Cyberterrorism: How Can American Foreign Policy Be Strengthened in the Information Age?

Jonathan Matusitz

Introduction

This article contains an analysis of how cyberterrorism, the direct result of the continued globalization of information (also called the Information Revolution or Information Age), is likely to affect American foreign policy in the first decade of the twenty-first century and beyond. Cyberterrorism is the intentional use of threatening and disruptive actions against computers, networks, and the Internet. By examining its similarities to and differences from conventional terrorism, American policymakers are attempting to place cyberterrorism into a new framework and address the problems posed by this phenomenon. Another goal of this study, then, is to demonstrate that in order to assess the importance of information technology in the making of American foreign policy, it will be necessary to exercise special care and establish security measures, anticipating and questioning some of the false assumptions raised by cyberterrorism.

This new millennium has probably become the period of America’s greatest dominance and supremacy. The dream of Woodrow Wilson to expand diplomacy internationally seems to have been fulfilled in the past 90 years of the nation’s history. Information has gone global; it pervades the political and international realm. Through information the United States is now better positioned than any other country to amplify the command of its hard and soft power resources. Nevertheless, because the Information Age has revolutionized how America communicates with the world (and vice versa) and because this vast openness of interchange is available to everyone, violent objectors and cyberterrorists have become more powerful as well. This is bad news for America.

American Foreign Policy: The Twenty-First Century Context

At the end of the twentieth century, the 1999 National Security Strategy advanced the conclusion that the United States should contribute to the expansion of information technology globally, to worldwide benefits and democracy, and to the employment of new technologies in order to improve American public diplomacy in the new Information Age. Today, in the twenty-first century, it is evident that such globalization has changed the nature of governments and sovereignty and has transformed economies, societies, and world politics. In fact, the Information Age has turned out to be a pivotal point for the United States. The impact of the technological revolution of the past 10 years on American foreign policy has proved to be as determining in scope and character as was the origin of the cold war. The United States is better positioned than any other country to communicate its hard and soft power resources through information technology.

Nevertheless, the top American foreign policy issue is its vulnerability to new security threats.
The changing nature of security and how the United States achieves it are basic factors defining the international context of American foreign policy. The terrorist attacks of September 11, 2001, and our ongoing campaign against terrorism draw attention to this reality. Our adversaries are not only nation-states but also, as exemplified by Al Qaeda’s network, increasingly potent and ambitious nonstate actors who rely on cyberspace and other technological innovations to commit their crimes or communicate their threats. Until 2004, the tenets of American foreign policy were based on the conclusions that concessions or deals should not be made with terrorists, that they should be brought to justice for their crimes, that we should isolate and apply pressure on states that sponsor terrorism, and that we should bolster the counterterrorist capabilities of countries willing to work with the United States. Now a new type of terrorist has emerged—the cyberterrorist—and the question remains: how can American foreign policymakers be prepared to counter them?

A Definition of Cyberterrorism

Considering the reality of cyberterrorism, it is fair to say that American foreign policy is at an historic turning point. The predominance of computers and their associated networks has moved us into the Information Age. Computers have remodeled terrorism in the same manner that they have changed everyday life. Terrorism in this day and age not only consists of conventional terrorism, in which classic weapons (explosives, guns, etc.) are used to destroy property and kill victims, it also consists of cyberterrorism involving the creation of weapons (malicious software and electromagnetic weapons) to destroy data in cyberspace in order to cause a disruption in the physical world.

The concept of cyberterrorism was born in the mid-1980s, when Collin, a senior research fellow at the Institute for Security and Intelligence (ISI) in California, coined this hyped-up, techno-phrase by combining two elements: cyberspace and terrorism. Almost two decades later, cyberterrorism is still hard to define because it remains a term that lacks a clear, widely accepted definition. The word has been described in many ways and from different perspectives. One of the definitions of cyberterrorism tells us that it is the intentional use of threatening and disruptive actions against computers, networks, and the Internet in order to cause harm or to further ideological, political, or similar objectives or to intimidate any person in furtherance of such objectives.

An example of such a type of cyberterrorism could be penetrating a top-secret federal computer system and stealing data, damaging files, or changing information in order to destroy infrastructure targets and cause a disruption in the federal computer network. Other cyberterrorist acts—such as destroying the actual machinery of the information infrastructure, breaching dams, disrupting monetary systems, damaging the mass media, shutting down power grids, disseminating false information, sabotaging operations, erasing data, threatening to divulge confidential information or system weaknesses, or changing prescription dosages by hacking into a computer system—sound unbelievable but are based on reality. Examples of cyberterrorism in the form of waging war against computers and the Internet can be as simple as malicious software, computer viruses, Trojan horses, computer network worms, DOS attacks, stolen passwords, insider collusion, and organized floods of electronic traffic that overwhelm computers.

Cyberterrorism is a much more urgent concern for Americans than are physical threats largely because computers are what most of the American infrastructure depends on to carry out important operations such as storing vital information and controlling the delivery of power, communications, and financial services. By examining cyberterrorism’s similarities to and differences from conventional terrorism, American policymakers are attempting to place terrorism into a new theoretical structure, address the
problem, and identify cyberterrorism’s implications for American foreign policy.

Implications for American Foreign Policy

As one can see, the globalization of information through computers (and their associated networks) is directing the world into the dark side of the Information Age. Computer technology has facilitated terrorism in the same way that it has facilitated our existence. The terrorist attacks of 9/11 and the war on terror highlight this reality. Not only are our enemies increasingly nonstate actors, but they are also hackers attempting to destroy entire infrastructures that are only a mouse click away. This is a top foreign policy issue because the cyberterrorism phenomenon exemplifies our vulnerability to new security threats. Therefore, the changing nature of security and how we attain and accomplish it are basic factors defining the international context for American foreign policy. What does cyberterrorism mean for American foreign policy? There are four implications.

Four Implications for American Foreign Policy

The first implication is that the Internet alone has raised numerous policy issues in such areas as the privacy of communications, encryption, electronic commerce, international trade, intellectual property protection, Internet governance, cybercrime, and information warfare, all of which have exerted a significant impact on foreign policy. These policy issues are the targets of young, Internet-savvy individuals who fill many of the leadership positions in current terrorist groups, underscoring the belief that the threat of cyberterrorism will grow in subsequent decades. These Internet-savvy terrorists are, in fact, well prepared to coordinate cyberattacks on national critical infrastructures. They also could disrupt military and private information systems. Although the United States has not yet experienced a major cyberattack, as many people fear, “everything,” as the old saying goes, “is possible.” It does not require much imagination to anticipate such a threat from the intrusions we have seen.

Second, because cyberterrorism knows no national boundaries and is international in scope and effect, computer attacks will cause difficulties for governments in such areas as controlling commerce, the movement of citizens and foreigners, and the circulation of information and ideas. Consequently, cognizance of the predicament of distant people will be much more significant. Individuals will be more dissatisfied with the uneven distribution of wealth and resources; they will move to other places in order to have a better life. By the same token, bitterness toward American diplomats, foreign policymakers, and even Americans in general will likely grow as American culture continues to propagate around the world.

A third problem lies in the realm of global relations that cross borders beyond government control. This realm has a good and an evil side. On the one hand, this realm includes actors such as bankers electronically transferring huge sums. On the other, it includes terrorists, among whom are hackers disrupting Internet operations. Power within this realm is broadly distributed, and so it makes no sense to speak of unipolarity or hegemony. A major implication of this development is that unilateral American foreign policy cannot cope with this type of crime. Consequently, American foreign policy has to become multilateral.

Fourth, we all know that certain terrorist groups are taking advantage of technology to influence American foreign policy. With respect to cyberterrorists, however, they are less likely to reach their foreign policy objectives than many other violent objectors or activists. The reason lies in the fact that cyberterrorists may feel a sense of empowerment because they can, for in-
stance, manipulate federal computers. Yet they will not necessarily succeed in changing any foreign policy. The main implication of this is a change on the part of American foreign policymakers themselves: They will strengthen cyberdefense policies, both nationally and internationally, rather than live up to the expectations of the cyberterrorists. A reaction of that kind will result in increasing defense against such acts, particularly attacks against important infrastructures. At the international level, the United States has addressed issues such as mutual legal assistance treaties, extradition, the sharing of intelligence, and the need for uniform computer crime laws so that cyberterrorists can be investigated and prosecuted. This effort speaks to all forms of hacking and computer network attacks, as well as to computer and telecommunications fraud. It also covers state-sponsored cyberterrorism and computer network attacks as a military weapon.17

It can be said that cyberterrorism is challenging to American foreign policy.18 As we have seen, its threat causes some of our policy decisions to be changed. One senses the importance of strengthening our cyberdefense without procrastination at both the national and international levels. If one compares the potential impact of terrorism with that of cyberterrorism, one finds that the impact of cyberterrorism on American foreign policy issues is similarly difficult to control or even to assess. No doubt the issue of cyberterrorism is playing a part in the international revolution that is taking place.

A Case Study of Cyberwar in Foreign Policy: The U.S.–China Encounter

The U.S.–China encounter is an example of cyberwar in foreign policy that occurred during a period of international tension. Immediately after NATO’s unintentional bombing of China’s embassy in Belgrade in the spring of 1999, angry Chinese hacked several American government sites. Newsbytes reported that the slogan “Down with Barbarians” was placed in Chinese characters on the home page of the U.S. embassy in Beijing.19 In addition, private computer hackers in China defaced many American Web sites and then sent computer viruses on a massive scale. This was clearly an instance of the cyberterrorist targeting of American foreign policy. The U.S.–China encounter exemplifies the notion that cyberterrorists are participants in political crises. That realization is particularly alarming because their actions can exceed the control of the American government. It appears that Washington was not able to prevent Chinese hackers from making a difficult situation even worse, both politically and economically.20

Cyberterrorism at the International Level

In a similar fashion, although it is evident that cyberterrorists are more extreme about their nationalist positions than are diplomats and other political leaders, the messages they convey inflame passions and have led some officials to conclude that their communications represent an alternative conduit of information that can be used to put pressure on the negotiating process between two countries. More important, the danger implicit in cyberterrorism creates problems for some governments, seemingly forcing them to promote more security on the Web sites maintained in their countries, and pushing other governments to consider using cyberterrorists and their weapons to advocate their interests.

A different view is called for. Why use cyberterrorists to counter other cyberterrorists? Are there not better strategies that American foreign policymakers should follow in order to eliminate or at least decrease the threat posed by cyberterrorism? New approaches to American foreign policy are certainly necessary. Armed with such strategies, American policymakers will be able to assess in depth the advantages and disadvantages that specific approaches will bring to the implementation of the national interests of the United States in the Information Age.
How Can American Foreign Policy Be Strengthened in the Information Age?

One may wonder what the consequences of information technology will be for the future of American foreign policymaking, but it is a truism that foreign policies always emerge from an understanding of how our national interests can be improved in the best way possible. The task for American foreign policymakers is to determine how serious the threat of cyberterrorism is, how we can protect ourselves against computer attacks, and how countering such attacks can further our own interests. So far it has been demonstrated that attempts to assess the impact technology has on policymaking processes have not been very fruitful. But the need to make that assessment stems from the wish for peace and prosperity. If we cannot win the war against terrorism, then how can we win the battle against cyberterrorism? Which foreign governments are likely to be most allegiant or most important? Do we need to change our foreign policy completely? To answer these questions, which constitute only a sample of all the questions that should be asked in order to improve the situation, the author offers six suggestions as to how American foreign policy can be strengthened in the Information Age and how it can fight cyberterrorism effectively. What is needed are (a) a new diplomacy, (b) multilateral policymaking, (c) help from foreign governments, (d) private services, (e) a better reliance on scientific and technological innovations, and (f) more emphasis on culture.

A New Diplomacy Needed

A new diplomacy? Yes. Although Americans possess unmatched communications skills and excellent information technology, a new diplomacy that can be used in the process of the globalization of information is needed to protect our citizens from cyberterrorism and to reinforce people’s faith in American foreign policy. The American government has already set up organizations to protect Uncle Sam from cyberattacks. Unfortunately, these efforts are premature and will encounter considerable hurdles. One of the problems is that rumors and stories about cyberterrorism increase as a result of fear of the unknown. We have adequate reasons to believe that cyberterrorism has become an important national security concern. Accordingly, a new American foreign policy and diplomacy to fight cyberterrorism must stem from a clear understanding of its potential and inherent risks and limits.

In line with these contentions and despite our protective foreign policy, we need a new, promising, and more dynamic diplomacy to comply with the plethora of requirements of the Information Age. American foreign policymakers should move faster to build open, reliable networks for communication within and between American agencies and U.S. missions abroad. For instance, as networks of cyberterrorists become stronger and closer and as their communication moves very rapidly, diplomats must deal with situations in which there is an increase in threatening events and reverberations that resonate throughout the environment. Policymakers’ responses to cyberterrorist acts need to be quicker and more effective. In effect, their reactions will call for different, efficient, and fast policymaking processes.

Another motive for a new diplomacy is the need to undertake a more rational quest for peace that should be pursued within prudent limits. As Joseph Nye suggested, “Prudence alone cannot determine the national interest in the information age. Better consequences will flow if interests are rationally pursued within prudent limits.” One objective should be to win the battle of global information flows and dominate the airwaves as Great Britain once dominated the seas and oceans. This new diplomacy, designed to win the battle of global information flows, involves training intelligence agents about cyberterrorism. Intelligence agencies strive to compete with information that is available in the open literature.
Intelligence is still a vital component of the policy process, of course, but it increasingly consists of integrating information from sources that are mainly heterogeneous.

It has been reported that foreign governments also have employed cyberattack techniques against other countries. One of the tasks of our new diplomacy, then, is to address this threat. Even if a government has not started a cyberwar and even if its skills and resources may never be commensurate with those of another government (that actually did commence a cyberwar), it is the responsibility of American foreign policymakers to act as peacemakers among belligerent countries that use cyberterrorism as a tool to attack others.

**Multilateral Policymaking Needed**

The United States must avoid unilateralism and engage nations in multilateral policymaking to maximize and uphold its expertise at influencing outcomes. It must summon international coalitions to address shared threats and challenges, the biggest one being terrorism. The foreign policy of the Information Age involves more than hegemony or unipolarity; it is insufficient to concentrate only on the military and economic dimensions. Doing so will not sustain dominant foreign policy paradigms.

Besides, we exist in a soft power world in which governments are not the only players. Many transnational players (i.e., multinational corporations, nongovernmental organizations [NGOs], individual hackers, and cyberterrorists) play roles over which no national government exerts much control. Consequently, power is widely dispersed and cannot be determined rationally by employing such simplistic terms as hegemony or unipolarity. That is why multilateral policymaking is needed.

**Help from Foreign Governments Needed**

Because the United States has acquired unmatched means of communication and sophisticated information technology, it is the most vulnerable country to cyberterrorism. Consequently, America’s diplomacy must be supported not only by trained diplomats and intelligence agents but also by foreign governments. A partial list of cyberterrorist acts that would be difficult to prevent includes but is not limited to hacking, sending viruses, and stealing files. Those acts of cyberterrorism can target virtually all nations. Thus international cooperation to bring about effective responses is necessary. Adapting to those needs, the American government should cooperate with others by changing the meanings of sovereign jurisdiction and controlling the roles of private actors.

Because the United States cannot solve such problems by itself, it needs the cooperation of other nations to ensure the maximization of safety. In pursuing its foreign policy objectives, the United States should be more open to international compromises and accommodations with other governments. The idea of openness is crucial. Traditionally domestic policy has been made in public, whereas foreign policy has been made in secret. As the boundaries between the domestic and foreign realms have blurred, it has become apparent that no clear separation between the public and the secret can remain. Consequently, an important implication for American foreign policy is the imminent need to develop further ways to improve information sharing with other governments in order to respond more effectively to cyberterrorism. International cooperation is not only a simple matter of consultation among governments. Given the participation of multiple actors in diverse forums, it is also a matter of making concessions and agreeing to others’ ideas and objectives. Such forums include numerous national and subnational governments, each possessing a plurality of agencies and global treaty organizations. These organizations have become abundant, and their relationships have grown very complex.

The task for the American government and other governments is to join forces that reach beyond ordinary technological countermaneuvers.
by essentially redesigning the entire approach to understanding cyberterrorism. For instance, it has been reported that cyberterrorism and organized crime are more closely linked than they appear to be. This kind of connection shows that cyberterrorism cannot be fought only with traditional military means. Additional diplomatic tactics and strategies are necessary. That is why the United States will have to collaborate with complex and diverse organizations such as the European Union in order to take action in underhanded realms, those “gray areas” where cyberterrorism and organized crime coexist and even support each other. In implementing the goal of improving American foreign policy, we must acknowledge that receiving help from strong and stable nations in the world (whether neighbors or remote partners) is in our own best interests. This, then, is a priority of American foreign policy.

Because within the realm of identifying our responsibilities should be the understanding that it is necessary to single out having strong and stable allies in the world as our most important objective, it should be clear that the United States should help other countries as well. The United States has the skills and technology to create and integrate complex information systems. Technology of that kind is very appealing and could be useful to other nations. Helping them develop their own information societies and defend themselves against cyberterrorism can have positive consequences for our relationships. Also, we can help other countries by designating the U.S. Information Agency as a formal member of the National Security Council and by organizing policy planning conventions and assemblies in which recommendations concerning foreign publics and communication strategies can be discussed and become the bases for policy decisions.

Governments also should collaborate against others. For example, countries that engender cyberterrorism or knowingly harbor cyberterrorists should be prohibited from receiving American economic and computer-based assistance as well as basic aid from other nations. In addition, according to American ambassadors, 45 countries limit access to the Internet typically by forcing their inhabitants to subscribe to a state-run Internet service provider, which may filter out “objectionable” Web sites. Such collaboration between the American government and foreign governments in the war against cyberterrorism may make people feel safer and therefore lead them to believe that if diplomats can play a growing role in understanding and controlling the threat of worldwide cyberterrorism, foreign policy may improve.

**Private Services Needed**

Also necessary for American foreign policy are benefits derived from private services. In addition to governments, private services such as those provided by NGOs and other private organizations serve important roles in political and international policy. Governments tend to lose some of their power and must share the stage with more actors from the private sector. For instance, it would be interesting to investigate how companies and organizations build firewalls against terrorism. Foreign private sectors may contribute to the betterment of American foreign policy if they share the tactics and strategies they use to protect themselves against cyberattacks. Likewise, private services can help eliminate cyberparasites and assist countries with their global marketing efforts. After all, private services, whether for international trade or foreign business, are strong components of foreign policy.

**Better Reliance on Scientific and Technological Innovations**

Until 2004, although federal computers were regularly but “slightly” penetrated by hackers, no group demonstrated the ability to conduct widespread cyberwarfare activities against critical infrastructures. Nevertheless, identifying a strategic cyberterrorist attack and responding as
appropriately as possible certainly constitutes a significant foreign policy issue.\textsuperscript{34} Consequently, it is important to consider the impact of technology and science on several levels: in the area of the national interest, in international treaties, and in the global realm of the economy. Experts and leaders in the scientific and engineering communities have increasingly begun to emphasize technology’s potential to play a crucial role in hindering or circumventing cyberterrorist threats. The technological nature of policy issues requires openness because only in the context of an open review by a global community of scientists and engineers can sound technical conclusions be drawn. Therefore, the critical role played by science and technology in defining and conducting foreign policy has already made us aware of the danger of terrorism, particularly cyberthreats.

We must prepare not only to fight technology-equipped enemies in an era in which U.S. control of information is resented and fought by our former allies but also, for the sake of our national interest, to rely more heavily on scientific and technological strategies in order to improve American foreign policy. Innovative resources are necessary to render more intelligible what we have learned for offensive use. For instance, solid protection against cyberterrorism is partly founded on encryption technology that provides the authentication, probity, nonrepudiation, and confidentiality services necessary for assuring the integrity of information. In fact, powerful digital signature-based authentication used to give positive access control is probably the most effective tool that provides protection against cyberterrorism.\textsuperscript{35} In the same perspective, American foreign policymakers can provide for encryption technology in international treaties or update the U.S. Export Control Policy on Encryption Technology. This approach would deter cyberterrorists from striking and show the efficaciousness and significance of the effects of protecting critical infrastructure, as well as the increased safety of global electronic commerce and economic prosperity.\textsuperscript{36}

At the economic level, markets have accepted scientific and technological innovations more readily than many agencies. Yet economic upheavals and other economic propellants often mask more significant foreign policy concerns. In general, models still focus on the experiences and approaches of the old economy, which is still poorly equipped with information technology. That is why new development models (i.e., the installation of firewalls in businesses) are necessary to provide full protection against greedy enemies.\textsuperscript{37} Consequently, policymaking will have to model itself increasingly on the best practices available, for instance, building software against cyberterrorism. No matter what, the most effective strategies for providing protection against cyberterrorism must differ from many of the approaches that were used by the old economy in the twentieth century.

\section*{More Emphasis on Culture}

At the cultural level, cyberterrorism exemplifies the notion that the Information Age has already spawned a negative impact on worldwide culture. For instance, American movies and cartoons that emphasize cyberterrorism are distributed on other continents and do not necessarily give a good image of the United States. As the stereotype projects, “Your cultural image is your country’s image.” Therefore, an important task of American diplomats is to decrease the growing resentment of allies and others based on the cyberterrorist culture exported to their countries by the United States. As part of changing the culture of cyberterrorism, more movies and cartoons should be released that emphasize counter-cyberterrorism culture and how the battle against the evil side of the Information Age can be won. This cultural package could be used by American foreign policymakers as a tool to convince others that movie scripts or cartoon stories can reflect reality and show how the future may turn out if the war on cyberterrorism is not fought in the most effective way.
Discussion

This article has demonstrated that if foreign policy is not improved, cyberterrorism, the direct result of the continued globalization of information, may grow and affect international relations. In fact, it already has. The U.S.–China encounter illustrates how cyberterrorists can be participants in political crises. Such an intervention is particularly alarming because it can be beyond the control of the American government. Because cyberterrorism knows no national boundaries and is international in scope and effect, computer attacks will pose difficulties for governments in controlling commerce, the movement of citizens and foreigners, and the circulation of information and ideas. The danger cyberterrorism represents may reach such a degree that it will cause our decision makers to change some of our policies in radical ways. Showing no tolerance for procrastination, they will strengthen our cyberdefenses at both the national and international levels.

We must confront sweeping changes propelled by the Information Age in our quest to advance our interests. The changing nature of security and how to attain it are basic factors that define the international context of American foreign policy. American foreign policy can be strengthened in the Information Age and cyberterrorism can be fought effectively if the six suggestions offered in this article are taken into consideration. In summary, what is necessary are (a) a new diplomacy, (b) multilateral policymaking, (c) help from foreign governments, (d) private services, (e) better reliance on scientific and technological innovations, and (f) more emphasis on culture. In other words, efforts to decrease cyberterrorism will have to advance progressively on the basis of collaboration and other strategies mentioned above.

Using traditional military means to wage cyberwar is useless. Instead, diplomats and foreign policymakers must learn about the subject and communicate their findings clearly and widely.

Can we really win the war on cyberterrorism? If we cannot defeat it, we can at least reduce it, attenuate it, and to some degree control it. As the Information Age collides with the war on cyberterrorism, that challenge becomes even more critical and daunting. It follows that American foreign policy is at a pivotal point; intelligence agents are not facing traditional terrorism but a more subtle form of global terrorism that is growing and alarming. The rapid evolution of issues calls for different foreign policymaking processes. The power of the Internet and other forms of information technology should be exploited to change and politically motivate societies and not be used as a weapon against critical infrastructures. Just as the Internet can be used by independent actors to move public opinion, so can the United States and its policymakers and diplomats use it in cooperation with foreign governments.

This article contains an explanation of why the war against global cyberterror is a mandatory, not an optional, policy for the United States. The future of international relations will be shaped mostly by how the good and evil sides of the Information Age interact and how the United States and other countries respond. After moving to other nations to take up their assignments, American diplomats must reassess where power comes from in this Information Age. They will need to use sources of power such as new high-tech tools to develop new concerns about the propagation of technological capabilities and to acquire awareness of new underhanded collaboration between hackers and would-be terrorists. All of this will require an immense mastery of technology and, above all, communication. No matter what sources are used, when it comes to reaching an agreement through diplomacy, no technology will replace human contact.

For future directions, given the powerful trends evident in the globalization of information and based on the main tenets of international relations theory and foreign policy, it may prove interesting to conduct further investigations of how international policymaking is increasingly
becoming involved in global policy processes. Accordingly, it would be useful to answer the following questions: In an Internet world where global communication is a mouse click away, is all policy foreign policy? If so, in the war against cyberterrorism, what consequences follow for the policymaking process? Because the cyberterrorism agenda can be very different in the United States from what it is in other parts of the world, is it necessary for American diplomats to inform and persuade the foreign policy public that cyberterrorism is an issue of high international priority?

Another suggestion for future research is to investigate how the United States and its allies can develop a treaty that imposes the same Internet regulations on their inhabitants. Even more important than the benefit that would be obtained by forcing users to subscribe to a state-run Internet service provider that would filter out objectionable Web sites is the major benefit that would flow from having strict Internet rules. It would be easier to detect where cyberattacks come from. They would, of course, come from a country that has no such Internet regulations. By the same token, because current laws regarding Internet regulations are unique to each country, it would be fruitful to find out how legal liability and jurisdiction can become serious matters of concern for the judicial and legal systems. The major task of American diplomats is to resolve questions of uncertain jurisdiction and those issues that fall across multinational borders.

No matter what measures are taken to protect the United States and the rest of the world from the danger of cyberterrorism, American diplomats now have many strategies they can follow. In this Information Age, we must identify, study, and adopt all necessary changes that will promote the achievement of our national interests. American foreign policy will always reflect America’s drive for peace and success. After all, one of our long-term goals remains the same: living in a safe, multicultural civil place that appeals to our values and ideals.

### About the Author

Jonathan Matusitz is a doctoral student in the Department of Communication at the University of Oklahoma. His academic focus is terrorism, particularly cyberterrorism.

### Notes

11. J. Arquilla, D. Ronfeldt, and M. Zanini, “Networks, Netwar and Information-Age Terrorism,” in Countering the New Terrorism, I. O. Lesser et al., eds. (Santa Monica, 1999); M.


