How Can We Deter Cyber Terrorism?

Jian Hua¹ and Sanjay Bapna²
¹School of Business and Public Administration, University of the District of Columbia, Washington, D.C., USA
²Morgan State University, Baltimore, Maryland, USA

ABSTRACT  In order to deter cyber terrorism, it is important to identify the terrorists, since punishment may not deter them. The identification probability relies heavily on tracking cyber terrorists. However, there are legal and technical challenges to tracking terrorists. This paper proposes suggestions and insights on overcoming these challenges. Three types of infrastructures must be present in order to deter cyber terrorism: technical, policy, and legal. We list some of the key items that academics as well as practitioners need to focus on to improve cyber-terrorism deterrence.

KEYWORDS  cyber terrorism, cyber terrorist, information security, cyber deterrence, legal

1. INTRODUCTION

Considerable research and investigative efforts have been spent studying terrorism and terrorists. Prevention of bombing, kidnapping, and other common types of terrorism has been among the focal concerns in the struggle for world peace. However, terrorists do not restrict themselves to common and regular methods. The terrorist’s attack of September 11, 2001, is a primary example. It is common knowledge that information technology (IT)-based information systems are vulnerable. Hence, it is possible for terrorists to utilize the vulnerabilities of IT-based information systems to attack their adversaries and to launch an information war (Jormakka & Molsa, 2005; Embar-Seddon, 2002).

Currently, terrorism is spreading globally and being facilitated by information technology (Gable; Hua & Bapna, 2009; Foltz, 2004; Embar-Seddon). In a statement before the Senate Select Committee on Intelligence, the director of the National Intelligence testified that terrorists have intentions to deploy cyber attacks against the United States (Gable, 2009). Cyber attacks against the U.S. government in 2009 were expected to increase about 60% compared to the number of attacks in 2008, most of it coming from Chinese state and state-sponsored computers (U.S. Government, 2009). Attacks against Supervisory Control and Data Acquisition systems (SCADA) computer networks that operate the critical infrastructure have risen dramatically in 2009 and account for 20% of the 164 incidences reported since 1982 (Aitoro, 2009a). The reason cyber terrorists cannot launch attacks to cause significant damage is that these cyber terrorists have not gained the...
Sufficient expertise, which could be available within the next few years (Aitoro, 2009b).

Gable (2009) cites several recent incidences of cyber terrorism:

- A distributed denial of service (DDOS) attack launched on July 2009, which affected 27 U.S. and South Korean government agencies including the Secret Service and the U.S. Pentagon, may have been the work of cyber terrorists residing in the United Kingdom.
- Attacks on Estonian government Websites in 2007 effectively crippled the government transactions in that country.
- The information for the stealth fighter jet program was stolen.
- The U.S. Air Force’s air traffic control systems were intruded.

Currently, cyber-terrorism research has focused on three orientations: technology, legal, and economic. All of these orientations are receiving increasing attention. The technology-oriented research stream focuses on the technical means to prevent cyber attacks (Hansen et al., 2005; Griffith, 1999). The legal-oriented research stream examines the legal perspectives in order to prosecute cyber terrorists (Trachtman, 2004; Walker, 2006; Gable, 2009). The economic-oriented research stream develops and analyzes economic models to determine the level of investment necessary to safeguard information assets (Hua & Bapna, 2009). In this paper, our research specifically focuses on deterrence and prevention from cyber terrorism and thus borrows on the technical, legal, and economic orientation streams.

Because cyber terrorism can result in economically devastating threats to nations, we need to develop a framework to deter cyber terrorism. In this paper, we develop such a framework, relying on existing interdisciplinary literature and cyber-terrorism cases. Three types of infrastructures – technical, policy, and legal – must be present in order to craft cyber-terrorism deterrence policies. This paper is divided into five sections. In section 2, a comprehensive literature survey of terrorism, cyber terrorism, and deterrence is provided.

### 2. LITERATURE REVIEW

The word “terrorism” came about during the French Revolution when terror was used by the government to suppress counter-revolutionary adversaries. Most terrorists share two common aspects: (1) they assault civilians, and (2) they target victims that are not their true targets but rather these victims do influence the target audience. The term terrorist refers to a person who practices terrorism. Terrorism and terrorists have a strong negative connotation. Terrorists know that they cannot be superior to their adversaries in conventional resource-intensive warfare. Hence they rely on terrorism and low-intensive conflict to erode the enemy’s moral and physical capacities (Oprea & Mesnita, 2005).

Victoroff (2005) proposed a comprehensive typology to illustrate the dimensions of terrorism (Table 1). The demographic data about terrorists have been presented in studies by Hassan (2001), Pedahzur, Perliger, and Weinberg (2003), and Sageman (2004).

People commonly believe that terrorists are insane or psychopathic. Strictly speaking, the psychopathic ailment can be divided into two conditions: clinical illness and personality disorder. The person with clinical illness cannot differentiate right from wrong, but the person with personality disorder can. As such, terrorists are rarely psychotic or insane (Victoroff, 2005).

Contrary to common beliefs, terrorists are also rarely sociopathic. There is no evidence, from any empirical study, that demonstrates that terrorists are antisocial. Considerable evidence supports the observation that terrorists are regarded as heroes, at least by their groups or local communities. The Middle Eastern students
who join an Islamic radical group may enjoy popular support and believe they are serving their society in a pro-social way. Contrary to common understanding, terrorists are altruistic in their groups (Keet, 2003; Krueger & Maleckova, 2003).

In this section, we define cyber terrorism and delineate the differences and similarities between terrorism and cyber terrorism. Types of cyber attacks and the dangers of cyber attacks are provided. We then discuss the literature on deterrence and how it relates to cyber terrorism.

2.1. Cyber Terrorism

The term “cyber terrorism” is used to describe the new approach adopted by terrorists to attack cyberspace (Parks & Duggan, 2001). It is an extension of traditional terrorism. The threat of cyber terrorism is more dangerous than that of common information security attacks (Rogers, 1999; Verton, 2003). Cyber terrorism is becoming a major concern for most countries (Foltz, 2004).

Two ways to define cyber terrorism have been proposed (Rollins & Wilson, 2007):

- Effects-based: Cyber terrorism exists when computer attacks result in effects that are disruptive enough to generate fear comparable to a traditional act of terrorism, even if done by criminals.
- Intent-based: Cyber terrorism exists when unlawful or politically motivated computer attacks are done to intimidate or coerce a government or people to further a political objective or to cause grave harm or severe economic damage.

We define cyber terrorism as an activity implemented by computer, network, Internet, and IT intended to interfere with the political, social, or economic functioning of a group, organization, or country; or to induce physical violence or fear; motivated by traditional terrorism ideologies. Cyber terrorism includes all the dimensions as proposed by Victoroff as shown in Table 1, where the terrorism methodology is driven extensively by computer and computing network architectures. The main goal of cyber-terrorism attacks is to create fear and panic among civilians or to disrupt or destroy public and private infrastructures (Morgan, 2004). The most dangerous cyber-terrorism attacks are those that affect national infrastructure or business systems.

Cyber terrorists can be differentiated from the other hacker groups by their attack motives. (Embar-Seddon, 2002) even though the cyber attack methods and the targets attacked by cyber terrorists are the same as those adopted by other hacker groups. Cyber terrorists can launch DDOS attacks to disrupt public servers within government, telecommunication services, transportation communication systems, and utility distribution systems. They can also intrude into public media systems to spread rumor or alert civilian targets. Although cyber terrorists cannot cause death on a large scale, such as physical terrorism incidents, they might cause large monetary losses exceeding that of physical terrorism or induce fear comparable to physical terrorism acts. Thus, preventing cyber terrorism is as important as preventing terrorism.

Foltz (2004) listed some of the potential threats of cyber terrorism, including:

- Access a drug manufacturer’s facility and alter its medication formulas to be deadly (Wehde, 1998).
- Access hospital records and change patient blood types (Gengler, 1999).
- Report stolen information to others (i.e., troop movement) (Desouza & Hensgen, 2003).
- Manipulate perception, opinion, and the political and socioeconomic direction (Stanton, 2002).
- Facilitate identity theft (Gordon & Ford, 2002a).
- Attack critical infrastructure including electrical power systems; gas and oil production,
transportation, and storage; water supply systems; banking and finance; homeland security; telecommunication; agricultural and food supply; and public health (Embar-Seddon, 2002).

In its 1996 report *Cyberterror: Prospects and Implications*, The Center for the Study of Terrorism and Irregular Warfare at the Naval Postgraduate School in Monterey, California, defined three levels of cyber terror capability:

- **Simple-Unstructured**: The capability to conduct basic hacks against individual systems using tools created by someone else. The organization possesses little target analysis, command and control, or learning capability.
- **Advanced-Structured**: The capability to conduct more sophisticated attacks against multiple systems or networks and possibly to modify or create basic hacking tools. The organization possesses an elementary target analysis, command and control, and learning capability.
- **Complex-Coordinated**: The capability for coordinated attacks capable of causing mass-disruption against integrated, heterogeneous defenses (including cryptography). Ability to create sophisticated hacking tools. Highly capable target analysis, command and control, and organization learning capability.

According to the Center's estimates, a terrorist group may be able to reach the advanced-structured level within two to four years after starting from scratch and within six to ten years to reach the complex-coordinated level. However, using outsourcing or sponsorship means, a group may reach the complex-coordinated level must faster.

Compared with other terrorism approaches, cyber terrorism requires fewer people and fewer inputs. Pure cyber terrorism does not require cyber terrorists to show up in the target area. Cyber terrorists can remotely launch attacks and remain anonymous. Cyber terrorists can use proxy servers and IP-change methods to hide their real addresses. Because cyber terrorists can easily hide their identity, it is difficult for government agents to trace and capture them. This poses tremendous challenges to thwart cyber-terrorist attacks.

### 2.2. Deterrence

Deterrence theory has been widely employed in the fields of economics and criminology to study the behavior of criminals and antisocialists (Becker, 1968; Pearson & Weiner, 1985). In criminology, deterrence theory asserts that the probability of criminal behavior varies with the expected punishment, which consists of the perceived probability of being caught and the punishment level (Pearson & Weiner). The decision to undertake a criminal action by an individual is made when the individual’s expected payoff is greater than the expected punishment and cost. Moreover, the individual moves in and out of illegal activities as the opportunities change (Anadarajan & Simmers, 2003). In the realm of cyber terrorism, the expected punishment level depends upon the legal national and international frameworks, and the perceived probability of being caught depends upon the ability to identify the perpetrators and the cooperation for information sharing between nations. We classify all deterring activities in terms of three dimensions: technical, policy, and legal. The ability to use technical means to prevent cyber terrorism is not relevant to this paper, but the ability to identify terrorists using technical means is of relevance. Policy decisions, such as how often to share breaching information, are under the control of governments and organizations. Governments and societies operate under their legal infrastructures, and their ability to prosecute cyber terrorists falls under the legal dimension.

In criminology, deterrence theory focuses on the effects of punishment. In economics, deterrence theory focuses on the reward of legal behavior and the punishment of illegal behavior (Becker, 1968). In economics, deterrence theory asserts that individuals make rational decisions to maximize benefits and minimize costs. A person can make a decision to undertake a criminal activity when the expected payoff from the criminal activity exceeds the expected expense from the potential cost and punishment (Straub & Welke, 1998). Deterrence theory has an underlying assumption that human behaviors pursue pleasure and avoid pain. To deter potential criminals from committing unlawful behavior, it is necessary to impose countermeasures that increase the cost or reduce the benefits associated with doing so (Becker). Thus, for cyber terrorism in the existing legal infrastructure, the costs to commit terrorism can be increased significantly by
raising the probability of being tracked. Using different perspectives (e.g., policing, education, economics, and behavioral), we show that increasing the punishment level may not lead to deterring cyber terrorism.

Cameron (1988) studied the theoretical effect of crime deterrence and compared this effect with empirical works from other economists. Since Becker (1968) published his famous crime and punishment theory, a large body of literature on crime believed that police expenditures were an effective input to deter crime. To prove Becker’s belief, Cameron conducted a survey to test whether punishment deterred crime, in theory, and to test the effectiveness of the police in deterring crime. In comparison, a literature review indicated that punishment often increases crime or that police inputs were positively correlated with crime. After careful examination, the author found that studies using aggregate data failed to demonstrate the deterrence effects of policy inputs. On the other hand, the studies of individual prisoners and victims suggested that police inputs do have a positive deterrent effect on the supply of crime. The paper provided nine reasons why punishment may not deter crime:

1. risk in legal activities,
2. reductions in private sector deterrence efforts,
3. spillover/displacement effects,
4. effects of criminals with a target income,
5. effects on industry supply behavior for organized crime,
6. adaptive behavior,
7. practical certainty,
8. cognitive dissonance, and
9. income and substitution effects.

Nations have different legal structures for punishing criminal activities not only for these reasons but also from societal mores. Due to conflicting results of the research on punishment, it is unclear as to what degree punishment levels may deter cyber terrorism.

Workman and Gathegi (2007) studied the effects of attitudes towards the law and the effects of social influence. Their study began by investigating the counterproductive-behavior literature. Punishment and ethics education were found to be effective in deterring cyber criminal behavior. Punishment was more effective in deterring people who tried to avoid punishment or negative sequences, other than ethics education. Ethics education more so than punishment was effective in deterring people who had a strong social consciousness. People who had a high level self-control were more responsive to ethics training. People who had a low level of self-control were more responsive to punishment for information security contravention. Based on the well-know fact that terrorists are willing to sacrifice their lives, it is unlikely that the punishment level will be an effective tool in deterring cyber terrorists.

Oksanen and Valimaki (2007) discussed copyright violations and solutions on the Internet. The two authors formed a traditional behavioral economic model on the deterrence effect of lawsuits against Internet copyright violations. The general deterrence theory attempted to reduce the successful rates of criminal behavior. Their observations supported the theory that individuals tried to maximize their payoffs by calculating utilities. The authors also found that the strategy of minimizing risk was not only theoretically practiced but also extensively used. The classic deterrence model heavily relied on the utility theory and had many limitations. The two authors found that the classic deterrence model should incorporate the reputational cost of violations and the reputational benefit of violations (Sunstein, 2003). The reputational cost means the unofficial sanction applied by the individual’s peers. The reputational benefit comes from the support of the individual’s community or peers (Rebellon & Manasse, 2004). The reputational benefit may play a significant role in individual decision making. This literature shows the possible existence of the reputational benefits behind cyber terrorism. The increased reputation from peer groups after a successful cyber attack may motivate cyber terrorists to advertise their activities.

Straub and Welke (1998) considered deterrence theory as a theoretical basis for security countermeasures to reduce information security risks. They derived four distinct activities from deterrence theory: deterrence, prevention, detection, and recovery. With respect to internal computer abuse, they believed that managers were the key to successfully deterring, preventing, detecting, and pursuing remedies. The authors claimed that deterrent countermeasures were passive because they had no inherent provision for enforcement. They also believed that security training for internal employees was a form of deterrent countermeasures, which can convince potential internal computer abusers that
the company was serious about the security and would sue the computer abusers. This research clearly points to the influence of managerial policies for deterrence, prevention, detection, and recovery from cyber threats, which may have a similar impact on cyber terrorism.

The punishment may be to a person, group, or to a party to which the person belongs. The punishment may not just be imprisonment and fine. For cyber terrorism, the punishment may include antiterrorism wars against the state in which the cyber terrorists reside. Thus, the punishment to cyber terrorists may be more severe and in some cases exceed the losses they caused to the victims. Determining the proper punishment is an important issue in the legal field. Becker (1968), in his classical paper about punishment determination, believed that punishment determination has to consider the social cost of punishments and that all punishments can be converted to monetary values. Legal systems in most societies specify punishments that increase with the level of social harm caused by the criminal activities (Rasmusen, 1995). As cyber terrorism becomes more harmful, based on Becker’s theory, increasing the punishment substantially for the sake of the additional deterrence may be worth the costs. However, since the research on punishment level is inconclusive, it is difficult to quantify the level of punishment that will stop cyber terrorism.

Based on the literature survey, a functional form of punishment level on the deterrence effect for cyber terrorism is plotted in Figure 1. While the functional form is a sigmoid curve, low levels of punishment levels have little or no impact on deterrence. Only at high punishment levels do deterrence effects show up. From an economic perspective, such high punishment levels may be achieved only by means of very high investment levels, for example, extensive crippling of parts of the cyber infrastructure.

Wible (2003) proposed two approaches to deter cyber hackers: (1) reinforce the criminal law and increase punishment, and (2) decriminalized the least dangerous kinds of hacking in ways that demarginalize the hacking community. Rational economic models on deterrence perceive all potential criminals are rational. However, little empirical research supports the rational economic models on deterrence (Sheizen, 1995). The failure reason of rational economic models on deterrence is that the hackers’ perception of the probability of identification and punishment is more complex than what we thought (Zimring & Hawkins, 1973).

In a recent workshop that discussed how information warfare on the United States might be deterred, several important findings were proposed (IWAR, 2008). We map these findings into three dimensions of cyber deterrence: technical, policy, and legal.

- The workshop participants always assume that a visible set of defenses was the beginning to deter cyber attacks (policy).
- Current employed defenses were inadequate to deter well-prepared cyber attacks (technology).
- Deterrence of cyber-attacks was understood to depend upon the nature of attackers (policy, legal).
- Deterrence requires identification of the value held by the potential attackers and the capacity to communicate with those attackers (policy).
- It may be impossible to create an omnipotent deterrence policy that will be effective (technology, legal, policy).

![FIGURE 1 Effect of punishment level on deterrence. (color figure available online.)](image)
• Cyber attackers could be deterred by explicit threats and retaliatory actions implying future threats (legal, policy).
• Aggressive domestic and international law enforcement can certainly have a deterrence effect on potential adversaries. To deter cyber attackers, realistic threat of capture and punishment should be used (legal).
• Electronic IDs combined with computer hardware and software can also deter potential cyber attackers (technology).

3. CHALLENGES TO THE DETERRENCE ON CYBER TERRORISM

Deterrence theory can be applied to all cyber crimes including cyber terrorism (Ginges, 1997; Frey & Luechinger, 2002; Carns, 2001). The literature review (section 2.2) indicated that the impact of deterrence (deterrence effect) is positively correlated with the identification probability, and it also may be positively correlated with punishment level. Keeping the potential punishment severity unchanged, the deterrence effect will be determined by the identification probability. The identification probability depends upon the capability to track cyber terrorists. Thus, to increase the impact of deterrence on cyber terrorism, the identification probability must be increased. An inability to track cyber terrorists would make it difficult for local and international jurisdictions to track the entire network of cyber terrorists as well as to prosecute them due to the lack of proof of identification of these cyber terrorists. In this section, we describe the technical means available to cyber terrorists to avoid being tracked.

From a cyber terrorist’s perspective, the advantages of cyber terrorism are anonymity and the ability to remotely control the terrorist act. To attack a victim anonymously, a cyber terrorist has to make sure that he or she cannot be tracked. An experienced cyber terrorist could utilize the vulnerabilities in software, hardware, networks, Internet, human beings, and jurisdictions to avoid being tracked back.

To avoid being tracked back, cyber terrorists can employ three methods: (1) spoofing their media access control (MAC) and Internet protocol (IP) addresses, (2) using a public Internet, and (3) using proxy servers.

To access a switched network, a cyber terrorist’s computer must have a MAC address. A MAC address is unique and assigned to a network interface card (NIC) by its manufacturer for identification purpose. Similarly, if this cyber terrorist wants to access a routed network, his computer must an IP address. There are many programs available on the Internet to spoof MAC and IP addresses. A fake MAC address could cheat a firewall by bypassing a network access restriction and erase intruders’ fingerprints (a MAC address is unique and combined with a NIC card). A cyber terrorist can use a sniffer hacking tool to pick up MAC addresses from the traffic of a target network, spoof the MAC, and disguise himself as an authorized user to bypass the network access control of the target. IP address spoofing is a fairly old intruding method. In DDOS attacks, a cyber terrorist can spoof the IP addresses of source computers. Because the IP addresses are changing, it is difficult for the target to trace and defend against DDOS attacks. Of course, spoofing MAC and IP address currently cannot guarantee complete anonymity. If an investigator can trace back to the Internet service provider (ISP) of the cyber terrorist, the cyber terrorist location still can be narrowed to a small list with the connection logs provided by the ISP.

Some cyber terrorists may think of using public Internet connections such as those available at the free library or in Internet cafés. Usually these free Internet connection services do not require any identification. However, this method is not completely safe for a cyber terrorist, for example, if there are video cameras in these public areas. Investigators can use recorded video and the Internet connection logs to make a narrow suspect list.

Cyber terrorists who are good at sniffing could abuse a private wireless connection which does not have encryption protection. It is not known how to track a cyber terrorist in a wireless network (Velasco, Chen, Ji, & Hsieh, 2008). Closest access point, triangulation, and radio frequency fingerprinting are commonly used techniques for tracking in wireless networks, but all of them are inaccurate (Zeilando & Ngadi, 2008). Cyber terrorists can hide themselves in a neighbor area to utilize intruded wireless network as a proxy server and escape detection by investigators.

Proxy servers are the most common methods to prevent tracking back. Usually there are many hops between a cyber terrorist host and a target host. Cyber terrorists can utilize proxy servers to cover their locations. For example, if a cyber terrorist is living in Iraq, he can use several anonymous proxy servers hosted...
in other countries as intermediators. If the last proxy server is located in the United States, the target victim will assume the connection from a domestic area, which is not in the highly restricted area. In the other side, those anonymous proxy servers are used by many users every day. If one of those proxy servers dumps its log every two to three hours, it is difficult for investigators to find the cyber attack’s cyber path. The clue chain is broken. Sometimes cyber terrorists could use zombies as proxy servers, which are totally under their control. If cyber terrorists install special programs in their zombies to physically clean the Internet collection logs every minute, it is difficult for investigators to collect evidence. If one of those proxy servers is located in a country that does not consider cyber attacks a crime or never cooperates with the United States, it becomes impossible for investigators to collect evidences. We still think the clue chain is totally broken.

If we cannot find the location of cyber terrorists, we cannot punish them and alert their community. Tracking cyber terrorists is a big problem that must be solved. However, the history of the Internet shows that it was not designed with foolproof tracking functions. The Internet was originally designed for and used by scientists and researchers. While the Internet does have logging capabilities, these capabilities can be foiled and the Internet protocol has no other means of recording a user’s activities. Moreover, high-speed Internet development hinders tracking cyber terrorists. For example, the primary duty of an Internet route is to route packets as fast as possible in order to facilitate high-speed connections. If the Internet speed is too fast, it is impossible for a regular router to keep a sufficient log. For example, a router on the Internet with a speed of 1,000 gigabytes needs a 6,000 gigabyte memory to record one minute of traffic. The writing speed of the memory must be 100 gigabytes per second. Even though this kind of memory exists, it can increase the price of the router and the expense incurred for Internet usage. Also, current literature has not shown any available network infrastructure for tracking.

In summary, the design of the Internet, which is based on the TCP/IP, poses serious challenges to the identification of cyber terrorists. TCP/IP has several weaknesses that are inherent in the architecture of the protocol. A group knowing about these protocols can effectively sabotage it to their advantage (Bellovin, 2004). Moreover, even private networks not connected to the Internet, but based on the TCP/IP protocol they are susceptible to breaches from “springboard” attacks (US-CERT, 2005).

4. ENHANCING CYBER-TERRORISM DETERRENCE

Wible (2003) believes that reinforcing the criminal law and increasing punishment will improve the deterrence effect of cyber crimes. Similarly, increasing the identification rate will increase the deterrence effect of cyber terrorism. In order to deter cyber terrorism, the legal and law enforcement communities will need to signal the cyber terrorist community that the identification rate and the punishment severity have been increased. While it is believed that cyber terrorists fear punishment, punishment can only occur if the cyber terrorists can be traced, found, and identified. If the cyber terrorists believe they will never be identified, increasing punishment severity will be less effective in deterring hacking activities. Thus, the first line of defense is to increase the identification rate since it will be more effective in deterring potential cyber terrorism activities. Signaling mechanisms from the legal community that punishment severity has been increased also need to be sent to the cyber-terrorist community.

We propose a framework to enhance the deterrence effect for cyber terrorism (see Figure 2). This framework relies on three critical infrastructures to deter cyber terrorism activities: the technical, policy, and legal infrastructure (section 2.2).

The proposed framework incorporates six entities: the national government, fee-based Internet service providers, organizations, free Internet service providers, citizens, and other countries. As per the framework, the national government plays a leading role in enhancing deterrence for cyber terrorism. Any national government has five responsibilities in this deterrence war:

1. Enhance cooperation among different international jurisdiction areas. Without international cooperation and agreements, the evidences used to track and sue the cyber terrorists could be destroyed. From an international legal perspective, several bases of jurisdictions are available to prosecute cyber terrorists: nationality of the victim or the perpetrator (e.g., anti-child sex tourism, victims of terrorism), territorial jurisdiction based on a
state’s borders (e.g., antitrust conspiracies effecting local businesses), universal jurisdiction based on the extreme gravity of the crime (e.g., piracy, slavery, war crimes), and protective jurisdiction based on the threat to a state e.g., counterfeiting, treason. Gable (2009) argues that universal jurisdiction is most suited to cyber terrorism and is the most efficient way of deterring such crimes. Universal jurisdiction can be based on treaties among nations or in customary international law. Numerous treaties exist to prosecute terrorists, such as the Convention to Prevent and Punish Acts of Terrorism Taking the Form of Crimes Against Persons and Related Extortion that are of International Significance, and the International Convention for the Suppression of Terrorist Bombings. These treaties can conceivably be applied to cyber terrorism (Gable). Similarly, the United Nations (UN) Security Council has condemned terrorism through Security Council Resolutions 1373, 1566, and 1624. UN Resolution 51/210 is specifically aimed at cyber terrorism.

2. Fund research on adoption of Internet authentication technologies. Current technologies to track sophisticated cyber terrorists are lacking in tracing capabilities primarily due to the design of the TCP/IPv4 protocol (see section 3). With increased investments in universal adoption of IPv6, tracking problem of any packets can be solved. However, even IPv6, which uses the secure Internet Protocol Security (IPsec) to encrypt all data packets at OSI Layer 3, may not solve all issues, especially since IPv6 with backwards compatibility defeats the purpose of authentication. Moreover, terrorists may manage to acquire a previously authenticated machine. Increased funding may be directed towards creation of protocols and processes that embed authentication at all levels (Lipson, 2002).

3. Enhance cooperation between law enforcement and local ISPs. If ISPs can use advanced technologies to record all connection requests, it is much easier for investigators to track and lockdown the cyber terrorists (Morris, 2001; Benoist, 2008).

4. Educate and train the public to protect them from cyber terrorism. A policy of mandating all wireless users to implement an access control scheme to their wireless networks should prevent cyber terrorists from acquiring Internet resources easily. The policy may mandate that the default configuration of all wireless access points be set to a secure protocol and prohibit any access without a unique key assigned to
of these five policies, the first four deal with policy decisions that a central/local government needs to make. The legal infrastructure is the glue that binds these and other cyber security policies.

Internet service providers’ responsibilities include (1) adopting the latest authentication technologies and (2) logging the Internet connections. By adopting the latest authentication technologies, it will be difficult for cyber terrorists to spoof their MAC and IP addresses. By logging the Internet connections, investigators can obtain the raw historical data about all users’ activities. The technical infrastructure of cyber terrorism deterrence should support all such responsibilities.

Free Internet service providers need to tighten their access control of free Internet services. Proper identification should be required to use their free Internet services, especially for their free wireless Internet services. Free training on Internet security should be provided by local governments to their citizens. Education and mass marketing efforts to citizens should focus on the citizens to secure their home wireless networks against unauthorized uses. The technical and policy infrastructures of cyber terrorism deterrence should support the free Internet service providers.

Organizations’ responsibilities include (1) adopting the latest authentication technologies and (2) training employees to prevent cyber terrorism. By adopting the latest authentication technologies, organizations can tighten the access control of their wired network and wireless access points. It will be difficult for cyber terrorists to use the evil twin method to intrude wireless access points. By training employees against cyber terrorism, organizations can minimize the vulnerabilities of human beings. It will be difficult for cyber terrorists to utilize social engineering and rogue access points, which are unauthorized access points built by an individuals or a department. The technical and policy infrastructures of cyber-terrorism deterrence should support organizations.

All nations should adopt similar policies. However, not all nations may have the resources to fund all levels of deterrence. Nations at risk, such as the United States, can fund the adoption of the latest Internet authentication technologies and share that information. They should tighten their access control of the Internet usage along with the help of their local ISPs. If a country refuses to adopt anti-cyber-terrorism procedure, policies can be implemented that monitor their incoming Internet IP packets and slow down the rate at which Internet packets are handled within the affected nation. That country may be put on a black list (e.g., Financial Action Task Force blacklist) until that country implements the satisfactory level of anti-cyber-terrorism procedures. An international legal infrastructure needs to be created for cyber-terrorism deterrence.

Figure 3 shows the impact of increasing resources in each of the three infrastructures. The lowest most
plot (in red) shows a base deterrence function – it takes considerable resources to achieve a significant deterrence level. Improvements in the legal infrastructure result in shifting the plot to the left; that is, fewer resources are needed to achieve the same deterrence level (shown in blue). By improvements in resources allocated towards the policy infrastructure along with improvements in the legal infrastructure, lesser resources are needed to achieve the same deterrence level (shown in green). By further improving the technical infrastructure, fewer resources are needed for a target deterrence level (shown in purple). In this figure, the placement of improvements in the technical, policy, and legal infrastructures can be swapped without loss of generality. However, to achieve any meaningful benefit for deterrence for cyber terrorism, resources need to be expended for all the three infrastructures.

5. CONCLUSION

Cyber terrorism is threatening our national security and a major attack can be mounted at any time. This paper explores the literature on cyber terrorism, cyber terrorists, and deterrence aspects. In order to deter cyber terrorism, we customarily think of increasing the punishment severity unilaterally. However, the effect of deterrence depends not only on the punishment severity but also on the proper identification of the terrorists. To increase the identification probability, we must increase the probability of successfully tracking cyber terrorists. However, the tracking mechanisms have many legal and technical challenges, which are discussed in this paper. We proposed a framework to overcome these challenges and enhance our capabilities to deter cyber terrorism. We propose three types of infrastructures to deter cyber terrorism: technical, policy, and legal. Each of the three infrastructures must be present in order for a deterrence policy to be effective. For each of the three infrastructures, we have listed key areas that need to be examined.

In this paper, while we have listed the key areas to be examined, we have not done any sensitivity analysis on each of the key areas. For example, we have not addressed the issue of determining the marginal benefits of expending resources on each of the key areas. Our future work addresses this by developing an optimal resource allocation model to deter cyber terrorism. This paper provides a foundation to work on such extensions that may be of interest to practitioners and academic researchers alike.

This paper has discussed several issues with respect to deterring cyber terrorists, focusing on the identification aspects of terrorists. However, an open issue still remains on how to signal the identification and punishment level to the cyber-terrorist community. We suggest that positive news reports disseminated on TVs or newspapers can alert potential cyber terrorists (e.g., http://www.cybercrime.gov/). Cyber terrorists will be warned that this is not a “catch me if you can” game but a “we can catch if you do” game. Evaluating the effect of sending signals to the cyber-terrorist community is the focus of our ongoing research project.

REFERENCES


**BIOGRAPHIES**

**Jian Hua** is an associate professor in the Department of Marketing, Legal Studies, and Information Systems at the School of Business and Public Administration, the University of the District of Columbia. His research interests include information security, cyber internal control, and cyber auditing. His paper has been published or accepted by several academic journals and conferences. His research has won the Best Interdisciplinary Research Paper in 2009 Decision Science National Conference. He also served as a chair of Information Systems Security session in 2010 Decision Science National Conference. He received his BS in Power Engineering from Southeast University (China), his MS in Information Engineering, and PhD in Business Administration from Morgan State University.

**Sanjay Bapna** is an associate professor in the Information Sciences and Systems Department at
Morgan State University. He has more than 20 years of experience in data gathering and modeling techniques. He has worked extensively as a principal investigator for numerous funded studies related to commercial vehicle operations with the State of Maryland. His peer-reviewed papers on computer security, privacy, and decision making have been published in top-quality journals including *Decision Sciences* and *Decision Support Systems*. A joint paper with Dr. Jian Hua was recently awarded the prestigious 2009 Best Interdisciplinary Paper Award by the National Decision Sciences Institute. Another of his papers has been awarded the Best Paper by the International Association of Computer Information Systems. He obtained a B. Tech. in Chemical Engineering from the Indian Institute of Technology and MBA and PhD with specialization in information systems from the University of Iowa.