote a political ideology. In general, acts of hacktivism are aimed at leveraging use of code to have “effects similar to regular activism or civil disobedience.”<sup>9</sup> Unlike cyber terrorism, hacktivism is not focused on creating a sense of fear or horror. Hacktivists often target decisionmakers directly to express their dissatisfaction with various policies, whereas terrorists usually target innocent victims or third parties. For example, it is commonplace for “patriotic hackers” of one country to express their anger at foreign governments by launching cyber protests (which usually involve Web defacements and denial-of-service attacks). In several cases, national governments have

specifically asked such hackers to cease their activities for fear of escalating tensions with other countries.<sup>10</sup>

The term *hacking* generally refers to the activity of illegal computer trespassing.<sup>11</sup> Hacking is sometimes done to uncover weaknesses in computer systems or networks in order to improve them (often with permission from the owners of these targets). Such hacking is called “white hat” hacking and is not usually malicious. In contrast, “black hat” hacking refers to malicious exploitation of a target system. Although hacking techniques can be used for a variety of purposes (including hacktivism, cyber terror, or cyber crime), black hat hackers can be defined as those who exploit weaknesses in computer systems for personal gain. In some cases, that gain may be financial, in which case the activity would be classified as cyber crime; however, many hackers are motivated by the prospect of aggrandizement, by the challenge of breaking into high-value systems, or by personal vendettas against a specific target. According to one computer security expert: “The most common motivation [for hacking] is ego-gratification and it drives all the script-kiddies to deface Web sites—digitally spray-painting their name on the Internet and brag to their friends. Usually, the sites they hit are pretty easy targets and the defacement is a yawn to the rest of us. A more compelling motivation is retaliation.”<sup>12</sup>

There is no single, widely accepted definition of cyber crime. However, the majority of definitions focus on the use of computers or networks to facilitate criminal acts such as spamming, fraud, child pornography, and data theft. The methods used for cyber crime can sometimes be the same as those used for hacktivism or hacking; what distinguishes these from each other is the motivation of the perpetrator. In the case of cyber crime, the goal is economic gain, not political change, ego gratification, or civil disobedience.

*Cyber espionage* can be defined as the use of information technology systems and networks to gather information about an organization or a society that is considered secret or confidential without the permission of the holder of the information.<sup>13</sup> Cyber espionage is conducted by a wide range of actors, including individuals, groups, companies, and nation-states. Although cyber espionage is often cloaked in secrecy, the world was given a glimpse at the magnitude of the problem when it was revealed in late 2007 that the British intelligence agency MI5 had sent a letter to over 300 senior executives in industry warning them about Chinese cyber espionage activities. In the letter, the British government “openly accused China of carrying out state-sponsored espionage against vital parts of the Britain’s economy, including computer systems of major banks and financial services firms.”<sup>14</sup> The FBI has also identified Chinese espionage activities as being a major threat to U.S. national security.<sup>15</sup>

In this chapter, the term *information war* encompasses two concepts that were defined by John Arquilla and David Ronfeldt in 1997: *netwar* and *cyberwar*. *Netwar* refers to the information-related conflict at a grand level between nations or societies. It means trying to disrupt, damage, or modify what a target population “knows” or thinks it knows about itself and the world around it. . . . In other words, *netwar* represents a new entry on the spectrum of conflict that spans economic, political, and social as well as military forms of “war.”<sup>16</sup>

The term *cyberwar* is more focused on the military aspects of competition: *Cyberwar* refers to conducting, and preparing to conduct, military operations according to information-related principles. It means disrupting if not destroying the information and communication systems, broadly defined to include even military culture, on which an adversary relies in order to “know” itself.<sup>17</sup>

Thus, the term *information war* can be understood to refer to cyber conflict at the nation-state level involving either direct military confrontation or indirect competition via disruption and deception. Many nations across the globe are developing doctrine for information warfare, and there are indications that activities of this kind are already occurring. For example, a recent report notes that sophisticated attacks against several Western nations have originated in China.<sup>18</sup> While this does not prove that the Chinese government is conducting information warfare, the circumstantial evidence is fairly strong.

The distinctions among these six threats are somewhat artificial. The boundaries between cyber terrorism and hacktivism, or between cyber crime and cyber espionage, may be blurry. Similarly, single actors can engage in multiple activities: terrorist groups can also commit cyber crime or hacktivism, criminal groups can conduct cyber terror or cyber espionage, and nation-states can undertake cyber espionage or information warfare. However, the distinctions are still useful for analytic purposes. For example, the recent cyber attack against Estonia has been called everything from a “cyberwar” to a “cyber terror attack.” Using our framework to examine a series of after-action reports about the incident, we see that the attacks against Estonia were clearly an instance of hacktivism. Hacktivism directed at a nation-state is not new; Chinese hacktivists have launched attacks against both the United States and Taiwan several times over the last 20 years in response to a number of incidents, such as the accidental

U.S. bombing of the Chinese embassy in Yugoslavia in 1999. Palestinian and Israeli hackers have engaged in a mutual battle of nationalistic hacktivism for years. What makes the Estonian case interesting is that the consequences of the attack were more serious than in previous instances, that botnets were used for the attack (thus tying hacktivism to cyber crime), and that servers from the Russian government were implicated in the attack (although they were likely just unwitting nodes in the botnets).<sup>19</sup> To paint the Estonian cyber attacks as the first instance of either state-sponsored information war or cyber terror is misleading and unhelpful.

By placing a cyber attack in the proper context, it becomes easier to assess the risks it poses and to select appropriate policies for responding. This is especially important for cyber terrorism, which is usually mischaracterized. Cyber terrorism is quite distinct from hacking, cyber crime, hacktivism, or cyber espionage, all of which are exceedingly common and some of which pose serious threats to U.S. national security.

### ***Assessing the Risks of Cyber Terrorism***

Many assessments of cyber terrorism focus strictly on the threat that such attacks pose to the United States. However, to truly understand the seriousness of the issue, one needs to examine the vulnerabilities that such threats can exploit and the consequences that such attacks would have if they were successful. To perform this comprehensive assessment, we utilize a risk management framework developed by the RAND Corporation.<sup>20</sup> The RAND framework defines the risk of terrorism in terms of three variables: threat, vulnerability, and consequence.

*Threat* (T) is the probability that a specific target is attacked in a specific way during a specified time period. In other words, Threat = P (attack occurs).

*Vulnerability* (V) is the probability that damage (which may involve fatalities, injuries, property damage, or other consequences) occurs given a specific attack type, at a specific time, on a given target. Thus, Vulnerability = P (attack results in damage/attack occurs).

*Consequence* (C) is the expected magnitude of damage given that a specific attack type,

at a specific time, on a given target, results in damage. In mathematical terms, Consequence = E (damage/attack occurs and results in damage). The overall risk is a product of the three terms defined above. In other words:

$$\text{Risk (R)} = T * V * C.$$

Or, to put things in terms of probabilities:

$$\text{Risk (R)} = P (\text{attack occurs})$$

\*P (attack results in damage/attack occurs)

\*E (damage/attack occurs and results in damage).

### ***Threat***

To determine the level of threat posed by cyber terrorism, one has to examine the resources, capabilities, structure, and motivations of a given terrorist group in terms of a specific type of attack. To that end, it is useful to group cyber terrorism threats in three broad categories: simple unstructured (simple), advanced structured (advanced), and complex coordinated (complex).<sup>21</sup> Each of these threat levels is associated with a given set of capabilities, resources, structures, and motivations. Table 19–2 summarizes the characteristics of these levels.

The following discussion explores what it takes for terrorists to operate at each of the three levels described in table 19–2. We then assess where terror groups are operating today and where they may be headed in the future.

*Simple threats.* Carrying out cyber attacks of any kind requires two kinds of capabilities: analytical and technical.<sup>22</sup> Analytical capability refers to the ability to analyze a potential target in order to identify its critical nodes and vulnerabilities (and potentially its connections to other targets). Technical capability refers to knowledge of computer software and hardware, networks, and other relevant technologies.

Simple cyber attacks can be carried out by anyone who has basic computer skills and rudimentary analytical capabilities. No special resources or organizational structures are needed; a single individual could download hacker tools from a Web site, pick a target, and launch an attack. Such attacks are generally focused on a specific target. Web defacements are a good example of this type of attack. Simple attacks are extremely common on the Internet today; anyone willing to devote a few hours of time researching hacker tools can perform such attacks.

*Advanced threats.* Advanced cyber attacks differ from simple ones in their sophistication. At this threat level, the attacker has the ability to write programs or to modify those of others, and also has a working knowledge of networks, operating systems, and possibly even defensive techniques. For example, such an attacker often understands the functioning of common firewalls and intrusion detection systems. This allows the attacker to develop more sophisticated attacks than those found in the previous category. According to a Naval Postgraduate School study, people at this level must have technical capabilities equivalent to a Microsoft Certified Systems Engineer.<sup>23</sup> To reach this threat level, a terrorist group would need to recruit or hire at least one person with a solid education in computer science or a great deal of experience working with computer systems. In addition to stronger technical skills, advanced threats require more sophisticated analysis and planning than simple attacks. Terrorists at this level would need to analyze target networks and systems to find vulnerabilities or circumvent

defenses. They might also want to model the possible effect of a successful cyber attack to determine what would happen in different scenarios. For both of these reasons, groups wishing to operate at this level would likely need to create a simple testbed to allow the attackers to rehearse their attack plans or to experiment with different scripts.

While advanced threats are clearly more sophisticated than simple ones and can cause a great deal of economic damage, they still fall short of the kind of massive cyber attacks often portrayed in the press. Frequently developed and launched by an individual or perhaps a small team, they generally target known vulnerabilities and are aimed at a single type of system or network. Thus, advanced attacks would likely be used against a single organization or against a number of organizations that use similar technologies. Multiple attacks, if they occur, would likely occur in sequence rather than simultaneously. An example of an advanced cyber attack was the Nimda computer virus, which caused billions of dollars of damage worldwide.<sup>24</sup>

*Complex threats.* Complex attacks are significantly more difficult to accomplish than the previous two attack types, but they pose by far the biggest threat to U.S. assets. In contrast to the previous two threat levels, complex attacks cannot be carried out by a single hacker or even a small team of computer experts. These attacks require a team of individuals (or perhaps multiple teams) with expertise in a number of technical areas, including but not limited to: networks, operating systems, programming languages, infrastructure topologies and control systems (for example, supervisory control and data acquisition systems), intelligence-gathering and analysis, and planning. Obtaining the depth and variety of technical expertise alone would pose a daunting challenge for most terrorist groups.

Because attacks of this nature require the coordination of multiple attack vectors, a sophisticated testbed would be needed to test attack methods and rehearse the attack itself.<sup>25</sup> The testbed alone would be expensive and would require dedicated manpower for upkeep and maintenance. In addition, the planning and coordination skills required to pull off a complex attack are not trivial. A terrorist group would need an estimated 6 to 10 years to develop such a capability internally.<sup>26</sup>

Table 19-2 Cyber Threat Levels

	<b>Simple</b>	<b>Advanced</b>	<b>Complex</b>
<b>Target Scope</b>	Single system or net	Multiple systems or nets	Multiple networks
<b>Target Analysis</b>	None	Elementary	Detailed
<b>Effects</b>	Unfocused	Focused	Scalable
<b>Resources Required</b>	One or more computer-literate people	One or more sophisticated programmers; simple testbed	Several expert programmers, analysts, and planners; sophisticated testbed
<b>Structures</b>	None	None	Synchronized teams
<b>Potential Use</b>	Harassment	Tactical attacks	Strategic attacks

*Source:* This table is based on material found in Bill Nelson et al., *Cyberterror: Prospects and Implications* (Monterey, CA: Center for the Study of Terrorism and Irregular Warfare, 1999). A similar table can be found in Joseph F. Gustin, *Cyber Terrorism: A Guide for Managers* (Lilburn, GA: Fairmont Press, 2004).

## *Vulnerability*

We have examined the ability of terrorist groups to launch attacks against different types of targets. To assess the risks facing the United States from such attacks, we must determine the likelihood that a given attack would actually cause damage. This depends on two key variables: the characteristics of a specific system or network, and the range of countermeasures employed to protect that system or network. Because most organizations use a variety of computer systems and networks, a large number of characteristics must be examined to assess the vulnerability of an organization's cyber assets. A partial list of key technical factors includes the operating systems, all user applications, and network architectures and configurations.

Every computer technology has inherent vulnerabilities that could be exploited. For this reason, all security-conscious enterprises employ a range of countermeasures that seek to mitigate these vulnerabilities. Countermeasures can be technical, process-oriented, or people-oriented. Typical technical counter-measures include firewalls, intrusion detection systems, encryption, hardware tokens, and biometrics. Process-oriented countermeasures focus on policies and procedures, such as access control policies, authentication procedures, and configuration management practices. People-oriented countermeasures focus on minimizing vulnerabilities associated with human behavior, the single biggest risk in any organization. Countermeasures of this type might include background checks on employees, training requirements, physical barriers, and the use of monitoring software.

It is evident that one cannot assess the vulnerability of a given target to a specific attack without delving into the details of both the attack and the target. However, we can make some general statements about the ability of different types of attackers to exploit the vulnerabilities inherent in different types of targets. Simple threats could take advantage of well-publicized vulnerabilities found in standard operating systems (for example, Windows Vista), applications (such as Internet Explorer), and networks (for example, wireless standards such as 802.11g). Many enterprises do not spend the time and money needed to block all such vulnerabilities, so it is possible that a simple attack could succeed against some organizations. However, organizations that are strongly focused on security will be much less vulnerable to these simple types of attacks.

While advanced threats can take advantage of well-publicized vulnerabilities, they might also use their more extensive knowledge to find less well known vulnerabilities in a given system. In fact, the real danger with these threats is that they might find and exploit a weakness quietly, without fanfare or bragging on hacker Web sites. Advanced attackers might be able to find vulnerabilities in applications and networks that affect multiple organizations, but they are limited in their ability to exploit those vulnerabilities in a coordinated and systematic manner. They usually target one organization or system at a time. An example of this type of attack is the Nimda virus, a worm designed to exploit vulnerabilities found in Windows IIS Web servers. If a given Web server was not properly patched, then the worm infected the local files of that server as well as network drives connected to it, created copies of itself, and emailed those copies to other servers and clients. While the Nimda virus spread extremely quickly throughout the world and caused a fair amount of financial damage, it was designed to exploit a single vulnerability, and it spread sequentially from machine to machine.

Complex threats can identify and exploit vulnerabilities in multiple organizations simultaneously. Like advanced threats, these experts can find vulnerabilities that are not well

known and exploit them to gain entry into networks and computer systems. By coordinating their efforts across multiple networks or systems, they could leverage vulnerabilities found in the connections and dependencies between organizations. This could cause more damage, as ripple effects spread the attack throughout the network of targeted organizations, such as those comprising the electric power grid.

The challenge of actually exploiting different vulnerabilities across multiple organizations is tremendous. In order to launch a well-coordinated complex attack, an attacker would need a team of experts to analyze the network and system vulnerabilities of each potential target and then model how those targets are related in order to develop a good idea of what would happen when the attacks were launched. Of course, attackers could choose simply to launch a series of different scripts against different vulnerabilities and hope that the results would be to their liking. However, such attacks would fall under the advanced category and are more characteristic of individual hackers than well-organized terrorist groups, which would generally prefer to plan a major attack meticulously to maximize the chances of success.

The discussion so far has focused on vulnerabilities inherent in the system being attacked, but one must also consider the range of countermeasures that have been or could be implemented in response to an attack. For example, if an organization that is a target of a distributed denial-of-service (DDOS) attack can rapidly ramp up its bandwidth dramatically, the attack could fail. A whole range of technologies and processes in use today could, if implemented in a timely and proper manner, prevent many of the most common network attacks. That being said, there is no question that the attacker has the advantage against the defender when it comes to information security. Attackers (as a whole) outnumber defenders by a large margin, they do a better job of sharing information on successful attack strategies than defenders do with defense strategies, and they only need to succeed a small fraction of the time to achieve their goals. This is one reason why having a defense-in-depth strategy and a good recovery capability is so important for targeted organizations—topics that we will address again later in this chapter.

In summary, simple attacks exploit known vulnerabilities. Examples include DDOS attacks and downloadable scripts that can be launched by anyone. Advanced attacks can identify new vulnerabilities but are limited in how they can exploit them due to constraints in knowledge and resources. Examples include new viruses and zero-day attacks (exploits of vulnerabilities that take place the same day as knowledge of the vulnerability becomes available) of applications and operating systems. Complex attacks can identify and exploit vulnerabilities across multiple networks, systems, and organizations. A hypothetical example would be an attack against multiple infrastructure targets (logistics, communications, transportation) in the United States to hinder military deployments.

The likelihood of a given attack being successful depends on the nature of attack, the nature of the system being attacked, and the countermeasures (if any) that have been put in place to prevent such attacks from succeeding. This game of cat-and-mouse is highly dynamic because attackers and defenders are constantly developing new techniques and technologies to defeat each other.

### *Consequences*

To assess the consequences of a specific attack against a given target, one must analyze how the system fails (does it degrade gradually or dramatically?), the response processes and

procedures that are in place (how quickly can system administrators patch the exploited vulnerability and get the system working normally?), the continuity of operations measures or backup alternatives that may exist (if a secondary site backs up the targeted system continuously, the impact of the attack might be minimal even though it was completely successful in bringing down the targeted application or network), and the resilience of the affected population.

If an attack is successful and damage occurs, one needs to examine two issues: the magnitude of damage and the type of damage. It is fairly obvious why the scale of damage resulting from an attack must be determined, but why is the type of damage important? The answer to this question goes to the heart of the debate about why cyber terrorism has not occurred. Terrorists seek to achieve political, social, or religious goals through the use of violence that instills a sense of fear and horror. To that end, terrorist attacks tend to be extremely violent, bloody, and photogenic. They want to hurt or kill their victims in a way that disturbs as many people as possible and is seen by as many people as possible. It is obvious that explosives can achieve these goals. The question is: Can cyber attacks do so as well? In the case of both simple and advanced attacks, the answer is probably no.

History shows that the majority of cyber attacks, even viruses that cause billions of dollars of damage to an economy, are not going to cause the levels of fear and/or horror desired by most terrorists. Even the temporary disablement of a component of a critical infrastructure may not cause the desired emotions— such disruptions occur rather frequently due to human error and natural disasters, and people generally do not panic. On the other hand, the U.S. populace appears to have an irrational fear of terrorism (based on actual versus perceived risks), and thus it is possible that a cyber terror attack, if sufficiently newsworthy, could create a sense of fear.<sup>27</sup> In addition, a complex attack causing serious damage to the U.S. economy would likely engender a genuine feeling of fear and panic in the population.<sup>28</sup>

### ***Overall Assessment of Current Cyber Terror Risks***

It is difficult to assess with certainty the risks posed by cyber terrorism. However, there is strong circumstantial evidence pointing to the conclusion that terrorist groups are limited to launching simple cyber attacks and exploiting existing vulnerabilities. For example, a recent assessment of terrorist capabilities to launch cyber attacks found the following:

Any cyber attacks originating with terrorists or cyber jihadists in the near future are likely to be conducted either to raise money (e.g., via credit card theft) or to cause damage comparable to that which takes place daily from Web defacements, viruses and worms, and denial-of-service attacks. While the impact of these attacks can be serious, they are generally not regarded as acts of terrorism. Terrorists have not yet demonstrated that they have the knowledge and skills to conduct highly damaging attacks against critical infrastructures... their capability is at the lowest level, namely that required to carry out simple-unstructured attacks.<sup>29</sup>

Another key indicator of the limited cyber knowledge and skills found in jihadist terrorist groups was their heavy reliance on a single individual who had a moderate level of ability in this area: Irhabi 007 (real name: Younis Tsouli). This 22-year-old living in London became “the top jihadi expert on all things Internet-related” after 9/11.<sup>30</sup> Despite this ominous

sounding label, Irhabi's skills were quite mundane by hacker standards: he was able to hack Web sites and servers using standard toolkits found on the Internet. More importantly, Irhabi spent much of his time showing fellow jihadists how to perform such simple tasks as posting videos to Web sites and joining anonymous chat rooms. He also provided tutorials on the fundamentals of hacking Web sites to launch basic denial-of-service attacks.<sup>31</sup> The fact that he was functioning as *the* Internet expert for a number of major terrorist and insurgent groups until his arrest in 2005 implies that these groups had limited education and expertise in computer attack methods and practices. While Irhabi's tutorials have almost certainly raised the overall cyber capabilities of terrorists, which is worrisome, there is little evidence that these groups have progressed beyond the simple attack category.

This tentative conclusion is further bolstered by an analysis of terrorist activities and cyber attacks from 1996 to 2003.<sup>32</sup> The data in table 19–3 show three things. First, cyber attacks were extremely common.<sup>33</sup> Second, terrorists were quite active; they conducted an average of over 200 attacks per year. And third, the fact that there were no known cases of cyber terrorism during a period in which terrorists were quite active and hundreds of thousands of cyber attacks were occurring suggests that terrorists either are not trying to conduct cyber attacks or are trying and failing.

While it is possible that a small number of cyber terror attacks did happen and were simply not reported, the overall trend is clear: terrorists were not focused on conducting cyber attacks. Similar patterns hold true for 2003 through 2007. For example, it was reported early in 2008 that “every day, the Defense Department detects three million unauthorized probes of its computer networks; the State Department fends off two million.”<sup>34</sup> In 2006, the State Department cataloged 14,352 terrorist incidents around the world, none of which were classified as cyber terrorism.<sup>35</sup> Both hackers and terrorists are keeping quite busy, but their activities are not intersecting in any meaningful way. Why?

It is not possible to provide a definitive answer to this question, but a reasonable explanation can be pieced together. First, it appears that terrorist groups in general do not have the expertise to conduct advanced or complex cyber attacks. This means that terrorists are currently limited to exploiting the same basic vulnerabilities that are constantly being targeted by thousands of hackers around the world. While such attacks can work—they succeed all the time against poorly defended systems—it does mean that cyber attacks conducted by terrorists would have roughly the same impact as techniques used by ordinary hackers, hacktivists, and cyber criminals. To put things in context, DOD alone faced 80,000 intrusion attempts in fiscal year 2007. The presence of a few simple cyber attacks from terrorist groups would be lost in the sea of cyber attacks, some of them quite serious, already faced by DOD.

A similar story holds true for the private sector. For example, in 2006, the Department of Homeland Security warned U.S. financial services companies about “an al Qaeda call for a cyber attack against online stock trading and banking Web sites.”<sup>36</sup> Did the financial community respond with alarm and fear? Hardly. The financial sector's reaction was “muted, with markets showing little or no reaction.”<sup>37</sup> The threat was simply not viewed as being worthy of panic. In the words of one executive, “I'm not saying that there aren't precautions to be taken, but I just can't fathom how there would be serious havoc.”<sup>38</sup> Given the constant stream of cyber attacks that the financial sector faces on a daily basis, and the lack of sophistication found in terrorist hacking circles, this executive's assessment should not be surprising. It also turned out to be accurate: either no attacks occurred or they occurred but failed to work, because the financial companies operated as usual during the period in question.

In comparison to cyber terrorism, using physical means to create terror is fairly easy to do and is quite effective.<sup>39</sup> Put in these terms, it is not surprising that terrorists prefer to inflict damage with physical means and then use the Internet to magnify the results of their handiwork.<sup>40</sup> In fact, al Qaeda's own training manual makes the point that explosives are the preferred weapons of terrorists because "explosives strike the enemy with sheer terror and fright."<sup>41</sup> They also create carnage that is highly photogenic and inspires strong emotions, horrifying victims and inspiring allies and supporters. Indeed, despite its sophisticated planning and analytic capabilities, all of al Qaeda's operations to date have focused on high explosives; what have changed are the delivery mechanisms and the targets.

From a terrorist perspective, cyber attacks appear much less useful than physical attacks: they do not fill potential victims with terror, they are not photogenic, and they are not perceived by most people as highly emotional events. While it is possible that a complex attack on a critical infrastructure would create some of these desired effects, including a sense of panic or a loss of public confidence, terrorists appear to be incapable of launching such attacks in the near future. Faced with a choice between conducting cyber attacks that would be viewed mostly as a nuisance or using physical violence to create dramatic and traumatic events, terrorists have been choosing the latter. This choice is not surprising given our assessment earlier in this chapter. Other security experts have reached similar conclusions:

Cyber terrorism has grabbed the headlines recently, but most of that is overblown...We know what terrorism is. It's someone blowing himself up in a crowded restaurant or flying an airplane into a skyscraper. It's not infecting computers with viruses, disabling the Internet so people can't get their e-mail for a few hours, or shutting down a pager network for a day. That causes annoyance and irritation, not terror...Stories of terrorists controlling the power grid, or opening dams, or taking over the air traffic control network and colliding airplanes, are unrealistic scare stories. This kind of thing is surprisingly hard to do remotely. Insiders might have an easier time of it, but even then they can do more damage in person than over a computer network.<sup>42</sup>

### *Assessment of Future Cyber Terror Risks*

Is the risk of cyber terrorism likely to change in the future? In the spirit of policy analysts everywhere, this author must answer: "It depends." There are several factors at play—some of which favor the prospects for cyber terrorism and some of which oppose them.

*Threat.* One of the key considerations that might push terrorists toward a greater use of cyber attacks is having the ability to launch either a complex cyber attack or a series of sustained and well-targeted advanced attacks. In order to achieve such capabilities, terrorist groups would have to obtain the services of several highly educated or experienced computer scientists, engineers, or self-taught hackers. There are two options for getting there: insourcing or outsourcing. The former option would require terrorist groups either to recruit experts or to grow them internally through education and training. Historically, terrorist groups have had trouble doing either. One trend that works in their favor is the growth of computer literacy across the world. As computer know-how spreads, the chances that terrorist groups will be able to recruit people with strong computer skills (or induce potential recruits to obtain such skills) will likely increase over time. The fact that the jihadist movements are attracting to their cause well-educated young men in Europe further increases these odds.<sup>43</sup>

Terrorists have a second option: they could choose to obtain computer expertise through outsourcing. The main benefit of this approach is that it would allow the groups to access needed knowledge quickly and relatively cheaply. On the other hand, there are numerous risks associated with outsourcing cyber attacks to experts outside of a terrorist group. For example, one avenue to pursue would be to hire people from the hacking community. Some hackers are quite skilled and could help terrorist groups launch an advanced attack. However, hackers and terrorists often have different personalities, skill sets, and group cultures.<sup>44</sup> By going outside of their group, terrorists increase the risk of being caught because many hackers like to brag about their exploits.

Table 19-3. Number of Cyber and Terrorist Attacks, 1996-2003

Type of Incident	Number of Occurrences
Computer security attack	217,394
Conventional terrorist attack	1,813
Cyber terrorist attack	0

*Source:* James Lewis, “Cyber Terror: Missing in Action,” *Knowledge, Technology, and Policy* 16, no. 2 (Summer 2003).

Another approach for terrorist groups looking for computer skills would be to hire criminal organizations for assistance with cyber attacks. This strategy is probably less risky than working with hackers, and it has the added benefit of the apparent willingness of some cyber criminals to work with any paying customer. Criminal groups might also be willing to launch attacks for terrorist organizations in order to bolster their reputations. Cyber criminals could provide terrorists with fairly sophisticated capabilities for delivering cyber attacks. For example, many criminal organizations have created large botnets in order to perform (or threaten to launch) DDOS attacks. In addition, cyber criminals are constantly developing malicious code attacks that can take over a target system in order to steal valuable information that the criminals can use or sell. For example, according to one IT research company, “Phishing attacks are becoming more surreptitious and are often designed to drop malware that steals user credentials and sensitive information from consumer desktops.”<sup>45</sup>

The downside of this strategy is that cyber criminals are in the business of making money, not taking down national infrastructures. In fact, these groups rely heavily on several U.S. infrastructures, such as telecommunications and financial services, to conduct their operations. While some of their capabilities, such as botnets and malicious code, could be used by terrorists to attack critical systems, these capabilities alone are unlikely to cause large-scale damage of any lasting impact. Launching a complex attack requires detailed analysis, planning, and rehearsal and, as several studies have indicated, it would take a dedicated and well-financed team several years of effort to prepare a truly serious strategic attack on U.S. infrastructures. Criminal groups are simply not in that business. Their capabilities might allow terrorists to launch advanced attacks against companies or countries—and such attacks are certainly worrisome—but companies and countries already face such threats on a daily basis. It is not clear how much benefit terrorists would gain by using such attacks against their desired targets.

A final avenue for terrorist groups to bolster their attack capabilities is to obtain state sponsorship. There is little question that nation-states have the potential to pose the most

serious threat to U.S. national security. Many nations have the resources, personnel, and motives to develop the ability to launch complex cyber attacks against other countries. The key question is: Would such nations choose to aid and abet terrorist groups, either directly or indirectly, in obtaining the capacity to launch cyber attacks that could truly cripple another nation? There are numerous factors (some leading to benefits and others to risks) that nations must weigh when deciding what relationship to have with terrorist groups. At present, it appears that the nations with the most advanced cyber capabilities are unlikely to support terrorist groups directly, while nations that have a history of supporting terrorist groups are more limited in their cyber capabilities. However, a deeper analysis is required to assess the possible future risks of state-sponsored cyber terrorism.

*Vulnerabilities and consequences.* One trend that increases the likelihood of cyber terrorism is growing reliance of critical infrastructures on commercial-off-the-shelf software and the Internet—both of which increase the number of vulnerabilities that can be exploited. A related trend is the growing interconnectedness of organizations (both private and public) via the Internet. This connectivity, while beneficial for economic efficiency and productivity, can create points of vulnerability that, if properly targeted and attacked, could cause real economic, physical, or psychological harm to U.S. citizens.<sup>46</sup> In addition, the tight coupling between different infrastructures and organizations might lead to a “ripple effect” that magnifies the consequences of a particular attack. This ripple effect was evident in both Hurricane Katrina and the cyber attacks against Estonia in 2007.

On the other hand, the growing complexity and connectedness of infrastructure targets make them harder to target and take down. The kinds of networks that terrorists would need to attack (usually referred to as scale-free networks) are robust against random failures but vulnerable to failures in key nodes.<sup>47</sup> The trick is to know which nodes to attack. In some networks, this is an extremely difficult thing to figure out due to the sheer complexity of the system. In other kinds of networks, identifying such nodes can be straightforward, but as society moves toward greater complexity and connectedness, identifying these nodes may also become difficult. This, in turn, would make the system as a whole more robust against random (or badly aimed) attacks. Then again, the growing availability of Internet-based information and of sophisticated software tools that can be used for network analysis may counteract the growing complexity of infrastructure networks. It is hard to predict which trend will come out on top.

*Summary.* There are strong reasons why cyber attacks have not been the weapons of choice for terrorists. Many of those reasons will hold in the future, but there are some trends that may make cyber terrorism both more attractive and feasible in the future. Dorothy Denning has identified five key indicators of cyber terror activity: computer network attack incidents; cyber weapons acquisition, development, and training; official statements; formal education in IT; and general experience in cyberspace.<sup>48</sup> Her analysis of these indicators found little evidence that terrorists have developed comprehensive and significant capabilities for cyber attacks against the United States. What is more surprising is that her analysis showed that terrorists made little progress in this area in the 5 years after 9/11. This is a critical finding because if terrorists were serious about exploiting the Internet for attacks (rather than for operational effectiveness or influence operations), one would have expected to see signs of that during a period that has seen an explosion in the number of terrorist groups, a rise in anti-American sentiment internationally, and a tremendous increase in Internet connectivity across the globe. One could legitimately ask of cyber terrorism: If not now, when?

Of course, one must be careful in extrapolating too much from an analysis of a 5-year

window. Denning's analysis *has* shown the terrorists are growing more interested in cyber attacks, if only for fund-raising and low-level attacks. Cyber terrorism could become a more serious risk at some point in the future.

### ***Terrorist Use of the Internet***

Terrorists are using the Internet to harm U.S. national security, but not by attacking infrastructure or military assets directly. Instead, terrorists are using the Internet to improve their operational effectiveness while simultaneously undermining U.S. military and diplomatic efforts to win the war of ideas. There is little doubt that they are doing both things well. The Internet enables terrorist groups to operate either as highly decentralized franchises or as freelancers. Much like information-age businesses, these groups use the Internet to create a brand image, to market themselves, to recruit followers, to raise capital, to identify partners and suppliers, to provide training materials, and even to manage operations. As a result, these groups have become more numerous, agile, and well coordinated, which makes them harder to stop.<sup>49</sup> Further, these groups have become experts at using the Internet to manipulate both public opinion and media coverage in ways that undermine U.S. interests. In short, rather than attacking the Internet, terrorists are using it to survive and thrive.

### ***Why the Internet?***

The Internet has five characteristics that make it an ideal tool for terrorist organizations. First, it enables rapid communications. People can hold conversations in real time using instant messaging or Web forums. Instructions, intelligence information, and funds can be sent and received in a manner of seconds via email. Second, using the Internet is a low-cost proposition. Terrorist organizations can now affordably duplicate many of the capabilities needed by modern militaries, government organizations, and businesses: a communications infrastructure, an intelligence-gathering operation, a training system, and a media-savvy public affairs presence. Third, the ubiquity of the Internet means that small terrorist groups can have a global cyber presence that rivals that of much larger organizations. Terrorist members can communicate with each other from almost anywhere in the world. A small terrorist cell may create a Web site that is viewed by millions of people and even examined daily by media outlets for news stories.<sup>50</sup> Fourth, the growth in bandwidth combined with development of new software has enabled unsophisticated users to develop and disseminate complex information via the Internet. For example, "In December 2004, a militant Islamic chat room posted a twenty-six-minute video clip with instructions on how to assemble a suicide bomb vest, along with a taped demonstration of its use on a model of a bus filled with passengers."<sup>51</sup> Finally, modern encryption technologies allow Internet users to surf the Web, transfer funds, and communicate anonymously—a serious (though not insurmountable) impediment to intelligence and law enforcement organizations trying to find, track, and catch terrorists. To do this, terrorists can download various types of easy-to-use computer security software (some of which is commercial and some of which is freely available) or register for anonymous email accounts from providers like Yahoo! or Hotmail.<sup>52</sup>

The combination of characteristics described above makes the Internet a valued strategic asset for terrorists. In fact, one could argue that the Internet, in conjunction with other modern communications technologies, is a *sine qua non* of the modern global extremist

movement.<sup>53</sup> What follows is an examination of how terrorists are using the Internet to influence target audiences and to improve their operational effectiveness.

### ***Influence Operations***

The Internet allows terrorist groups to control their image with target audiences and the media. Usually this is accomplished via Web sites: “A typical terrorist Web site usually includes information about the history of the group or organization; biographies of its leaders, founders, heroes, and commanders; information on the political, religious, or ideological aims of the organization; and news bulletins and updates.”<sup>54</sup> This information is presented in the best possible light. For example, most terrorist Web sites avoid mentioning the violent means used by that group to achieve its aims and instead focus on their justifications and valor in resisting whatever political, religious, or social repressions are driving their actions. Some Web sites are quite sophisticated; they feature high-quality graphics and up-to-date information and can be read in multiple languages. In addition to Web sites, terrorist groups use a variety of collaboration tools, such as chat rooms, to help foster a spirit of unity and collectivism among their followers similar to that found in many political campaigns.<sup>55</sup>

One goal of terrorist influence campaigns is to build a sustaining level of support and tolerance among their constituents. The Internet allows extremists to deliver well-coordinated propaganda campaigns that increase the levels of support among the general public; this in turn allows the terrorists to operate freely in these societies. For example, one of al Qaeda’s goals is to use the Internet to create “resistance blockades” in order to prevent Western ideas from “further corrupting Islamic institutions, organizations, and ideas.”<sup>56</sup> One technique is to distribute Internet browsers that have been designed to filter out content from undesirable sources (for example, Western media) without the users’ knowledge.<sup>57</sup>

In addition to influencing the general public and media, terrorist groups need to recruit active members who will work in direct support of the cause. In other words, successful terrorism requires the transformation of interested outsiders into dedicated insiders.<sup>58</sup> Once someone has become an insider, less intense but still continuous interactions are required to maintain the needed level of commitment to the cause. Before the advent of advanced communications technologies, this process was entirely based on face-to-face interactions, which limited the scope of a given group. However, the Internet allows groups to create and identify dedicated insiders, and to maintain fervor in those already dedicated to the cause, on a global scale.<sup>59</sup>

### ***Operational Effectiveness***

There is no doubt that the Internet has revolutionized how businesses, governments, and nonprofit institutions conduct their affairs. The same is true with terrorist organizations. By using the Internet, terrorist groups that used to operate as small localized cells with limited capabilities can now operate on a global scale. We have seen how cyberspace abets terrorist recruiting. The same medium can be used to train those recruits and turn them into effective fighters for the cause:

Using the Internet, jihadists have created a virtual classroom that teaches the online jihadist community how to produce and construct weapons ranging from simple IEDs [improvised

explosive devices] to nuclear, biological, and chemical weapons. Not only are jihadists taught military tactics; they also learn how to mine the Internet for information, protect their anonymity online, encrypt the contents of their computers, and use the Internet to benefit the global jihadist movement.<sup>60</sup>

This points to several other benefits terrorists gain from the Internet. For example, they can use it as an effective intelligence-gathering tool: “Terrorists have access not only to maps and diagrams of potential targets but also to imaging data on those same facilities and networks that may reveal counterterrorist activities at a target site.”<sup>61</sup> They can use anonymous communications mechanisms to conduct planning and operational command and control. Al Qaeda did just that for the 9/11 attacks. Terrorists can use the Internet to raise funds, without which they cannot operate effectively. The Internet allows terrorist groups to obtain money through a variety of means, including targeted donations (funds given directly to organizations such as al Qaeda, Hamas, or Hizballah), indirect donations (funds given to religious groups or other ideological/political organizations that can pass along the money to terrorists), and even through cyber criminal activities (such as identity theft or fraudulent scams).

Last but not least, the Internet enables terrorists to alter their organizational structures. In the words of one team of terrorism experts: Terrorists will continue moving from hierarchical toward information-age network designs. Within groups, ‘great man’ leaderships will give way to flatter decentralized designs. More effort will go into building arrays of transnationally internettted groups than into building stand-alone groups.<sup>62</sup>

This move from “hierarchical” to “horizontal” greatly complicates the counterterrorism problem facing the United States.<sup>63</sup> The United States knows how to take down traditional hierarchical organizations: it targets the center of gravity, removes it, and watches the group (military, criminal, or terrorist) descend into chaos. Unfortunately, this approach is not optimal against a highly networked, horizontal organizational structure that has no center of gravity. In fact, attempting to take out the leader of a leaderless organization may actually make things worse because decisionmaking authority may devolve to the next layer, or more accurately, the next circle, of the organization.<sup>64</sup>

## Recommendations

This section begins with prescriptions addressing the issue of cyber terrorism. It then offers recommendations for dealing with terrorist use of the Internet.

While cyber terrorism does not pose a serious risk to U.S. national security at this time, the other cyber threats described in table 19–1—especially crime, espionage, and state-sponsored information warfare—are more worrisome. The

U.S. Government is taking these threats seriously and is acting to minimize the risks they pose.<sup>65</sup> Of course, many if not most of these attacks are aimed at organizations in the private sector where the Federal Government has little day-to-day involvement in cyber security. The response of the private sector to these cyber threats has been mixed: some organizations have developed outstanding cyber defenses, while others have fallen woefully short. Overall, though, there is a clear understanding across all parts of the Nation that cyber threats are a real problem that will only get worse over time. As a result, most public and private sector organizations are taking steps to improve their cyber defenses. Although these efforts are primarily aimed at

countering cyber crime and espionage, they work equally well against hacktivism and cyber terrorism. While the offense generally has the advantage over the defense in such a cyber arms race, the fact that organizations are running to stay ahead of motivated and well-funded cyber criminals and thousands of hackers means that these organizations are probably moving fast enough to stay ahead of cyber terrorists.

Thus, it is imperative for organizations across the U.S. economy to continue bolstering their defenses against cyber attacks, and they should do so using a defense-in-depth strategy that focuses on protection, detection, and response. The latter in particular often receives insufficient attention. Security professionals tend to focus on preventing cyber attacks from succeeding, so most of their time, energy, and resources is spent on perimeter defenses such as firewalls and intrusion detection systems. The problem with this approach is that, sooner or later, an attack will succeed and the targeted system will go down or its integrity will be called into question. Another problem is that perimeter defenses do not help against malicious insiders, human errors, natural disasters, or systemic failures.<sup>66</sup> At that point, the key issue is availability: How can people get access to the information they need? Perimeter defenses and intrusion detection systems cannot help with that problem. That is why focusing on response is so critical.

Systems that are resilient can respond quickly after facing cyber attacks, human errors, and even natural disasters. Building in such resilience is expensive, inefficient (unless something bad happens), and time consuming. Organizations will need to conduct their own risk assessments to determine if such expenditures are worthwhile. However, the benefits of resilience are often underestimated by many organizations until it is too late. This is especially true for critical infrastructures that are possible targets of cyber terrorists or nation-states.<sup>67</sup> Because most of these infrastructures are owned and operated by the private sector, the issue of infrastructure resilience is a complex public policy problem that requires tradeoffs among options that all carry serious risks or costs. The risks of not acting are growing with each passing day.

On another front, the United States must make every effort to prevent terrorist groups from recruiting or hiring people with strong technical and analytical skills. If terrorists wish to develop the ability to perform complex and coordinated attacks, they will need to obtain the expertise somewhere. This is a vulnerability that the United States can exploit. Groups trying to grow their own experts may send members to universities in the United States or Europe. It may be possible for the United States and its allies to identify and track students who are affiliated with these groups. If terrorists attempt to hire outside experts, they could become vulnerable to infiltration by Western agents (professional or amateur) posing as IT experts with sympathetic beliefs. There is a window of opportunity right now. The Irhabi 007 incident shows that terrorist groups are currently lacking in deep IT expertise, but that situation is likely to change in the future. Once such expertise is resident within terrorist groups, it will be easier for them to develop internal training programs, and they will be less likely to seek outside training and education.

Finally, the United States needs to explore the potential utility of preemption and deterrence (cyber or kinetic) for preventing cyber terror attacks from occurring in the first place.<sup>68</sup> These options offer a number of benefits but they also pose a number of technical, operational, and legal challenges. Further study is needed to determine if, how, and when such options can be pursued.

### *Terrorist Use of the Internet*

The Internet enables terrorist organizations to operate as transnational, virtual organizations. They can use it to do fundraising, recruiting, training, executing command and control, intelligence-gathering, and information-sharing. Clearly, it is in the interest of the United States to disrupt or undermine these activities. The good news is that relying on the Internet is a two-edged sword for terrorist organizations: despite the many benefits associated with using this technology, it also carries liabilities. For example, terrorist reliance on Web sites and discussion forums allows outsiders to monitor their methods and track trends. It creates the opportunity for outsiders to pose as insiders in order to provide misinformation or simply to create doubt among the terrorists about whom to trust. The bad news is that terrorists are doing their best to minimize the liabilities associated with heavy reliance on the Internet. They are quick to learn from mistakes and to disseminate best practices on how to defeat the tactics used by intelligence and law enforcement agencies.<sup>69</sup>

The remainder of this chapter explores different strategies that the United States can pursue to counter terrorist use of the Internet. It does so by examining the strengths and weaknesses of targeting the three components of the “information environment” as defined by DOD: physical (infrastructure), information (content), and cognition (perceiving and deciding).<sup>70</sup>

### *Physical Infrastructure*

One approach to counter extremists’ use of the Internet is to target their communications infrastructure to deny or disrupt their ability to communicate or to maintain an Internet presence. The benefit of this strategy is that it would seriously harm their ability to operate effectively precisely because of their heavy reliance on this medium. It might also force the extremists to use other means of communication that are potentially more cumbersome for them and easier for the United States to monitor.

While attacking the Internet infrastructure of terrorist groups carries clear benefits, it also brings significant challenges. The majority of extremist organizations depend on commercially owned infrastructure for their communications needs. Most of that infrastructure, especially the elements that provide Web-based services, is hosted in the United States or Europe. As a result, a strategy of countering extremist activities by attacking their infrastructures would require the United States to target itself or its allies. There may be cases where the infrastructure in question is owned or operated by a company that resides in a country that is not allied with the United States. In such cases, a direct attack (either via physical or cyber means) on the targeted information infrastructure might prove to be useful in certain circumstances. The United States would have to weigh the perceived benefits of such an attack against the political and military risks associated with a potential act of war against another sovereign nation.

Another option would be for the U.S. Government to ask infrastructure providers to identify extremist clients and selectively terminate or disrupt their activities. Unfortunately, this is harder than it sounds. Extremists often pose as legitimate companies or use false information to register for accounts. They also tend to move between providers frequently. To complicate matters further, the issue of monitoring terrorist activities inside the United States requires both government and industry to weigh the rights of free speech against the needs for national security. There is no clear consensus on where to draw the line between these competing demands.

Finally, in the cases where infrastructure providers can identify extremists that are using their services, it might make more operational sense for the United States to monitor or eavesdrop on the extremists rather than just shut them down (in which case they would simply move to another provider). This approach— which could be called “tolerate, monitor, and exploit”—could provide the United States with valuable intelligence. It could also open the door to the planting of disinformation.

### *Content*

A second approach to countering extremists’ use of the Internet is to target their content. The goal here is to affect one or more of the three components of information assurance: confidentiality, integrity, and availability. By attacking the *confidentiality* of information, the United States would deny the terrorists the ability to communicate secretly and securely. This could be accomplished by using wiretaps, breaking encryption algorithms, or using undercover agents to gain access to secure chat rooms and Web sites (these sites are usually password protected and their locations are revealed only to trusted members via secure email or other covert means). While government agencies will clearly play a key role in such activities, nonprofit organizations such as the SITE Institute are also contributing to the cause by monitoring terrorist Web sites and providing information to a range of interested parties, including elements within the U.S. Government.<sup>71</sup>

By attacking the *integrity* of information, the United States would be able to do two things: secretly plant misleading information in order to get the extremists to take desired actions or to begin mistrusting each other; and openly reveal that they had compromised critical information (for example, by hacking into databases or Web sites) in order to raise doubts in the minds of the terrorists about the validity of all of their content. Surprisingly, nongovernmental organizations appear to be conducting these types of activities as well. For example, there are cases of individual citizens who have infiltrated terrorist networks via chat rooms and then worked with government agencies to bring about several arrests.<sup>72</sup>

Finally, by attacking the *availability* of their content, the United States would deny the extremists effective and timely access to their information. This could be accomplished in numerous ways, including both physical and cyber means such as denial-of-service attacks.<sup>73</sup> Given their heavy reliance on the Internet, limiting terrorist access to the content available via that medium alone would limit the effectiveness of these groups.

While attacking extremist content is generally easier than taking out the physical infrastructure upon which it depends, this strategy still requires the United States to overcome several challenges. One problem is that terrorist groups are adept at quickly moving their Web sites from host to host, which makes them difficult to track and shut down (trusted members of these groups use chat rooms, email, and other forums to share information about the new location of a moved Web site). Some of their activities masquerade as legitimate business operations. A related challenge is that the number of relevant Web sites is growing extremely quickly. Thus, significant resources would be required to keep track of the tremendous amount of extremist content appearing online. This also means that compromising some data, or denying access to a few Web sites or databases, might have a small impact on the overall extremist movement. In the words of cyber terrorism expert Gabriel Weimann: “Those who think that we can stop terrorism by removal of Web sites are either naive or ignorant about cyberspace and its limitations for interference.”<sup>74</sup>

A final problem is that terrorists tend to use secure chat rooms and encrypted emails to transmit critical pieces of information. Many use free anonymous email accounts provided by companies like Yahoo! and Microsoft. This allows them to use public computers at any location, such as a cyber café, to communicate. It is much harder to find and disrupt, alter, or deny these messages than it is to track Web sites, which is itself a challenge.

### *Cognition*

A third approach to countering terrorist use of the Internet is to focus on the cognitive domain rather than on either the infrastructure or the content per se. The goal is to influence how people perceive information and how they make decisions. In order for this approach, sometimes referred to as perception management, to be successful, it must be tied closely to the broader war of ideas against the extremist Islamic movement. For example, attempts to alter the perceptions of target audiences must consider factors such as language, culture, values, and context.

There are a number of advantages associated with perception management. First, it can be used to reduce the perceived legitimacy and attractiveness of terrorist movements. This, in turn, could have a cascading effect on the ability of terrorist groups to recruit, raise funds, maintain operational security, influence the media, and operate training bases. Perception management can also be used to influence allies and nonaligned parties in order to build support for U.S. policies and actions targeted against these groups. Another benefit of using perception management, especially the public diplomacy component, is that it can help spread U.S. values around the world. This reduces the likelihood of military conflict and improves the chances for beneficial economic relations, both of which reduce factors that can contribute to the success of terrorist groups.

The United States faces two significant challenges in the area of perception management. The first is that its current ability to operate a well-coordinated, government-wide strategic perception management campaign is limited. Shortcomings in the area of public diplomacy have been well documented, but many efforts on the military side have also come up short.<sup>75</sup> Developing a robust strategic perception management capability will require time and resources at the agency level (specifically at the State Department and DOD), and an effective interagency process for the development and coordination of coherent themes and messages—a significant challenge given the government's current structure. Former Secretary of Defense Donald Rumsfeld admitted as much when he said, "If I were rating, I would say we probably deserve a D or D+ as a country as to how well we're doing in the battle of ideas that's taking place. . . . So we're going to have to find better ways to do it and thus far we haven't as a government. The government's not well organized to do it."<sup>76</sup>

Finally, perception management campaigns, even ones that are well funded and organized, take many years to reach fruition. Changing how people think is not easy; it may take a generation or more. The United States needs to take a long-term view of the problem, much as it did during the Cold War. Unfortunately, such long-term thinking is rare in the current political climate because incentives work against spending money now to achieve benefits that will not accrue for years or even decades.

Despite the challenges associated with perception management, the "war of ideas" cannot be ignored; it is a critical component of U.S. efforts to counter terrorist movements. The following suggestions should be helpful no matter what specific strategy the United States

decides to follow in this area.

First, U.S. efforts to influence must be tied to real-world actions. While it is easy to focus purely on the principles of effective communications strategies, our words will ring hollow if they are not related to the realities experienced by the target audience. Thus, it should go without saying that what the United States does is as (if not more) important as what it says. To that end, diplomatic and military influence operations must ensure that target audiences are aware of the positive actions undertaken by the United States in the Muslim world, while simultaneously highlighting the negative actions being taken by our enemies. The corollary to this point is that the United States must effectively get its story out before the terrorists or insurgents can use the Internet to spin events in their favor. It is much harder to respond to or discredit initial stories, even ones that are untrue, than to establish the baseline facts or perceptions in the first place. Elements of the U.S. Government are making efforts in this area. For example, the State Department maintains a Web site in a number of languages (including Arabic, Farsi, and French) that is devoted to countering false stories that appear in extremist sources. It also focuses on countering disinformation likely to end up in the mainstream media. U.S. Embassies have used the Web site's resources to counter disinformation in extremist print publications in Pakistan and elsewhere. There are also military units deployed overseas that are exhibiting "best practices" in operational level influence operations.<sup>77</sup> Unfortunately, much work remains to be done for such examples to become the rule rather than the exception.

A related point is that the United States must view the war of ideas as being equally important as the military and law enforcement aspects of the war on terror. The "war of ideas" aspects of any decision involving the global war on terrorism must be considered at the highest levels of U.S. policymaking. That emphasis must then be communicated down the chain so that all players understand the importance of "message" in this war. Strategic communications cannot be seen as an afterthought of a military operation or as the sole responsibility of an office buried within the State Department. Similarly, information operations cannot be viewed simply as a set of activities done by a local commander in support of tactical objectives. Countering terrorist use of the Internet will require a government-wide approach to designing and implementing perception management strategies.

Third, the United States must reframe the terms of the war of ideas. Words like *jihad* and *mujahideen* are part of the popular lexicon describing antiterrorist operations in Iraq, Afghanistan, and elsewhere. However, such terms disempower the United States while legitimizing the terrorists' story line. *Jihad* literally means *striving* and is frequently used to describe every Muslim's responsibility to strive in the path of God. *Mujahideen* is closely translated to mean *holy warriors*. These terms may have worked to the U.S. advantage when Osama bin Laden was fighting against the Soviet Union in Afghanistan; however, use of those same words now paints the United States as a legitimate enemy of holy warriors who are engaged in a just war. The United States needs to adopt a formal lexicon of Arabic terms for referring to various players and concepts in the global war on terror.<sup>78</sup> For example, we should use terms such as *hirabah*, meaning *unholy war*, and *irhabists*, meaning *terrorists*, when talking about extremist groups.<sup>79</sup> Such words reframe the conflict between groups such as al Qaeda and the United States in ways that will resonate with Muslim audiences. Similarly, the United States can leverage values that are grounded in Islamic theory and traditions, such as honor, to emphasize peaceful ways to achieve political ends.<sup>80</sup>

As important as it is for the United States to improve its own communications efforts, a key part of countering extremist misinformation and propaganda is to have messages come from a

variety of sources, some of them preferably local. For example, it is critical for the United States to promote the views of well-respected Muslim clerics to counter the claims made by Islamic terrorists and extremists. There are examples of this type of activity taking place, including some efforts by the government of Saudi Arabia, but more needs to be done.<sup>81</sup> The United States should do everything possible to enable moderate Muslims to develop a strong, healthy, and responsive Internet and media presence of their own.

Last but not least, resources must be made available to support all of these efforts, plus others that are not mentioned here but are equally important, such as training and education to improve understanding of Muslim cultures and languages. Current U.S. resources dedicated to strategic communications, public diplomacy, and information operations are woefully inadequate.<sup>82</sup> On the military side, the lack of training and education in information operations at all levels— strategic, operational, and tactical—often requires commanders to both learn on the job and to build information operations teams “out of hide.”<sup>83</sup> While some leaders will certainly rise to the occasion, this approach is not a recipe for success in a complex, media-heavy war effort against adversaries who are highly adept at conducting their own influence operations.

## Conclusion

Terrorists are using the Internet to harm U.S. national security interests, but not by conducting large-scale cyber attacks. Instead, they are using it to plan and conduct physical attacks, spread their ideology, manipulate the general public and the media, recruit and train new terrorists, raise funds, gather information on potential targets, and control operations. As a result, terrorist groups can easily operate on a global front and use the networked nature of cyberspace to become both more effective and robust. Thus, it is critical for the United States to combine its cyber defense efforts with a well-developed strategy for countering terrorist use of the Internet. Such a strategy must be well resourced, developed, and executed in an interagency context, and flow coherently up and down the chain of command. It must address the war of ideas occurring between extremist groups and the West, and it must attempt to counteract the operational effectiveness that these groups gain by using the Internet. This task will not be easy, but it must be done. Technological and demographic developments portend a future in which the power of individuals and groups continues to grow relative to that of the nation-state. The United States will need to confront this reality if it wishes to thrive in the coming century.

---

<sup>1</sup> For example, “Our water and sewer systems, electricity grids, financial markets, payroll systems, air and ground traffic control systems . . . are all electronically controlled, electronically dependent, and subject to sophisticated attacks by both state-sponsored and freelance terrorists.” Joel Brenner, U.S. National Counterintelligence Executive, quoted in Jeanne Meserve, “Official: International Hackers Going after U.S.,” *CNN.com*, October 19, 2007, available at <[www.cnn.com/2007/US/10/19/cyber.threats/](http://www.cnn.com/2007/US/10/19/cyber.threats/)>.

<sup>2</sup> Evidence of terrorist use of the Internet is described in Stephen Ulph, “Internet Mujahideen Intensify Research on U.S. Economic Targets,” *Terrorism Focus* 3, no. 2 (January 18, 2006). The observation about the absence of cyber attacks comes from several sources, including Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington, DC: U.S. Institute of Peace, 2006); Dorothy E. Denning, “A View of Cyberterrorism Five Years Later,” in Kenneth Himma, ed., *Internet Security: Hacking, Counterhacking, and Society* (Sudbury, MA: Jones and Bartlett, 2006), 123–139; James Lewis, “Cyber Terror: Missing in Action,” *Knowledge, Technology, & Policy* 16, no. 2 (Summer 2003), 34–41; and Joshua Green, “The Myth of Cyber-Terrorism,” *Washington Monthly*, November 2002, available at <[www.washingtonmonthly.com/features/2001/0211\\_green.html](http://www.washingtonmonthly.com/features/2001/0211_green.html)>.

<sup>3</sup> This chapter focuses on terrorism associated with various fundamentalist Islamic movements.

---

<sup>4</sup> Department of Defense, Joint Publication 1–02, *Department of Defense Dictionary of Military and Associated Terms* (Washington, DC: The Joint Staff, April 12, 2001, as amended through October 17, 2007), 544.

<sup>5</sup> Dorothy E. Denning, “Is Cyber Terror Next?” in *Understanding September 11*, ed. Craig Calhoun, Paul Price, and Ashley Timmer (New York: The New Press, 2002), 193. Emphasis added.

<sup>6</sup> For example, see Dan Verton, *Black Ice: The Invisible Threat of Cyber-Terrorism* (Emeryville, CA: McGraw-Hill/Osborne), 2003, xx.

<sup>7</sup> Jon Swartz, “Cyberterror Impact, Defense under Scrutiny,” *USA Today*, August 3, 2004, available at <[www.usatoday.com/tech/news/2004-08-02-cyber-terror\\_x.htm](http://www.usatoday.com/tech/news/2004-08-02-cyber-terror_x.htm)>.

<sup>8</sup> Greg Bruno, “The Evolution of Cyber Warfare,” Council on Foreign Relations Backgrounder, February 27, 2008, available at <[www.cfr.org/publication/15577/](http://www.cfr.org/publication/15577/)>.

<sup>9</sup> “Hacktivism,” *Wikipedia*, available at <<http://en.wikipedia.org/wiki/Hacktivism>>.

<sup>10</sup> For example, see BBC News, “U.S. Hackers Told to Leave Iraq Alone,” February 14, 2003, available at <<http://news.bbc.co.uk/2/hi/technology/2760899.stm>>.

<sup>11</sup> “Hacker,” *Wikipedia*, available at <<http://en.wikipedia.org/wiki/Hacker>>.

<sup>12</sup> Carole Fennely, “Motivation to Hack,” *Internet Security News*, available at <<http://seclists.org/isn/2000/Nov/0039.html>>.

<sup>13</sup> “Espionage,” *Wikipedia*, available at <<http://en.wikipedia.org/wiki/Espionage>>.

<sup>14</sup> Rhys Blakely et al., “MI5 Alert on China’s Cyberspace Spy Threat,” *Times Online*, December 1, 2007, available at <[http://business.timesonline.co.uk/tol/business/industry\\_sectors/technology/article2980250.ece](http://business.timesonline.co.uk/tol/business/industry_sectors/technology/article2980250.ece)>.

<sup>15</sup> “FBI Thinks China is Greatest Threat,” *Newsmax.com*, November 4, 2007, available at <[http://www.newsmax.com/insider\\_report/China\\_Is\\_Greatest\\_Threat/2007/11/04/46612.html](http://www.newsmax.com/insider_report/China_Is_Greatest_Threat/2007/11/04/46612.html)>.

<sup>16</sup> John Arquilla and David Ronfeldt, *In Athena’s Camp: Preparing for Conflict in the Information Age* (Santa Monica, CA: RAND, 1997), 28.

<sup>17</sup> *Ibid.*, 30.

<sup>18</sup> McAfee Virtual Criminology Report, “Cybercrime: The Next Wave,” 2007, available at <[www.mcafee.com/us/local\\_content/reports/mcafee\\_criminology\\_report2007\\_en.pdf](http://www.mcafee.com/us/local_content/reports/mcafee_criminology_report2007_en.pdf)>.

<sup>19</sup> A botnet is a network of bots. A bot (short for robot) is a computer that has been compromised by a hacker with software that allows the hacker to control it remotely. Botnets can be quite large; some include more than a million machines.

<sup>20</sup> Henry H. Willis, *Guiding Resource Allocations Based on Terrorism Risk*, WR–371–CTRMP (Santa Monica, CA: RAND, 2006). This framework is quite similar to the one currently in use by the Department of Homeland Security. For a detailed analysis of the DHS approach, see Todd Masse, Siobhan O’Neil, and John Rollins, “The Department of Homeland Security’s Risk Assessment Methodology: Evolution, Issues, and Options for Congress,” CRS Report RL33858 (Washington, DC: Congressional Research Service, 2007), available at <<http://fpc.state.gov/documents/organization/80208.pdf>>.

<sup>21</sup> Bill Nelson et al., *Cyberterror: Prospects and Implications* (Monterey, CA: Center for the Study of Terrorism and Irregular Warfare, 1999), 15.

<sup>22</sup> *Ibid.*, 77.

<sup>23</sup> *Ibid.*, 86.

<sup>24</sup> For a good description of the Nimda virus, see <[www.symantec.com/security\\_response/writeup.jsp?docid=2001-091816-3508-99&tabid=2](http://www.symantec.com/security_response/writeup.jsp?docid=2001-091816-3508-99&tabid=2)>.

<sup>25</sup> The United States is still developing its own testbeds. In 2007, U.S. Joint Forces Command began working on an Information Operations Range, and the Defense Advanced Research Projects Agency solicited proposals for a computer attack “firing range.”

<sup>26</sup> Nelson, xi. Another study conducted by Gartner and the Naval War College reached similar conclusions. Richard Hunter, “Digital Pearl Harbor: Getting Real with Cyber- War,” presentation at National Defense University, Washington, DC, April 2005.

<sup>27</sup> For a discussion of the huge gap between actual risks and perceived risks of terrorism in the United States, see John Mueller, *Overblown: How Politicians and the Terrorism Industry Inflate National Security Threats, and Why We Believe Them* (New York: Free Press, 2006).

<sup>28</sup> For a discussion of this topic, see Robert A. Miller and Irving Lachow, *Strategic Fragility: Infrastructure Protection and National Security in the Information Age*, Defense Horizons No. 59 (Washington, DC: Center for Technology and National Security Policy, 2007).

<sup>29</sup> Denning, “A View of Cyberterrorism Five Years Later,” 135–136.

<sup>30</sup> Rita Katz and Michael Kern, “Terrorist 007, Exposed,” *The Washington Post*, March 26, 2006, B1.

- 
- <sup>31</sup> Evan F. Kohlman, "The Real Online Terrorist Threat," *Foreign Affairs* 85, no. 5 (September- October 2006), 121.
- <sup>32</sup> Lewis, 36.
- <sup>33</sup> In fact, there were probably more actual cyber attacks during this period than indicated here; data on cyber incidents almost always underrepresents the actual problem because organizations are often reluctant to admit that they have been attacked.
- <sup>34</sup> Lawrence Wright, "The Spymaster: Can Mike McConnell Fix America's Intelligence Community?" *The New Yorker*, January 21, 2008, 51.
- <sup>35</sup> Office of the Coordinator for Counterterrorism, "A Strategic Assessment of Progress against the Terrorist Threat," *Foreign Policy Agenda* 12, no. 5 (May 2007), 46–50. See also U.S. Department of State, *Country Reports on Terrorism 2006*, available at <[www.state.gov/s/ct/rls/crt/2006/](http://www.state.gov/s/ct/rls/crt/2006/)>.
- <sup>36</sup> Kristin Roberts, "U.S. Warns of Possible Qaeda Financial Cyberattack," *Reuters*, December 1, 2006, available at <[www.alertnet.org/thenews/newsdesk/N30222160.htm](http://www.alertnet.org/thenews/newsdesk/N30222160.htm)>.
- <sup>37</sup> *Ibid.*
- <sup>38</sup> *Ibid.*
- <sup>39</sup> This conclusion has been reached by a number of renowned security experts, including James Lewis, Bruce Schneier, and Ira Winkler. For example, see Ira Winkler, *Zen and the Art of Information Security* (Rockland, MA: Syngress, 2007), 76–79.
- <sup>40</sup> An excellent example of the effectiveness of this approach is the fact that al Zarqawi was able to accelerate the withdrawal from Iraq of about 50 Philippine soldiers by kidnapping a Philippine citizen and threatening to behead him. Clearly, the posting of previous beheadings on the Internet had its intended effect in this case. See Evan Osnos, "Philippines Begins Withdrawal," *The Chicago Tribune*, July 15, 2004, available at <[www.globalsecurity.org/org/news/2004/040715-philippines-withdrawal.htm](http://www.globalsecurity.org/org/news/2004/040715-philippines-withdrawal.htm)>.
- <sup>41</sup> Quoted in Lewis, 36.
- <sup>42</sup> Bruce Schneier, *Beyond Fear: Thinking Sensibly About Security in an Uncertain World* (New York: Copernicus, 2006), 237.
- <sup>43</sup> See Marc Sageman, *Understanding Terror Networks* (Philadelphia: University of Pennsylvania Press, 2004).
- <sup>44</sup> Nelson, 76.
- <sup>45</sup> Gartner, "Gartner Survey Shows Phishing Attacks Escalated in 2007; More than \$3 Billion Lost to These Attacks," press release, December 17, 2007, available at <[www.gartner.com/it/page.jsp?id=565125](http://www.gartner.com/it/page.jsp?id=565125)>.
- <sup>46</sup> See Miller and Lachow.
- <sup>47</sup> For an excellent discussion of scale-free networks, see Albert-Laszlo Barabasi, *Linked* (New York: Plume, 2003), or chapter 5 in this volume, "Cyberspace and Infrastructure."
- <sup>48</sup> Denning, "A View of Cyberterrorism Five Years Later," 127.
- <sup>49</sup> Henry A. Crumpton, Coordinator for Counterterrorism, Department of State, "The Changing Face of Terror: A Post-9/11 Assessment," statement before Committee on Senate Foreign Relations, June 13, 2006.
- <sup>50</sup> Weimann, 110. For example, many news services reported the 2004 beheading video of Nick Berg, which was originally uploaded on the Web site of the militant Islamist group Muntada al-Ansar (a group associated with al Qaeda). The popularity of the video can be inferred from the fact that "Nick Berg" was the second most frequent search term in Google in May 2004.
- <sup>51</sup> *Ibid.*, 126–127, citing Lisa Myers, "Web Video Teaches Terrorists to Make Bomb Vest," *MSNBC News*, December 22, 2004, available at <[www.msnbc.msn.com/id/6746756](http://www.msnbc.msn.com/id/6746756)>.
- <sup>52</sup> Some terrorist Web sites provide guides on how to use the Internet "safely and anonymously." See Jarret M. Brachman, "High-Tech Terror: Al-Qaeda's Use of New Technology," *The Fletcher Forum of World Affairs* 30, no. 2 (Summer 2006), 156.
- <sup>53</sup> For an excellent discussion of the impact of the Internet on terrorist recruitment, see Frank Cillufo et al., "NETworked Radicalization: A Counter-Strategy," report of the George Washington University's Homeland Security Policy Institute and the University of Virginia's Critical Incident Analysis Group, 2007.
- <sup>54</sup> Weimann, 52.
- <sup>55</sup> For a discussion of the similarities between political activism and terrorism, see Weimann, 23–31.
- <sup>56</sup> Brachman, 160.
- <sup>57</sup> *Ibid.*, 152.
- <sup>58</sup> This process, and the impact of the Internet upon it, is described in Sageman, 158–161.
- <sup>59</sup> The recruiting process is usually not entirely done in cyberspace. At some point, face-to-face interactions are used to assess the level of commitment of potential members. See Sageman, 163.
- <sup>60</sup> Rita Katz, Director, SITE Institute, "The Online Jihadist Threat," testimony before the Homeland Security

---

Committee, Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment, U.S. House of Representatives, November 6, 2007.

<sup>61</sup> Weimann, 113.

<sup>62</sup> John Arquilla, David Ronfeldt, and Michele Zanini, "Networks, Netwar, and Information- Age Terrorism," in *Countering the New Terrorism*, ed. Ian O. Lesser et al. (Santa Monica, CA: RAND, 2001), 41.

<sup>63</sup> See Ori Brafman and Rod A. Beckstrom, *The Starfish and the Spider* (New York: Penguin Group, 2006).

<sup>64</sup> *Ibid.*, 143.

<sup>65</sup> For example, there was a series of closed congressional hearings in early 2008 on a new classified Presidential Directive designed to improve the cyber security of all Federal Government networks.

<sup>66</sup> Some high-risk systems are almost guaranteed to fail at some point. See Charles Perrow, *Normal Accidents: Living with High-Risk Technologies* (Princeton: Princeton University Press, 1999).

<sup>67</sup> For a good discussion of this issue, see Stephen Flynn, *The Edge of Disaster* (New York: Random House, 2007).

<sup>68</sup> See chapter 13 in this volume, "Deterrence of Cyber Attacks."

<sup>69</sup> For example, see Abdul Hameed Bakier, "The Evolution of Jihadi Electronic Counter- Measures," *Terrorism Monitor* 4, no. 17 (September 8, 2006).

<sup>70</sup> Department of Defense, Joint Publication 3-13, *Information Operations* (Washington, DC: Department of Defense, 2006).

<sup>71</sup> See Benjamin Wallace-Wells, "Private Jihad," *The New Yorker*, May 29, 2006, available at <[www.newyorker.com/archive/2006/05/29/060529fa\\_fact](http://www.newyorker.com/archive/2006/05/29/060529fa_fact)>.

<sup>72</sup> For example, see Blaine Harden, "In Montana, Casting a Web for Terrorists," *The Washington Post*, June 4, 2006, A3.

<sup>73</sup> The goal here is to deny access to information without going after infrastructure. Clearly, destroying or disrupting the Internet infrastructure of terrorist groups would also affect the availability of their content. However, because targeting infrastructures is not easy, going after data directly may often be easier technically, legally, and politically.

<sup>74</sup> Greg Goth, "Terror on the Internet: A Complex Issue, and Getting Harder," No. 0803- 03003, *IEEE Distributed Systems Online* 9, no. 3 (2008).

<sup>75</sup> See, for example, U.S. Government Accountability Office, "U.S. Public Diplomacy: Interagency Coordination Efforts Hampered by the Lack of a National Communication Strategy," GAO-05-323, 2005, available at <[www.gao.gov/new.items/d05323.pdf](http://www.gao.gov/new.items/d05323.pdf)>.

<sup>76</sup> CBS News, "Rumsfeld: U.S. Losing War of Ideas," March 27, 2006, available at <<http://www.cbsnews.com/stories/2006/03/27/terror/main1442811.shtml>>.

<sup>77</sup> An excellent example is found in Ralph O. Baker, "The Decisive Weapon: A Brigade Combat Team Commander's Perspective on Information Operations," *Military Review* (May-June 2006), 13-32. This article should be required reading for everyone in the

U.S. Government remotely involved in the Long War, and especially for Active-duty forces heading to Iraq and Afghanistan. Chapter 14 in this volume, "Cyber Influence and International Security," also has a nice discussion of tactical influence operations.

<sup>78</sup> Jim Guirard, "Petraeus Aide's Call for a 'New Lexicon'," *TrueSpeak.org*, available at <[www.truespeak.org/print.php?id=petraeusaidescallforanewlexicon](http://www.truespeak.org/print.php?id=petraeusaidescallforanewlexicon)>.

<sup>79</sup> For more detail, see Douglas E. Streusand and Harry D. Tunnell IV, "Choosing Words Carefully: Language to Help Fight Islamic Terrorism," Center for Strategic Communications, National Defense University, May 23, 2006, available at

<[www.ndu.edu/csc/docs/Choosing%20Words%20Carefully-](http://www.ndu.edu/csc/docs/Choosing%20Words%20Carefully-Language%20to%20Help%20Fight%20Islamic%20Terrorism%2024%20May%2006.doc)

[Language%20to%20Help%20Fight%20Islamic%20Terrorism%2024%20May%2006.doc](http://www.ndu.edu/csc/docs/Choosing%20Words%20Carefully-Language%20to%20Help%20Fight%20Islamic%20Terrorism%2024%20May%2006.doc)>; and Jim Guirard,

"Hirabah versus Jihad: Rescuing Jihad from the al Qaeda Blasphemy," *The American Muslim*, July 6, 2003, available at

<[http://theamericanmuslim.org/tam.php/features/articles/terrorism\\_hirabah\\_versus\\_jihad\\_rescuing\\_jihad\\_from\\_the\\_al\\_qaeda\\_blasphemy/](http://theamericanmuslim.org/tam.php/features/articles/terrorism_hirabah_versus_jihad_rescuing_jihad_from_the_al_qaeda_blasphemy/)>.

<sup>80</sup> On the role of honor in Islam, see Akbar S. Ahmed, *Islam under Siege* (Cambridge, UK: Policy Press, 2003).

<sup>81</sup> For more details, see Robert Spencer, "Losing the War of Ideas," *FrontPageMagazine.com*, February 5, 2004, available at

<[www.frontpagemag.com/Articles/Read.aspx?GUID=3D75E317-8475-4677-97C8-4A5136A4C72](http://www.frontpagemag.com/Articles/Read.aspx?GUID=3D75E317-8475-4677-97C8-4A5136A4C72)>.

<sup>82</sup> See, for example, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, *Report of the Defense Science Board Task Force on Strategic Communication* (Washington, DC: Department of Defense, September, 2004).

---

<sup>83</sup> Baker, 20.