Information Security Journal: A Global Perspective, 21:102-114, 2012

ISSN: 1939-3555 print / 1939-3547 online
DOI: 10.1080/19393555.2011.647250

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

Address correspondence to Jian Hua, School of Business and Public Administration, University of the District of Columbia, 4200 Connecticut Avenue, Washington, DC 20008. E-mail: jhua@udc.edu

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, 2009; Hansen, Lowry,

Meservy, & McDonald, 2005; Chu,

Deng, Chao, & Huang, 2009). Many studies urge

paying more attention to

cyber terrorism (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 dra-

matically 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).

let alone terrorism. In section 3, we argue that in order to deter cyber terrorism, it is important to identify the perpetrators of cyber attacks, which pose both technical and legal challenges. In section 4, we develop a framework terrorism:

Gable (2009) cites several recent incidences of cyber based on the aspects learned from the literature review and challenges associated with current solutions.

· A distributed denial of service (DDOS) attack This framework clearly shows launched on July 2009, which affected 27 U.S. and that both national and international governments have tremendous South Korean government agencies including the

leverage to control cyber terrorism.

Secret Service and the U.S. Pentagon, may have been recommendations for national and inter-

the work of cyber terrorists residing in the United order to prevent and deter the

Kingdom. terrorism. We discuss the implica-

the section 5, "Conclusions and

· Attacks on Estonian government Websites in 2007 effectively crippled the government transac-

tions in that country. REVIEW

· The information for the stealth fighter jet program came about during the French

was stolen. was used by the government to

counter-revolutionary adversaries. Most ter-

· The U.S. Air Force's air traffic control systems were common aspects: (1) they assault

intruded. target victims that are not their

these victims do influence the

Currently, cyber-terrorism research has focused on term terrorist refers to a per-

three orientations: technology, legal, and economic. terrorism. Terrorism and terrorists

All of these orientations are receiving increasing atten- connotation. Terrorists know

tion. The technology-oriented research stream focuses superior to their adversaries in

on the technical means to prevent cyber attacks resource-intensive warfare. Hence they

(Hansen et al., 2005; Griffith, 1999). The legal-oriented low-intensive conflict to erode

research stream examines the legal perspectives in order physical capacities (Oprea &

to prosecute cyber terrorists (Trachtman, 2004; Walker, 2006; Gable, 2009). The economic-oriented research

stream develops and analyzes economic models to proposed a comprehensive typol-

determine the level of investment necessary to safe- dimensions of terrorism (Table 1).

guard information assets (Hua & Bapna, 2009). In this about terrorists have been pre-

We provide

national bodies in

incidents of cyber

tions of our work in

Implications."

2. LITERATURE

The word "terrorism"

Revolution when terror

suppress

rorists share two

civilians, and (2) they

true targets but rather

target audience. The

son who practices

have a strong negative

that they cannot be

conventional

rely on terrorism and

the enemy's moral and

Mesnita, 2005).

Victoroff (2005)

ogy to illustrate the

The demographic data

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. Since our focus on this paper is on deterrence, we examine the literature in these areas in details. The literature shows that punishment may not result in an adequate deterrence effect even for ordinary crimes,

How Can We Deter Cyber Terrorism?

103

↟TABLE 1 Dimensions of Terrorism (Victoroff, 2005)

Variable	Classification
Perpetrator Number	Individual vs. Group
Sponsorship	State vs. Substate vs. Individual

sented 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

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

Relation to authority	Anti-state/Anti-establishment/
Locale	Separatist vs. Pro-state
Military status	Intrastate vs. Transnational
Spiritual motivation	Civilian vs. Military
Financial motivation	Secular vs. Religious
Political Ideology	Idealistic vs. Entrepreneurial
Hierarchical role	Leftist vs. Rightist
Willingness to die	Sponsor vs. Leader
Target	Suicidal vs. Nonsuicidal
	Property vs. Individual vs. Masses
Methodology	
	of people
	Bombing, Assassination,
	Kidnapping, Mass Poisoning,
	other

group, organization, or country; or to induce 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 networks. 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 who join an Islamic radical group may enjoy popular groups. Cyber terrorists can support and believe they are serving their society in disrupt public servers within a pro-social way. Contrary to common understand- telecommunication services, transporta- ing, terrorists are altruistic in their groups (Keet, 2003; systems, and utility distribution Krueger & Maleckova, 2003). intrude into public media sys- tems to spread rumor or alert civilian targets. Although cyber terrorists cannot

In this section, we define cyber terrorism and delin- cause death on a large scale,

eate 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 such as physical large monetary losses ism or induce fear acts. Thus, preventing 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 sys-
tems; 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 pos-
sesses 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 ele-
mentary target analysis, command and control, and
learning capability.

· Complex-Coordinated: The capability for coordi-

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
nated 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

decisions, such as how often
information, are under the control
organizations. Governments and
their legal infrastructures, and
prosecute cyber terrorists falls under the
is of relevance. Policy
to share breaching
of governments and
societies operate under
their ability to
legal dimension.

In criminology,
deterrence theory focuses on the
In economics, deterrence the-
reward of legal behavior and the
behavior (Becker, 1968). In eco-
theory asserts that individuals make
maximize benefits and minimize
make a decision to undertake a

the expected payoff from the
exceeds the expected expense from
punishment (Straub & Welke,
theory has an underlying assump-
behaviors pursue pleasure and avoid
potential criminals from committing
is necessary to impose counter-
the cost or reduce the benefits
associated with doing
legal infrastructure, the costs
to commit terrorism can
effects of punishment.
ory focuses on the
punishment of illegal
nomics, deterrence
rational decisions to
costs. A person can
criminal activity when
criminal activity
the potential cost and
1998). Deterrence
tion that human
pain. To deter
unlawful behavior, it
measures that increase
rorism in the existing

be increased significantly by
attacks.

105 How Can We Deter Cyber Terrorism?

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 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
punishment may not deter crime:
two authors found that the

should incorporate the repu-
(1) risk in legal activities,
violations and the reputational benefit
(2) reductions in private sector deterrence efforts,
2003). The reputational cost
(3) spillover/displacement effects,
sanction applied by the indi-
(4) effects of criminals with a target income,
reputational benefit comes from
(5) effects on industry supply behavior for organized
individual's community or peers

2004). The reputational bene-
crime,
significant role in individual decision
(6) adaptive behavior,
shows the possible existence of
(7) practical certainty,
behind cyber terrorism. The
(8) cognitive dissonance, and
peer groups after a successful
(9) income and substitution effects.
cyber terrorists to advertise

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.

and recovery. With respect to
Workman and Gathegi (2007) studied the effects
they believed that managers
of attitudes towards the law and the effects of
successfully deterring, preventing,
social influence. Their study began by investigating
remedies. The authors claimed
the counterproductive-behavior literature. Punishment
countermeasures were passive because
and ethics education were found to be effective in

had many limitations. The

classic deterrence model

tational cost of

of violations (Sunstein,

means the unofficial

vidual's peers. The

the support of the

(Rebellon & Manasse,

fit may play a

making. This literature

the reputational benefits

increased reputation from

cyber attack may motivate

their activities.

Straub and Welke

ory as a theoretical

to reduce information

distinct activities from

prevention, detection,

internal computer abuse,

were the key to

detecting, and pursuing

that deterrent

they had no inherent

provision for enforcement. They also believed that deterring cyber criminal behavior. Punishment was security training for internal employ-more effective in deterring people who tried to avoid ees was a form of deterrent countermeasures, which punishment or negative sequences, other than ethics can convince potential internal computer abusers that

the company was serious about the security and would may be achieved only by means of very high invest-sue the computer abusers. This research clearly points ment levels, for example, extensive crippling of parts to the influence of managerial policies for deterrence, of the cyber infrastructure. prevention, detection, and recovery from cyber threats, which may have a similar impact on cyber terrorism. Wible (2003) proposed two approaches to deter cyber hackers: (1) reinforce the criminal law and increase punishment, and

The punishment may be to a person, group, or to a (2) decriminalized the least party to which the person belongs. The punishment dangerous kinds of hacking in ways that demarginalize may not just be imprisonment and fine. For cyber the hacking community. Rational economic models on terrorism, the punishment may include antiterrorism deterrence perceive all potential criminals are rational. wars against the state in which the cyber terrorists However, little empirical research supports the rational reside. Thus, the punishment to cyber terrorists may economic models on deterrence (Sheizen, 1995). The be more severe and in some cases exceed the losses failure reason of rational economic models on deter-they caused to the victims. Determining the proper rence is that the hackers' perception of the probability punishment is an important issue in the legal field. of identification and punishment is more complex Becker (1968), in his classical paper about punishment than what we thought (Zimring & Hawkins, 1973). determination, believed that punishment determina-

In a recent workshop tion has to consider the social cost of punishments that discussed how informa-and that all punishments can be converted to monetary tion warfare on the United States might be deterred, values. Legal systems in most societies specify punish-several important findings were proposed (IWAR,

ments 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

FIGURE 1 Effect of punishment level on deterrence. (color figure available online.)

107 How Can We Deter Cyber Terrorism?

↟· 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

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).

attackers could be deterred by explicit threats (legal, policy).

· Aggressive domestic and international law enforcement can certainly have a deterrence effect on

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

manufacturer for identification purpose. Similarly, if this cyber terrorist wants to access a routed network, his computer

(NIC) by its

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 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
international jurisdictions to track the entire network video and the Internet
connection logs to make a
of cyber terrorists as well as to prosecute them due to narrow suspect list.
the lack of proof of identification of these cyber ter-
rorists. In this section, we describe the technical means Cyber terrorists who
are good at sniffing could abuse
available to cyber terrorists to avoid being tracked. a private wireless
connection which does not have
encryption protection.
It is not known how to track
From a cyber terrorist's perspective, the advantages a cyber terrorist in a
wireless network (Velasco, Chen,
of cyber terrorism are anonymity and the ability to Ji, & Hsieh, 2008).
Closest access point, triangulation,
remotely control the terrorist act. To attack a vic- and radio frequency
fingerprinting are commonly used
tim anonymously, a cyber terrorist has to make sure techniques for tracking
in wireless networks, but all of
that he or she cannot be tracked. An experienced them are inaccurate
(Zeilandoo & Ngadi, 2008). Cyber
cyber terrorist could utilize the vulnerabilities in soft- terrorists can hide
themselves in a neighbor area to uti-
ware, hardware, networks, Internet, human beings, and lize intruded wireless
network as a proxy server and
jurisdictions to avoid being tracked back. escape detection by
investigators.

To avoid being tracked back, cyber terrorists can Proxy servers are
the most common methods to
employ three methods: (1) spoofing their media access prevent tracking back.
Usually there are many hops
control (MAC) and Internet protocol (IP) addresses, between a cyber
terrorist host and a target host. Cyber
(2) using a public Internet, and (3) using proxy servers. terrorists can utilize
proxy servers to cover their loca-
tions. For example, if
a cyber terrorist is living in Iraq,
To access a switched network, a cyber terrorist's com- he can use several
anonymous proxy servers hosted
puter must have a MAC address. A MAC address
is unique and assigned to a network interface card

in other countries as intermediators. If the last proxy to the Internet, but
based on the TCP/IP protocol they
server is located in the United States, the target vic- are susceptible to

breaches from "springboard" attacks
tim 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.

severity will be less effective

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

(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

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. Without international cooperation and agreements, the evidences used to track terrorists could be destroyed.

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

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. From an international legal perspective, several 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

Internet

Government

Service Providers

· Cooperate with other national jurisdictions to control share information

· Cooperate with other national jurisdictions to share information

· Tighten the access of the free Internet service

(See National Government Policies)

· Invest on Internet Authentication Technologies

· Educate citizens

· Cooperate with ISPs to tighten access controls

· Legal Infrastructure

Organizations

· Train employees to prevent Cyber-Terrorism

· Adopt latest security technologies

Internet Service Providers

· Adopt the latest security technologies

· Record users activities

Citizens

· Receive education on the Internet usage

FIGURE 2 Framework of enhancing deterrence for cyber terrorism.

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 jurisdic-

TCP/IPv4 protocol (see section 3). With increased investments in universal adoption of IPv6, track- ing 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, terror-

tion 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 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 each and every individual (Morris, 2001). However, this needs to be balanced by privacy rights.

5. Create a legal infrastructure that will lead to quick and effective prosecution of hackers and white collar computer crimes. The infrastructure becomes a signaling mechanism to potential cyber terrorists that will lead to quick and effective prosecution of hackers and white collar computer crimes. The infrastructure becomes a signaling mechanism to potential cyber terrorists

ists 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

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 ter-
and thus increases their costs of conducting harmful
evil twin method to intrude wireless
activities.
training employees against cyber ter-

can minimize the vulnerabilities
Of these five policies, the first four deal with pol-
will be difficult for cyber ter-
icy decisions that a central/local government needs to
social engineering and rogue access
make. The legal infrastructure is the glue that binds
unauthorized access points built by
these and other cyber security policies.
department. The technical and pol-

cyber-terrorism deterrence should
Internet service providers' responsibilities include
(1) adopting the latest authentication technologies and
(2) logging the Internet connections. By adopting the
adopt similar policies. However,
latest authentication technologies, it will be difficult for
have the resources to fund all lev-
cyber terrorists to spoof their MAC and IP addresses.
Nations at risk, such as the United
By logging the Internet connections, investigators can
adoption of the latest Internet
obtain the raw historical data about all users' activ-
technologies and share that informa-
ities. The technical infrastructure of cyber terrorism
tighten their access control of the
deterrence should support all such responsibilities.
with the help of their local ISPs.

to adopt anti-cyber-terrorism pro-
Free Internet service providers need to tighten their
be implemented that monitor
access control of free Internet services. Proper identifi-
Internet IP packets and slow down
cation should be required to use their free Internet ser-
Internet packets are handled within
vices, especially for their free wireless Internet services.
That country may be put on a
Free training on Internet security should be provided
Financial Action Task Force blacklist)
by local governments to their citizens. Education and
implements the satisfactory level of
mass marketing efforts to citizens should focus on the

rorists to use the
access points. By
rorism, organizations
of human beings. It
rorists to utilize
points, which are
an individuals or a
icy infrastructures of
support organizations.

All nations should
not all nations may
els of deterrence.
States, can fund the
authentication
tion. They should
Internet usage along
If a country refuses
cedure, policies can
their incoming
the rate at which
the affected nation.
black list (e.g.,
until that country
anti-cyber-terrorism

procedures. An international legal
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.

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

FIGURE 3 Impact of improved resource allocations in cyber terrorism infrastructures. (color figure available online.)

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.

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

Aitoro, J. R. (2009a). Cyber attacks against critical U.S. networks ris-

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

ing at a faster rate. Retrieved from http://www.nextgov.com/nextgov/ng_20091208_4177.php

Aitoro, J. R. (2009b). Terrorists nearing ability to launch big cyber attacks against U.S. Retrieved from http://www.nextgov.com/nextgov/ng_20091002_9081.php

Anandarajan, M., & Simmers, C. (2004). Personal web usage in the workplace: A guide to effective human resources management. Hershey: Idea Group Inc (IGI).

Becker, S. G. (1968). Crime and punishment: An economic approach. Journal of Politic Economy, 76(2), 167-217.

Bellovin, S. M. (2004). A look back at "security problems in the TCP/IP protocol suite". Proceedings of the 20th Annual Computer Applications Conference (pp. 229-249). Washington, D.C.: IEEE Computer Society.

Benoist, E. (2008). Collecting data for the profiling of web users. In Profiling the European citizen cross-disciplinary perspective (pp. 169-184). Houten, Netherlands: Springer.

Cameron, S. (1988). The economics of crime deterrence: A survey of theory and evidence. Kyklos, 41(2), 301-323.

Carns, M. P. C. (2001). Reopening the deterrence debate: Thinking about a peaceful and

prosperous tomorrow. Small Wars & Insurgencies,
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
Chao, H., & Huang, Y. (2009). Next generation

Ubiquitous cyber terrorism with the accumulation of
J. Hua and S. Bapna
fears. Journal of Universal Computer Science, 15(12),

Hensgen, T. (2003). Semiotic emergent framework to

of cyber terrorism. Technological Forecasting and

70(4), 385-396.

(2002). Cyberterrorism. American Behavioral Scientist,

Cyber terrorism, computer crime, and reality.

Management & Computer Security, 12(2/3), 154-166.

Luechinger, S. (2002). How to fight terrorism: Alternatives

Retrieved from http://ssrn.com/abstract=359824

Cyber-Apocalypse now: Securing the Internet

terrorism and using universal jurisdiction as a deterrent.

http://ssrn.com/abstract=1452803

Politicians speak out on cyber terrorism. Network

6.

Deterring the terrorist: A psychological evaluation of

strategies for deterring terrorism. Terrorism and Political

11(2), 7-16.

Chu, H., Deng, D.,

of terrorism:

all intangible

2373-2386.

Desouza, K. C., &

address the reality

Social Change,

Embar-Seddon, A.

45(6), 1033-1043.

Foltz, C. B. (2004).

Information

Frey, B. S., &

to deterrence.

Gable, K. A. (2009).

against cyber

Retrieved from

Gengler, B. (1999).

Security, 1999(10),

Ginges, J. (1997).

different

Violence, 9(1), 170-185.

112

Gordon, S., & Ford, R. (2002a). Cyberterrorism? Computer & Security, 21(7), 636-647.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. MIS Quarterly, 22(4), 441-469.

Griffith, D. A. (1999). Organizing to minimize a cyber-terrorist threat? Marketing Management, 8(2), 9-15.

Sunstein, C. (2003). Why societies need dissent. Cambridge, MA: Harvard University Press.

Hansen, J. V., Lowry, P. B., Meservy, R., & McDonald, D. (2005). Genetic programming for prevention of cyber terrorism through dynamic and evolving intrusion detection. Decision Support Systems, 43(4), 1362-1374.

Trachtman, J. P. (2004). Global cyber terrorism, jurisdiction and international organization. Retrieved from http://ssrn.com/abstract=566361

U.S. Government. (2009). 2009 report to Congress of the U.S.-China economic and security review commission. Retrieved from http://www.uscc.gov/annual_report/2009/annual_report_full_09.pdf

Hassan, N. (2001). An arsenal of believers: Talking to the human bombs. The New Yorker, 77(36).

Hua, J., & Bapna, S. (2009). The impact of cyber terrorism on investment for information system security. Proceedings of the 40th Annual Meeting of Decision Science Institute, New Orleans, LA.

US-CERT. (2005). Vulnerabilities in TCP. Retrieved from http://www.us-cert.gov/cas/techalerts/TA04-111A.html

Velasco, E., Chen, W., Ji, P., & Hsieh, R. (2008, August). Challenges of location tracking techniques in wireless forensics. Proceedings of International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Harbin, China.

IWAR. (2008). How might IW attacks on the United States be deterred? Retrieved from http://www.iwar.org.uk/iwar/resources/deterrence/iwdCh2.htm

Jormakka, J., & Molsa, J. V. E. (2005). Modeling information warfare as a game. Journal of Information Warfare, 4(2), 12-25.

Verton, D. (2003). Black ice: The invisible threat of cyber terrorism. Emeryville, CA: McGraw Osborne Media.

Keet, M. (2003). Terrorism and game theory: Coalitions, negotiations and audience costs. Retrieved from http://keetwitnie.tripod.com/TerrorismGameTheory.pdf

Krueger, A., & Maleckova, J. (2003). Education, poverty, political violence, and terrorism: Is there a connection? Journal of Economic Perspectives, 17(4), 119-144.

Lipson, H. F. (2002). Tracking and tracing cyber attacks. Retrieved from http://www.cert.org/archive/pdf/02sr009.pdf

Morgan, M. J. (2004). The origins of new terrorism. Parameters, 34, 9-42.

Morris, D. A. (2001). Tracking a computer hacker. Retrieved from http://www.leetupload.com/database/Misc/Papers/Asta%20la%20Vista/Web%20Papers/tracking_a_computer_hacker.doc

Nelson, B., Choi, R., Lacobucci, M., Mitchell, M., & Gagnon, G. (1996). Cyber terror: Prospects and Implications. Retrieved 16 May 2008.

Oksanen, V., & Valimaki, M. (2007). Theory of deterrence and individual behavior. Can lawsuits control file sharing on the Internet? Review of Law and Economics, 3(3), 693-714.

Oprea, D., & Mesnita, G. (2005). The information system and the global terrorism. Retrieved from http://ssrn.com/abstract=906289

Parks, R. C., & Duggan, D. P. (2001, June). Principle of cyber-warfare. Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, West Point, NY.

Pearson, F. S., & Weiner, N. A. (1985). Toward an integration of criminological theories. Journal of Criminal Law and Criminology, 76(1),

Victoroff, J. (2005). The mind of terrorist: A review and critique of psychological approach. The Journal of Conflict Resolution, 49(1), 3-41.

Walker, C. (2006). Cyber terrorism: Legal principle and the law in the United Kingdom. Penn State Law Review, 110, 625-665.

Wehde, E. (1998). U.S. vulnerable to cyber terrorism. Computer Fraud & Security, 1, 6-7.

Wible, B. (2003). A site where hackers are welcome: Using hack-in contests to shape preferences and deter computer crime. The Yale Law Journal, 112(6), 1577-1623.

Workman, M., & Gathegi, J. (2007). Punishment and ethics deterrents: A study of insider security contravention. Journal of the American Society for Information Science and Technology, 58(2), 212-222.

Zeidanloo, H., & Ngadi, M. (2009). Intruder Location Tracking. Proceedings of the 2009 Second International Conference on Computer and Electrical Engineering (507-511). Washington, D.C.: IEEE Computer Society.

Zimring, F., & Hawkins, G. (1973). Deterrence. Chicago, IL: University of Chicago Press.

BIOGRAPHIES

116-150.
Pedahzur, A., Perliger, A., & Weinberg, L. (2003). Altruism and fatalism: The characteristics of Palestinian suicide terrorists. Deviant Behavior: An Interdisciplinary Journal, 24, 405-423.
Rasmusen, E. (1995). How optimal penalties change with the amount of harm. International Review of Law and Economics, 15(1), 101-108.
Rebellon, C., & Manasse, M. (2004). Do "bad boys" really get the girls? Delinquency as a cause and consequence of dating behavior among adolescents. Justice Quarterly, 21(2), 355-390.
Rogers, M. (1999). Psychology of computer criminals. In Proceedings of the Annual Computer Security Institute Conference, St. Louis, MO.
Rollins, J., & Wilson, C. (2007). Terrorist capabilities for cyber attack: Overview and policy issues. Retrieved from http://italy.usembassy.gov/pdf/other/RL33123.pdf
Sageman, M. (2004). Understanding terror networks. Philadelphia, PA: University of Pennsylvania Press.
Sherizen, S. (1995). Can computer crime be deterred? Security Journal, 6, 177-181.
Skibell, R. (2003). Cybercrime & misdemeanors: A reevaluation of the computer fraud and abuse act. Berkeley Technology Law Journal, 18, 909-944.
Stanton, J. J. (2002). Terror in cyberspace. American Behavioral Scientist, 45(6), 1017-1032.

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. awarded the prestigious 2009 Best Interdisciplinary Paper Award by the

National Decision Sciences
He has worked extensively as a principal investigator for numerous funded studies related to commercial vehicle operations with the State of Maryland. His peer-reviews 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 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.

J. Hua and S. Bapna 114

DarthVader@umich.edu
skywalker@indiana.edu
princess.leia@iupui.edu
ian@caret.am.ac.uu
lazr@umich.edu
robotz@iui.edu