2-2002

Technological Facilitation of Terrorism: Definitional, Legal, and Policy Issues

James D. Ballard

Joseph G. Hornik

Douglas McKenzie
Grand Valley State University, mckenzid@gvsu.edu

Technological Facilitation of Terrorism

Definitional, Legal, and Policy Issues

JAMES DAVID BALLARD
JOSEPH G. HORNIK
DOUGLAS McKENZIE
Grand Valley State University

This article notes the difficulty in defining cyberterrorism and several problems associated with identifying the potential misuses of the Internet and the World Wide Web by terrorist groups. In particular, the use of digital steganography has recently been identified as an emerging and alarming trend by law enforcement and intelligence agencies. This technological innovation is used as a case study of the complexities surrounding cyberterrorism, its definition, and how democracies can deal with these advances in communication technology. Supplementing this discussion is a review of the various social, regulatory, and legal forms of social intervention related to controlling electronic communications. The conclusion of this article includes an analytical framework from which additional research into these issues could be conducted and suggests how policy solutions for said complexities could be formulated.

Terrorism, let alone cyberterrorism, is a very difficult subject to understand. As with the Internet itself, when one approaches any semblance of an intellectually satisfying level of analytical rigor, the subject metamorphoses, thus negating efforts at objectively defining or understanding it. We wrestle with this dilemma by offering some historical perspective on the subject and logically following that discussion with a case study of steganography, an emerging technology that challenges what has been defined as cyberterrorism. The inclusion of specific historical and technical details on steganography, a form of encryption that has recently been used by terrorist groups, is offered as evidence for the potential use of technological developments by terrorists.

Thereafter, a discussion is included that addresses the various social, regulatory, and legal forms of social control related to Internet communications. As evidenced by the discussion of steganography, the Internet revolution has created unique challenges for law enforcement and counterterrorism professionals using a legalistic approach to stopping political violence. These authorities are having a difficult time adapting to the rapid pace of change and the evolving applications of technology to new and unaddressed forms of illegality. This

AMERICAN BEHAVIORAL SCIENTIST, Vol. 45 No. 6, February 2002 989-1016

discussion will offer a brief examination of several existing attempts at social control of this technology while being mindful of the gap in attempts at controlling these developments.

Although no specific solutions to the myriad uses of the Internet are offered, the conclusion of this article includes an analytical framework from which additional research could be conducted. The hope is that this will provide a basis for further analysis of the impact of the Internet on the world of terrorism studies and thus in some small part facilitate effective counterterrorism policy.

DEFINING CYBERTERRORISM

Traditionally, the mere definition of terrorism, let alone a widely accepted operational definition, has confounded scholars and provided fodder for critics of terrorism studies (Dreyfuss, 2000; Herman & Chomsky, 1988; Schmid, 1988; Wieviorka, 1988). The reasons for this definitional dilemma vary and provide debate silage to numerous researchers (Cooper, 1978; Lesser, Hoffman, Arquilla, Ronfeldt, & Zanini, 1999). To summarize the debates, it is imperative to note that no single or globally accepted definition of terrorism exists. Many critics feel that the act of defining what constitutes an act of terrorism is as political as the actions being categorized. Thus, even the simple act of agreeing on a definition has been politicized and resulted in alternative methods of tracking these activities. As a result, scholars have attempted to move beyond the politically charged confines of a definitional approach and toward schemes classifying terrorism into tactics, motives, and variables associated with the perpetrators. In doing so, they have adapted, sometimes successfully, various strategies to provide a semblance of order to the ever changing tactics used by proponents of political violence and the situations to which the pejorative label of *terrorism* has been applied.

Although many acts of terrorism have transpired over the years, and governments have been forced to address the issues brought to the fore by purveyors of political violence, the systematic study of terrorism has been a fairly recent phenomenon. Still, campaigns of terror or of violent political protest, as well as the associated literature surrounding these topics, are not new. For example, starting around 1850, the anarchist movement was linked to radical political change, although in its early incarnations, it was conceived of as a nonviolent movement. Early anarchist philosophers such as Pierre J. Proudhon were more apt to speak of the virtues of radical, decentralized democracy and did not necessarily preach the violent overthrow of existing governments (Woodcock, 1956). Those anarchists who followed in the footsteps of Proudhon would eventually become disillusioned with this passive tactic of political change and ultimately turn to more violent forms of protest.

Tangential to this alteration in anarchist philosophy was Alfred Nobel’s taming of the volatile explosive nitroglycerin and the patenting in 1867 of this invention as dynamite (Nobel Foundation, 1972). This explosive would become the weapon of choice for many terrorists, including many post-Proudhon anarchists. Johan Most, a German immigrant to the United States, is a prime example. Most published an anarchist-inspired newspaper and advocated the use of this technological development when he noted that his followers should press their cause by using the "philosophy of the bomb" (White, 1998, p. 156). This tactic and level of technological sophistication by terrorists is still considered the norm today. Thus, historically and contemporarily, bombings are by far the most popular terrorist tactic used by proponents of political violence (U.S. Department of Justice, 1998; U.S. Department of State, 2000).

Given this legacy, definitions of terrorism have evolved gradually over time. Historically, the most influential study of terrorism that used tactics as one basis of analysis was the *RAND Chronology of Terrorism Incidents* (Hoffman, 1998; Hoffman & Hoffman, 1996). The research motivations behind RAND's efforts were to facilitate the collection of objective information on the extent of the problem of political violence and to shy away from the partisan debates surrounding the politically subjective definition of terrorism.[1]

Although the complete range of definitional deliberations are beyond this article, suffice it to say that the debates on what constitutes and defines terrorism are a case study in labeling theory. If one imagines a terrorist as a violator of social norms, or at least the treatment by society of anyone labeled a terrorist as being couched in similar terms, it is easy to imagine the negative consequences of the label, as cautioned by Thrasher (1936), or to see the social process of dramatizing terrorists' evil, as noted by Tannenbaum (1938). Likewise, Lemert's (1951) idea of primary and secondary deviance can be applied to campaigns of political violence. Lastly, Becker's (1973) belief that deviance is created by rule makers who are reacting to the actions of the more powerless in society is supported by the critics of terrorism studies. These criticisms give recognition to the process whereby societies use self-motivated definitions of what constitutes a single act or a campaign of political violence to maintain existing relations of power.

Such an application of social scientific theory to the analysis of terrorism is rare and not the tactic that many scholars have pursued in recent years. The primary way of defining terrorism has become legalistic (Ballard, 2000; Mullendore & White, 1996; U.S. Department of Justice, 1998). The most widely accepted definition of reality reflecting this approach is that used by the Federal Bureau of Investigation (FBI), which notes "terrorists represent a small criminal minority in any larger social context" (U.S. Department of Justice, 1995, p. iii). While citing various statutes and guidelines as the legal authority for its investigations, the FBI also indicates a separation between domestic and international acts of political violence. Additionally, the agency uses a tripartite classification system, including incidents, suspected incidents, and preventions, to organize its activities (U.S. Department of Justice, 1998, pp. i-ii).

Lesser et al. (1999) identified a similar and global pattern of legalistic response to terrorism when noting, "states were nonetheless able to reach a measure of consensuses in outlawing specific acts such as airline hijacking" (p. v). The implication of this statement is that although governments may not readily agree on what actions constitute terrorism or exactly who should be labeled a terrorist, they are able to form some degree of consensus on legal responses to specific acts and actions taken by political dissidents. This may be one of the prime motivations for the legalistic approach to defining terrorism.

As noted, even when agencies such as the FBI define and ultimately fight terrorism as a crime, they use typologies to categorize and organize actions that do not fit the norm of acceptable political behavior. A typology is a classification system designed to help lend some sense of order to the information under consideration. The organization of politically violent behavior into typologies has a long tradition in terrorism scholarship and has been coupled with the trend toward using legalistic definitions (Ballard, 1997; Bell, 1978; Wilkinson, 1974).

White (1998) noted that these typologies help agencies and academics grasp the scope and source of the problem under consideration, categorize and identify the kinds of acts under consideration, and define what types of policy responses are necessary to react to these types of acts. One of the most often cited criticisms of typologies is that they skirt the volatile issue of how political the act of defining terrorism is and how the label of *terrorist* has very real consequences for those to whom it has been successfully been applied (Schmid, 1988).

Similarly, the literature surrounding cyberterrorism has attempted to define this act and to identify categories that encompass the various actions that should be considered under this label. One of the most assessable sound bites on what defines cyberterrorism is that it is "hacking with a body count" (Collin, quoted in Grossman, 1999). Although image invoking, this definition is not exactly usable for more than a column inch of fodder or a quick quotation in the mainstream media.

Attempts to more specifically define cyberterrorism have followed three general patterns. First, a strict definition of cyberterrorism has shown up in the literature, usually predicated on one of the existing definitions of terrorism and altering that definition to account for the new medium of the Internet. One example of this pattern combines Collin's (1996) earlier work on what exactly constitutes the cyberworld and the definition of terrorism used by the U.S. Department of State (1996). The result is a hybrid definition that states, "cyber terrorism is the premeditated, politically motivated attack against information, computer systems, and data which result in violence against noncombatant targets by sub national groups and clandestine agents" (Pollitt, 2001).

The second pattern in the characterization of cyberterrorism uses existing legal statues and authorities to define what actions constitute this crime. In a similar process to Pollitt's (2001) definition, Denning (2000) used existing definitions of terrorism and incorporated legalistic elements to account for cyberattacks.[2] Thus, cyberterrorism becomes

> the convergence of terrorism and cyberspace. It is generally understood to mean *unlawful* [italics added] attacks and threats of attacks against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political and social objectives. (Denning, 2000)

The third method of signifying cyberterrorism incorporates partial elements of the definitional attempts with accounts of specific acts or actions. To date, these efforts are incomplete, yet they seem to mimic the propensity of counterterrorist professionals to classify incidents into categories that could eventually become typologies. For example, the Canadian Security Intelligence Service stated that it focuses on "the extent to which cyber-techniques are used for espionage, sabotage, or terrorism" (Bronskill, 2001, p. A3). Likewise, generalized fears of cyberattacks are also used to try to characterize activities that could be considered cyberterrorism. Here, the specific acts are not necessarily the focus of concern; rather, rationales for the attacks are given. Thus, cyberterrorism is "the intentional use of the computer to cause panic by destabilizing the U.S. economy or playing havoc with computer data systems" (McFeatters, 2001, p. E3). Again, these types of definitions seem to lean toward the classification of incidents and could foreshadow the development of cyberterrorism typologies.

In a pattern similar to that of general terrorism studies, the same definitional problems persist with respect to cyberterrorism. In fact, because of the rapid change in technology that is part and parcel of the Internet revolution, defining and addressing cyberterrorism offers a potentially greater challenge to scholars and policy makers. Noting three problem areas relative to such developments can help summarize the challenges posed to anyone wishing to define the problem or to create an analytical typology to inform the debates.

First, the operational definition of cyberterrorism changes over time. A generation in human terms may be 25 years, but in technological time, it may be only 3 years. The challenge of rapid development in tactics is not the same for general terrorism studies, in which for years, the most common tactic has been bombings (Hoffman, 1998; Hoffman & Hoffman, 1996). The rapid development and deployment of new technological innovations demand that counterterrorism professionals looking at Internet varieties of political violence be flexible and open to these innovations.

Second, the choices of what will be included in the definitions, or even in a typology, are usually based on the personal perspectives of researchers. For example, if the author of a typology is an expert on hacking, the work he or she promotes will generally focus on varieties of this activity. By being so narrow in its analytical focus, such a biased typology may miss a variety of relevant acts and activities that would help policy makers and counterterrorism agencies.

Finally, research on cyberterrorism, as on terrorism in general, is not without critics expressing legitimate concerns. An analytically rigorous definition or typology of cyberterrorism should anticipate these criticisms. At a minimum, researchers should consider issues related to researcher bias, hegemonic support for existing structures of power, the validity and reliability of the data contained in the typology, and the lag time in recognizing technological innovations. Although these are not the only criticisms that could be brought to bear, they represent indicators of potential areas that researchers can address in their design activities and/or issues they should remain cognizant of when reviewing their work as acceptable social scientific methodology.

In the end, defining cyberterrorism is an act of faith and a dedication to reason. It is faith in those who make policies and laws, in the agencies dedicated to stopping these activities, and in the power of reason over the passion of violence. Next, a case study of a technological innovation related to cyberterrorism is presented. We argue that this is one of the issues that may arise from the mists of technological acceleration and that could blindside counterterrorism professionals using non–critically examined definitions and/or inflexible typologies.

EMERGENT INTERNET TECHNOLOGY

Considering the definitional differences, classification ambiguities, and inherent social stigma associated with being labeled a terrorist, one can imagine that the technologies used by these same social actors may similarly affect the emerging field of cyberterrorism and influence the definition of what actions and activities constitute this form of terrorism. The following section examines digital steganography as a case study of how technological developments challenge definitions and the analytical techniques used by counterterrorism professionals. This discussion notes that digital steganography has recently been identified by intelligence agencies as a threat and details how it can be used by terrorist organizations to facilitate clandestine communications (Beth, Frisch, Simmons, Goos, & Hartmanis, 1992; Brassard, 1988; Harris, 2001; Imai & Zheng, 2000; Johnson, Duric, & Jajodia, 2000; Katzenbeisser & Petitcolas, 2000; Lam, Okamoto, & Xing, 1999; Williams, 1986).[3]

To examine steganography, it may be useful to note the etymology of the word. It is derived from the Greek *steganos* (covered or secret) and *graphy* (writing or drawing). In reality, it more closely embodies the meaning of the word *stegosaur*, a dinosaur of Cretaceous times that was "covered" by an armor of triangular, bony plates on its spine (Currie & Padian, 1997; Glut, 1972). In today's electronic communications environment, *steganography* has come to mean a message that contains "hidden writing" and implies that because of its technologically enhanced armor, this writing is not discernible to the casual observer.

The secret writing to be hidden (message) is distributed by algorithmic means in the file meant to contain the secret data (container). In digital steganography, the result of the algorithmic process is saved as a separate file. Expressed verbally, result file = container file + message file.

This process is not unrecognizable as similar to that used in cryptography. In fact, cryptography and steganography are often used synonymously.[4] However, there is an important philosophical difference between the techniques. Cryptography is the science of rendering information unreadable to others (Schneier, 1994; Schneier & Banisar, 1997). Although not readable to others, the result of this process makes it obvious that the message contains a secret. For example, the message "see me" is easily encrypted using a one alphabetic character shift to the right in the array of English letters (i.e., $s = t$, etc.). The resultant message, "tff nf," will draw attention from even the most casual observer, possibly causing the observer to attempt to decrypt the message. On the other hand, using simple steganographic techniques, the message "see me" is hidden in the body of another message, such as "**s**imply **e**nter **e**very **m**otor **e**lement," by using the first character of each word in the message. Because the container is a plausible sentence, the casual observer would not necessarily suspect that the sentence is a covert message (Petitcolas, Anderson, & Kuhn, 1998).

These definitions of cryptography and steganography suggest, rightfully so, that a combination of the two techniques would provide added security to anyone wishing to protect covert communications. Encrypting the data before hiding it in the container file adds a "second layer" of protection, and as a result of this convergence of technological techniques, various steganographic software programs include tools that encrypt messages before hiding them in container files.[5]

This process is essentially a procedure for hiding information from the prying eyes of an enemy, and that is not a new idea (Denning & Denning, 1998; Kahn, 1996; Pfleeger, 1989; Seberry, 1989). Throughout history, many different methods have been used to hide messages from enemies. These include invisible inks, open codes, and messages in hollow shoe heels. Ancient Greek writings refer to shaving a messenger's head, tattooing a message directly on the scalp, and then waiting until the hair had grown out enough to deploy the messenger. Likewise, milk, urine, and fruit juice were used by the ancient Romans to write between the lines of otherwise innocuous letters. During World War II, the Germans developed the microdot to hide information. A secret message was thus reduced to the size of a period and affixed to the dot of the letter *i* or hidden as other punctuation. Large amounts of printed data, including technical data, were transmitted via microdots, and the transmission was effectively hidden (Davern & Scott, 1995).

These methods of hiding information seem rather archaic given the transnational nature of the Internet and how communications technology has changed everyday life in the 21st century. Image and sound files are quite abundant on the Internet, and few would suspect that the images and messages that traverse electronic freeways contain hidden messages. In particular, these images are found on almost all Web pages and are increasingly commonly sent via e-mail. These developments set the stage for the potential use of steganography by those who would expose political violence.

Applying digital steganography to a message is based on several simple principles. The first is that the files that contain digitized images or sounds can be altered to a certain extent without losing their functionality. The second principle rests on the inability of humans to distinguish minor changes in image color or sound quality. This element of the steganographic transaction is especially easy to use in objects that contain redundant information, including the common 6-bit sound file and 8-bit and 24-bit image files. For example, with respect to images, changing the value of the least significant bit (LSB) of the pixel color will not result in any perceivable change of that color. Likewise, sound files could contain messages within the white noise present in most recordings.[6] In both cases, the message is hidden in the "noise" found in or introduced into computerized files.

This is an important analytical point because noise is a part of everyday life, and computerized noise is abundant. Many feel that digital communications free messages from such noise, but the idea that digital circuits are noise free is not necessarily true. A digital signal may be copied and recopied without changing the original message because of the error-correcting codes and sophisticated circuitry used in the processing of messages. However, this does not eliminate the original noise. As a result, digital photographs, digitized music, and digital videos all have significant amounts of noise left over from their creation (Wayner, 1996).

Herein lie the opportunity and the challenge for anyone wishing to hide a message or detect these types of hidden communications. The noise found in digital images and sounds can be used to the advantage of someone trying to hide information. As a rule, human beings cannot detect small amounts of distortion in sounds or images. Our senses are not fine tuned enough to accomplish this task, and small amounts of distortion in sound reproductions or in the color pallets of pictures go unnoticed.

Although there are individualized techniques used by the various steganographic tools, the least common denominator among most tool sets is the modification of some of the LSBs of a container file's individual bytes.[7] In most steganographic container files, the LSBs contain the modified noise or message, which when viewed apart from the rest of the byte appear random. For example, an 8-bit image will contain minor color differences that could pass casual inspection, and a 24-bit image will contain color changes that are almost imperceptible. These distortions in image or sound files, when interpreted with the use of software and an access code, will recreate hidden messages at some other time or place.[8] As Davern and Scott (1995) noted, modifying the LSBs of certain computer files would be disastrous to the integrity of the hidden data, but certain image files can have messages hidden in them without noticeable difference.[9]

To demonstrate how this is accomplished, it is important to note that all computer image files are composed of an array of dots called pixels. Each of these pixels has its own color, represented internally as specific and separate quantities of red, green, and blue, collectively known as RGB. In an eight-bit image such as a GIF (graphics interchange format)[10] or BMP (bitmap)[11] file, each pixel is described by a number from 0 to 255 that refers to an actual color in the "color lookup table" or palette (see Table 1). For each color level, a value of 0 implies that none of the color is present, and a value of 255 implies that the full amount of the color is present. A pixel with an RGB value of 0,0,0 is black, and a pixel with an RGB value of 255,255,255 is white. In the RGB model of color distribution, there are a total of 16,777,216 (256 × 256 × 256) possible colors. Most GIF files use only an eight-bit palette. This means that of the 16,777,216 possible colors, only 256 RGB colors are in the image, because eight-bit binary numbers can have only 256 distinct values.

Second, it is important to note that an image does not contain strings of bytes that describe individual colors listed in a left-to-right, top-to-bottom order. Generally, the image itself is stored as a series of digits from 0 to 255 that reference entries in the palette (a palette reference). An image can be thought of as a grid with an index into the palette in each grid cell. In this way, an image can be reconstructed by performing palette lookups to determine which color to insert at each pixel location.

To hide data within an eight-bit GIF or BMP container, existing tools most commonly use two techniques ("Steganography Thumbprinting," 1998). The first technique involves changing the LSBs of a palette reference (0 to 255) to hide a message. A program using palette reference modification may decide which color to point to on the basis of the color's LSBs. The program may not necessarily pay attention to the similarity of the colors, only to whether or not the LSBs serve its purpose of data hiding.

The second technique involves modifying a pixel's actual color by changing the LSB of the red, green, or blue elements in the color table. By altering the LSB of each color in the RGB element, a program can hide data by making almost identical copies of colors but with slightly different LSBs. The resulting colors are very close to the originals, and this is the point at which human perception, or the discrepancies therein, takes over.[12]

GIF and BMP files have been noted in the discussion so far, but other file types exist that represent images and sounds.[13] The major difference between file types from a layperson's perspective is how they are compressed and decompressed during actual use. Kurak and McHugh (1992) identified two types of compression: lossless and lossy. The type of compression used to store a file is important when selecting file types for steganography. Both of these compression methods save storage space when uploading and downloading, but the end results may be very different when a file is uncompressed.

When it is necessary that the original information can be exactly reconstructed, lossless compression is preferred, and steganographic container files require that the original information remain intact for recovery of a hidden message. This type of compression is typical in GIF and BMP images. Lossy

TABLE 1: Primary Red-Green-Blue Color Palette

Color	*Red*	*Green*	*Blue*
Red	255	0	0
Green	0	255	0
Blue	0	0	255
Yellow	255	255	0
White	255	255	255
Black	0	0	0

compression, on the other hand, may not maintain the integrity of the original image when it is reconstructed. JPEG[14] (from Joint Photographic Experts Group) images use this method of compression. Although there are exceptions, most readily available steganographic software programs do not support or recommend using JPEG files because of this characteristic.

The default alternative to JPEG images is to use 256-color or gray-scale images. In fact, GIF images of this type are prolific on the Internet. Many authors of steganographic software stress the use of gray-scale images because the shades of gray-scale images change gradually from byte to byte. Thus, this type of image is a good candidate for containing a message. This suggests that subtleties in color variation and the choice of image as the container are both important considerations when a terrorist selects an image for steganographic use.[15]

Regardless of the method used to actually hide the data, the programs used to accomplish this task all operate basically the same way. A container image is selected, a pass-phrase is assigned, a message is encrypted and hidden in the container, and a result file is generated. The recipient needs the same tool (software) and the pass-phrase to unhide the message. Basically, all a terrorist needs to do is choose a tool, “stego” a message, and e-mail the message to a friend or post it to a publicly available site. Thereafter, an accomplice can retrieve this container message using the correct pass-phrase and the same software. Because steganography is not yet widely known, and technologically viable images are prolific on the Internet, it is very likely that the result image will go unnoticed as it reaches its destination.

What if counterterrorism professionals want to know if an image has a message hidden in it? Is this a lost cause? With the basic knowledge of steganography detailed above, should they be suspicious of every image they see? How can they start to “see” these messages? There are several techniques used to find messages hidden in container files.

Steganalysis is the art of discovering and rendering useless such covert messages (Johnson & Jajodia, 1999). To understand how steganalysis locates hidden messages, it is important to note that hiding information in electronic media alters the media's fundamental properties. This alteration may ultimately introduce some detectable form of degradation or a pattern of unusual characteristics that can be detected, either initially or over time as a pattern emerges. These unusual characteristics act as indicators of covert activity and suggest to analysts the existence of a hidden message and even the actual software used.

Johnson and Jajodia (1999) noted that counterattacks on and analysis of hidden information may take several forms: detecting, extracting, and disabling or destroying hidden information. As argued so far, the result file of a steganographic transaction may have some amount of degradation, and this degradation is not perceptible to the human senses. If this degradation has certain characteristics, it might point to the existence of a message. Detecting hidden information is complex without knowing which tool was used to create an image and, obviously, the pass-phrase, or steganographic key. Steganographic tools vary in their approaches to hiding data, and the technical aspects of all of these techniques are beyond the scope and intent of this article.

To conduct steganalysis with the intent of uncovering hidden messages, it is imperative to compare and evaluate many original and result images to catalogue the patterns of anomalies they contain. Color composition, luminance, and pixel relationships must be studied for characteristics that are not normal to previous images. This process is then used to create a knowledge base from which decoding may transpire. Three fairly common patterns found from such analysis include the unusual sorting of color palettes, distortions in the relationships between colors in color indexes, and exaggerated noise profiles. Making these minute comparisons of multiple images will eventually identify patterns that may pertain to a particular software tool. Eventually, the analysis (knowledge) base created by this process is large enough to detect the presence of a hidden message and/or the software tool used to hide it.

Of course, recurring and thus predictable patterns are not always apparent, even if distortion is noticeable. Likewise, it would be reasonable to assume that a technologically savvy terrorist group would avoid detection by randomly changing software tools and/or steganographic methodologies. Another barrier to steganalysis is that the hardware, software, and processing time needed to accomplish the identification task can be overwhelming. When an image is suspect, or when an image is known to contain a message, it may not be possible to retrieve that hidden message within a time frame acceptable for counterterrorist purposes.

The alternative is to disable the message and render the hidden information useless. With each method of hiding information, there is a trade-off between the size of the payload (the amount of hidden information) that can be embedded and the survivability, or robustness, of that information to manipulation (Johnson & Jajodia, 1999). It is just this trade-off that offers counterterrorism professionals the opportunity to disable hidden messages.

Disabling or removing messages in image files comes down to image processing techniques. Processing a suspected image using a lossy compression technique such as JPEG uses is enough to make the hidden message useless to an adversary. Another method is to overwrite the area of a file that may contain noise space useable for message hiding. Here, an agency suspecting a hidden message overwrites this area with a new message or more likely with heightened levels of noise.

The developers of steganographic tools and the users of steganalysis techniques are at odds in this cat-and-mouse game. New methods of hiding data will result in new methods of finding data, and research continues in each area. Several conclusions from the discussion of steganography and steganalysis are relevant for counterterrorism professionals:

- Although steganography has been used in various formats for thousands of years, digital steganography currently has a relatively low visibility to frontline law enforcement agencies.
- Hiding a message with steganographic methods reduces the chances that the message will be detected.
- The best container for hidden messages is an innocuous image, for example, an image of a cat, a horse, or a car. Terrorists would most likely pick an image that cannot be compared to an original.
- There are a large number of steganographic tools available both for purchase at low cost and as freeware.
- These tools are easy to use, and most computer hobbyists would be able to master them in a relatively short time.
- Methods beyond visual examination are being explored to detect messages hidden by such software tools.
- Manual examination of every image is impossible given the number of images on the Internet.
- If counterterrorist professionals want to find a hidden message in an image, they probably can, given time, technology, and funding. Disabling a message may be faster but will not provide the same depth of intelligence.

SOCIAL, REGULATORY, AND LEGAL ISSUES

The Internet is a global community, albeit one that simultaneously exists in multiple locations, cultures, and societies. It is a community with ill-defined and constantly changing norms of behavior. It also has a structure of limited sanctions for violations of these rules. In traditional social organizations or societies, sanctions are generally categorized as either formal or informal (Garland, 1990). Informal sanctions are not necessarily codified in legal or regulatory authorities, and the power to enforce them by and large rests in the interaction between social actors. In the case of the Internet, informal rules have periodically been collected and organized into texts for the mass market (Shea, 1994; Van Der Leun & Mandel, 1996). Similarly, informal calls for good behavior emerge out of this interactive milieu. Contemporary evidence of this emergent process can be found on sites related to protecting children from harmful Internet interactions (Magid, 2001). Even Internet service providers (ISPs) have rules that apply to misbehavior, and they enforce these rules as a matter of business practice (Yahoo! Inc., 2001). Using these types of socially informal rules, companies such as Yahoo! and eBay attempt to regulate the content of their Web sites and oversee the transactions that flow through their portals.

In contrast, formalized norms of behavior are generally codified in legal and regulatory authorities. As a case in point, in the United States, terrorism is defined by Title 22, Section 2656f(d) of the U.S. Code and by Title 28, Section 0.85 of the Code of Federal Regulations. Equally noteworthy, the general legalistic approach used by counterterrorism agencies in the United States is presented by the following: "Although various Executive Orders, Presidential Decision Directives, and congressional statutes address the issue of terrorism, *there is no single federal law specifically making terrorism a crime* [italics added]. Terrorists are arrested and convicted under existing criminal statutes" (U.S. Department of Justice, 1998, p. i).

In the case of cyberterrorism, such preexisting authorities are currently under review, and attempts to prosecute or to use them challenge preexisting norms related to freedom of expression and other civil liberties. The following discussion will help illustrate how difficult enforcement of these legal authorities can become when the issues of the Internet are enmeshed with counterterrorism policies.

The efficiency and convenience of the information age is available to law-abiding citizens and terrorist alike. Issues surrounding cryptography, steganography, and cyberterrorism exist as part of a technological landscape that changes with the warp speed of the latest silicon chip. U.S. government efforts to detect terrorist acts must conform to the requirements of the U.S. Constitution and federal statutes, many times documents written long before the advent of the computer.[16] The Bill of Rights, for example, went into effect in 1791. Can such a document, fashioned in the "horse-and-buggy" age, continue to meet the challenges of the high-speed Internet age? How should the courts and legal systems respond to Internet-based terrorism threats within the boundaries of First Amendment free speech guarantees, Fourth Amendment search and seizure protection, and other individual liberty protections?

One of the key legal and policy issues facing law enforcement is how terrorists threaten pubic safety by using commercially available encryption products to prevent law enforcement from engaging in reasonable searches on the basis of probable cause of criminal activity (in legal arguments, steganographic tools would fall within the purview of encryption products). Such encryption devices allow terrorists to communicate among themselves through a variety of electronic communication modes while thwarting law enforcement from gathering evidence of criminal wrongdoing by means of lawful electronic surveillance and search and seizure (Smith, 2000).

These encryption devices provide security for a vast array of legitimate electronic communications, including conventional and cellular telephone conversations, fax transmissions, Internet communications (e-mail, etc.), personal computers, wireless communications, electronically stored information, remote keyless entry systems, radio frequency communications systems, advanced messaging systems, and the like.

The illegitimate use of encryption devices may affect law enforcement in a number of areas, but this discussion will focus on electronic surveillance and search and seizure. In the United States, both of these activities must be performed within the boundaries defined by the Fourth Amendment. The Fourth Amendment's protection of "the right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures" extends to private communications, just as it does to private things and locations (*Katz v. United States*, 1967). The definition of a search is the same for the surveillance of communications as it is for visual and physical searches: It includes activities that either physically intrude into a protected location or violate a reasonable expectation of privacy. The surreptitious use of an interception device for surveillance purposes always intrudes on a reasonable expectation of privacy and always amounts to a search.

The federal statutes governing the use of wiretaps require a judicial interception court order authorizing the operation after a showing that specific communications are being used in furtherance of serious criminal activity and that normal investigative procedures have been tried and failed or reasonably appear to be unsuccessful or too dangerous (Omnibus Crime Control and Safe Streets Act, Title III, 1968; 18 U.S.C. § 2518(1)(c), 1994; *United States v. Giordano*, 1974). Only after a court order is issued can law enforcement use a device to intercept oral communications, wire communications, and electronic communications related to serious criminal activity (Omnibus Crime Control and Safe Streets Act, Title III, 1968).

As noted, encryption is now commonly used to protect various types of electronic communications, from e-mail to data on computer hard drives. Once an interception order for electronic surveillance is issued, law enforcement is faced with the hurdle of decryption that hinders the effective execution of that order. Recently, policies designed to address these issues have been passed. For example, the Communications Assistance for Law Enforcement Act of 1994 mandates that new telecommunications switching equipment be wiretap ready.

Encryption devices also affect searches and seizures under the Fourth Amendment. More and more criminally related material is being stored on hard drives, floppy disks, and various other electronic devices. Such electronic hardware is increasingly the subject of Fourth Amendment searches and seizures and, as noted, increasingly protected by encryption.

These encrypted materials from criminal activities provide a curious legal challenge. Unlike intelligence gathering aimed at global sources of terrorism and performed, for example, by the Central Intelligence Agency (CIA), state and federal law enforcement activities are aimed at gathering criminal evidence that will sustain a prosecution and conviction in open court. Under the Sixth Amendment, a defendant has the right of access to evidence and the right to cross-examine witnesses who testify against him or her. Because of the need to safeguard techniques and technologies, all of the particular methods used by the intelligence community to decode encrypted data may not be available to local law enforcement. Law enforcement officials understand that if indeed the information and techniques are shared, the evidence gathering process is subject to exposure in open court.

The challenge for law enforcement is to have commercially available encryption devices that encompass some technical means that would allow plain-text access, pursuant to a judicial interception court order, to encrypted electronic communications related to terrorists' actions or encrypted computer files lawfully seized under a search warrant (Smith, 2000). In this manner, the safeguarded techniques used by intelligence agencies will remain secure, and local law enforcement agencies can proceed with their investigations.

Encryption, like steganography, works by applying a mathematical function called an algorithm to scramble data and other communications. The algorithm used to unscramble, or decrypt, the information is generally called the decryption key. Several options that allow local law enforcement access (also known as a back door) are available. Key recovery allows immediate access to the plain text of encrypted data, and key escrow is an encryption system that provides access to encrypted data through special data recovery keys (Smith, 2000).

Both key recovery and key escrow are basically software solutions to the problem of access to encrypted information. In addition, back doors can be hardwired into the very structure of the Internet. Cisco Systems has developed a "clear zone" within computer routers it sells to ISPs. With this hardware in place, law enforcement can go to a system administrator armed with a search warrant and receive the plain text of the encrypted electronic communications that are the subject matter of the warrant (Smith, 2000).

More problematic for law enforcement is the use of "end-to-end" encryption devices that bypass ISPs and, for example, can be attached to any phone in the world. If a coconspirator has a similar device with the proper code to decrypt, the resulting conversations are encrypted end to end. Although such communications may be intercepted, they cannot necessarily be decrypted easily because the encryption hardware is in a nonrecoverable format (Smith, 2000).

There are few contemporary statutory restrictions on domestic encryption products. The only restrictions on encryption products are the export controls designed to protect national security interests and the federal government under the Export Administration Regulations (EAR) (1999), established to implement the provisions of the Export Administration Act of 1979.

American courts are divided over whether regulating the export of encryption products is a violation of the law. Three cases show the split in judicial thinking. In *Karn v. United States Department of State* (1996), the plaintiff argued that the U.S. Department of State's regulation of two disks containing encryption source code was a violation of his free speech protection under the First Amendment.

The federal district court rejected Karn's First Amendment claim and based its decision on the government's need to regulate items that have national security implications. The court held that the regulation of the two disks was content neutral and within the regulatory power of the federal government as long as other conditions were met. The additional conditions included "whether the regulation is (1) 'within the constitutional power of the government, (2) furthers an important or substantial government interest,' and (3) is narrowly tailored to the government interest" (*Karn v. United States Department of State*, 1996, p. 10). The controlling test that the court used is found in *United States v. O'Brien* (1968), in which the Supreme Court held that laws prohibiting conduct may be applied to persons engaged in speech when the laws serve a substantial government interest that is not related to suppressing a speaker's message. The disks in *Karn v. United States Department of State* (1996) passed the *O'Brien* test because of the national security interest in regulating products that might harm the United States.

In the next case, *Bernstein v. United States Department of State* (1999), the plaintiff argued that encryption regulations violated his First Amendment rights by limiting his freedom to teach, publish, or discuss with other scientists his encryption research. In the initial case, the district court held that source code is speech for First Amendment purposes. In the second hearing, the district court ruled that particular government regulations were unconstitutional prior restraints on free speech under the First Amendment. The court extended its rationale to the new EAR regulations in the third hearing.

On appeal, the Ninth Circuit Court of Appeals reviewed Bernstein's case and affirmed the lower court's finding that certain EAR regulations violate the First Amendment. The court found that source code is expressive language for First Amendment purposes. The court asserted that source code serves the same expressive function for programmers as equations do for mathematicians or graphs do for economists. The court acknowledged that the government might impose certain restrictions on materials that are content neutral, narrowly tailored, and leave open different channels for interaction.

Having previously determined in prior decisions that source code constitutes expressive activity, the court held that the encryption regulations were an unconstitutional prior restraint in violation of the First Amendment. In 1999, the Ninth Circuit Court voted to withdraw the three-judge panel opinion and rehear the case by the en banc court. In 2000, the court decided to remand the case to the district court in light of new encryption regulations adopted on January 14, 2000.

Although the opinion discussed above is no longer the law, it is relevant in light of the struggle over encryption export regulation because the issues of First Amendment rights related to such codes are as yet unresolved. The third case of the triumvirate, *Junger v. Daly* (1998/2000), illustrates this point. Junger, the plaintiff and a law professor, claimed that the export regulations violated his First Amendment right to free speech. The federal district court found that encryption software is functional rather than expressive; that the encryption source code is exported to transfer functions, not to communicate ideas. Therefore, the source code is not expressive under the First Amendment. The court reasoned that although exporting source code occasionally has communicative elements, that remains insufficient to extend First Amendment protections. The Sixth Circuit Court of Appeals reversed the decision and found that because computer source code is an expressive means for the exchange of information and ideas about computer programming, the First Amendment protects it. The case was remanded back to the district court to consider whether national security interests should outweigh the interests in allowing the free exchange of encryption source code.

All three cases highlight the difficulty the courts have in applying the Supreme Court's First Amendment analysis, set forth in the *United States v. O'Brien* (1968) test, to a complex technological problem. Encryption source code does not fit neatly under the traditional First Amendment categories of the written or spoken word, because it can be both expressive and functional. However, the Supreme Court has consistently held that First Amendment protection can extend to certain types of conduct or "symbolic speech," as it did in the *O'Brien* case.

Proponents of restrictions on the export of encryption, such as the federal government, law enforcement agencies, and the military, see encryption as a threat to national security. Some even favor regulation of domestic encryption, such as requiring people to automatically make copies of their encryption keys for deposit with the government or a designated third party. Law enforcement officials believe that the widespread availability of nonrecoverable encryption would severely impair their ability to fight crime and terrorism (McClure, 2000).

The First Amendment is also implicated when terrorists use the Internet to communicate criminal conspiracies among themselves. Although the free speech protection provided by the First Amendment may be the crown jewel of American democracy and civil liberties, courts will not allow terrorists to indiscriminately hide behind the First Amendment shield.

In *Brandenburg v. Ohio* (1969), the Supreme Court held that the First Amendment protects the right to advocate violence and other unlawful acts unless the advocacy is both directed toward inciting or producing imminent lawless action and likely to incite or produce such action. In *United States v. Barnett* (1982), the defendant claimed First Amendment protection for his printed instructions for the manufacture of PCP and other illegal drugs. Calling the defendant's argument "specious," the Ninth Circuit Court explained that the First Amendment did not provide a defense to a criminal charge in which the provider of information used only words to carry out his illegal purpose. The court stated that it was not necessary for the government to show that there was a personal meeting between the defendant and the drug manufacturer to prove the offense of aiding and abetting.

In *United States v. Mendelsohn* (1990), the court was also unwilling to extend First Amendment protection from aiding and abetting to computer software. Makers of computer software containing a bookmaking program claimed a First Amendment defense. The Ninth Circuit Court discussed the need for evidence showing that the speech involved was merely a form of communication that was distant from an immediate connection to the criminal act. Although computer programs receive First Amendment protection under other circumstances, the court believed the bookmaking program was so intimately connected with the execution of a criminal act (i.e., copyright infringement) that there was no entitlement to First Amendment protection. The First Amendment defense was not allowed when the words were more than mere advocacy but functioned as facilitating the actual crime.

In *Rice v. Paladin Enterprises* (1997/1998), relatives and representatives of three murder victims filed suit against Paladin Enterprises, the publisher of the book *Hit Man*. This book contains 130 pages of detailed instructions on how to commit a murder and how to become a "hit man" for hire. James Perry took the instructions to heart and murdered a woman, her quadriplegic son, and the son's nurse. The woman's ex-husband hired Perry to murder the family so that he could receive a $2 million settlement the son had received as a result of the accident in which he became paralyzed.

Although the lower district court held that the First Amendment protected Paladin Enterprises' publication of *Hit Man*, the Fourth Circuit Court of Appeals reversed this decision and held that the First Amendment did not prevent the finding that Paladin aided and abetted in the criminal act carried out by Perry. Additionally, the court noted that the Department of Justice had advised Congress that *Brandenburg v. Ohio* (1969) could not prevent the punishment of speech that involved aiding and abetting. According to the court, the text within *Hit Man* functioned as the preparation of a group of people for violent action and the encouragement of that action. The court concluded that someone could incite imminent lawless action not only through a call to action but also through speech that although advocating nothing, functioned as an instruction book for committing crimes.

There are a variety of difficult technological and legal issues facing law enforcement as it combats cyberterrorism. The law defined through court decisions and statutes is emerging as it responds to these new technological developments. Nevertheless, in America, the Bill of Rights continues to be the most viable framework within which the government, performing the delicate balancing of individual liberties and national security, battles threats of terrorism. Just as this country has wrestled with legal issues related to cyberterrorism, so have and so will other democracies. Many experts believe that one of the best cures for such debates are hard facts and empirical data on the extent of the problem. The next section grapples with this issue and offers a framework with which such data could be collected.

SUMMARY AND ANALYTICAL TYPOLOGY

As noted above, counterterrorism professionals have recently been faced with the reality of terrorists using advanced technology to hide their communications from prying eyes (Tenet, 2001). The prospect that terrorist organizations or in fact any group that could potentially evolve into a violent political movement could be using the Internet to advance their cause is not science fiction but reality. The reality is also that counterterrorism agencies are not organizationally prepared to defend against such advances in technology (Arquilla & Ronfeldt, 1996; Myers & Beatty, 2001). In fact and to date, discussions of cyberterrorism have not necessarily included digital steganography or many other forms of technological criminality as one of the terrorist forms that need to be addressed in policy or practice.

This section concludes the article with an administrative schema that may help organize the various cyberterrorism-related incidents that have already transpired and will continue to transpire. In this way, the actual frequency of events will start to become documented, the scope of the problem can be measured across time, and these empirical data can then be used to rationally inform policies designed to minimize the effects of cyberterrorism, even those varieties that have yet to be identified.

Using a similar approach to the construction of a database as that used by well-known terrorism and incident tracking typologies, we suggest that a secondary source–based analytical methodology be adopted. When researching the proposed cyberincident typology detailed below, we consulted various preexisting sources such as the *RAND Chronology of Terrorism Incidents*, the U.S. Department of Energy’s Safeguards Summary Events List, and organizational structures used by private security industry databases from such companies as Risks International (Ballard 1997; Fowler, 1981; Hoffman & Hoffman, 1996). The discussion herein focuses on three key areas: what variables are needed to track this form of terrorism, what selection criteria should be used for the secondary sources, and what categories could be used to facilitate this data collection and organization activity.

Variables that are selected to help track incidents of cyberterrorism should be articulated prior to any collection of data, and several are suggested below. All terrorist incidents encoded within the proposed data set should be categorized by use of a range of variables that will allow for relational analysis between the incidents. Each incident should be categorized by date, and each entry should include various data classifications commonly associated with terrorism research and cyberterrorism attacks. The following list of variables may be helpful in defining a data set: type of action or incident; tactics used; economic impact; fatalities involved; injuries that transpired; target of the attack by category; agency charged with preventing the attack; legal authorities violated during incident; nationality or race of targets; country where the attack transpired; country where the attack originated; characteristics of perpetrators; characteristics of victims; media source where data were gathered, actual and by category; verification of media sources by use of secondary reports; political or social motivation behind the attack; where support for the actions originated; technological platform; and other variables identified by experts. Updates to this list of variables should be made on a periodic and scheduled basis. Likewise, as to the actual incidents used as the data for such a typology, they must also be reviewed on a periodic and systematic basis because the initial reporting of the incident may contain inaccuracies, and the investigative facts can change over time.

Selecting which incidents to include in the database may be the most significant error-reducing, or error-introducing, decision facing researchers. To overcome the nationalistic myopia that infuses some data sets, the proposed database should include incidents of both a domestic (globally defined)[17] and an international nature. These include incidents in which the attackers were citizens of the country where the attack transpired and/or incidents in which attackers went beyond their national borders to perpetuate the attack, selected target victims with connections to a foreign state, or attacked infrastructure facilities in such a manner as to create an international incident.

Publicly available media sources that are chosen to supply the data entry process will likewise influence the quality of the data to be classified in the typology. The *RAND Chronology of Terrorism Incidents* uses publicly available sources such as newspaper reports. Although this choice may have been a good idea in the 1970s, when cyberculture was nonexistent, contemporary cybersociety demands a more inclusive methodology to locate acceptable information sources. Because cyberculture may well be reported, if not transpire, in a different medium, researchers should consider the need to open up the sources and possibly include underground Web sites, alternative and developmental technology reporting sources, and other sites where technological advancements and illustrative incidents may be reported while being missed by mainstream media outlets such as newspapers.

Given the many suggestions and limitations noted herein, it is reasonable to assume that the task of constructing a typology would be difficult, expensive, and time consuming. Next, we offer one typology designed to ignite the dialogue on what would be an effective methodology to study cyberterrorism. Anyone wishing to actually construct a working typology and start the collection of data in a systematic and longitudinal research effort may find this effort a mere starting point.

This typology has defined four categories and various subcategories from which a more detailed analysis could transpire. These four categories are information attacks, infrastructure attacks, technological facilitation of attacks, and fund raising and promotion of causes. Table 2 delineates these four categories, offers a definition of each, and coupled with the discussion below, suggests how various contemporary incidents could be incorporated within this analytical structure.

TABLE 2: Cyberincident Typology

Category	*Definition or Explanation*
Information attacks	Cyberterrorist attacks focused on altering or destroying the content of electronic files, computer systems, or the various materials therein.
Infrastructure attacks	Cyberterrorist attacks designed to disrupt or destroy the actual hardware, operating platform, or programming in a computerized environment.
Technological facilitation	Use of cybercommunications to send plans for terrorist attacks, incite attacks, or otherwise facilitate traditional terrorism or cyberterrorism.
Fund raising and promotion	Use of the Internet to raise funds for a violent political cause, to advance an organization supportive of violent political action, or to promote an alternative ideology that is violent in orientation.

Maybe the most commonly recognized form of cyberterrorism is the information attack, which can be defined as an attack focused on altering or destroying the content of electronic files, computer systems, or the various materials therein. Reporters, scholars, and counterterrorism professionals seem to focus on these activities not necessarily because of their potential for damage but rather because they are the most visible and widely reported events. Many individualized cases of online harassment, identity theft, online threats to schools, use of computer viruses, denial of service incidents, and other activities have been described as cyberterrorism (Associated Press, 2001; DiDio, 1998; Frazier, 2001a; Kwang, 2001; Lieberman, 2000). Considering the definitions of terrorism and how easily the label is appropriated by anyone wishing to vilify others, these assorted activities may have been categorized as cyberterrorism more out of ignorance than as a social scientific–based mythological application of operational definitions.

Researchers need to determine if the incidents thus classified actually represent cyberterrorism or if they would better be addressed as civil and legal matters. The primary consideration should be their motivation or intent. In many cases, the incidents commonly referred to as cyberterrorism may not reach this threshold simply because the intent or motivation was not social or political in nature. This observation supports the perspective of various commentators who have noted that many of the attacks being called cyberterrorism are nothing more than defacements and minor annoyances (Allen, Meserve, & Arena, 2001; Hunker, 2000).

The second form of cyberterrorism involves those attacks directed at seriously disrupting or destroying infrastructure. This includes attacks on the actual hardware, operating platforms, or programming in a computerized environment. Here, the effect of the attack may damage data, but the intent is more directed at destroying the systems, or any system, that control the data or computerized environment (Barger, 1996; Spiegel, 2001). Although some overlap exists with the first category, once again, incidents included herein should represent evidence that an attack had a larger purpose and intent.

Recent Web attacks between private citizens in the United States and China serve as illustrations. Hackers from both sides attacked information and infrastructure sites in the other country during a time of heightened political tension. These attacks focused on government Web sites, electric grid controls, and Internet service portals (Frazier, 2001b; Kwang, 2001). The reports indicate that what started as a data attack, or hacking, quickly escalated into a potentially more serious series of attacks. These follow-up infrastructure attacks had a far greater potential for social harm and economic impact than the original hacking.

The third category of cyberterrorism is not an attack per se but rather the use of the Internet to facilitate traditional terrorism or cyberterrorism. As noted in the section on steganography, this emerging trend is worrisome to counterterrorism professionals (Lesce, 1999). Louis Freeh, while still the director of the FBI, noted, "uncrackable encryption is allowing terrorists to communicate without fear of outside intrusion" (quoted in Kelley, 2001a, p. 7A). The CIA and the FBI agree that terrorists are using these technologies to facilitate planning and to disseminate information on how to conduct terrorist attacks (Kelley, 2001b, 2001c, 2001d; Sloan, 2001; Tenet, 2001). The encryption of messages, the use of steganography to hide plans, file sharing of information on how to plan attacks, the dissemination of information on violence rationales, and Web sites providing bombing information are just a few of the ways the Internet can be used to facilitate attacks.

The final category in the cyberincident typology reflects uses of the Internet to raise funds for a violent political cause, advance an organization supportive of violent political action, or to promote an alternative ideology that is violent in orientation. For example, many alternative political organizations, which may or may not support terrorism, have Internet presences (Grier, 2001; Piller, 2001; Roy, 2001). These commentators have suggested that these types of activities equate to the creation of virtual states, and these cybercountries could promote terrorism in both the real and virtual worlds. Likewise, incitements to violence and fund raising by alternative political organizations have the potential to offer justifications and financial support to terrorist attacks (Appel, 2001; Schlosberg, 2001). Although these activities do not necessarily reflect overt cyberterrorism, they do represent tacit planning and support. They should be considered important investigative facts when trying to affix a location for responsibility and ultimately for sanctions ex post facto to the incident.

Hoffman (2001), commenting on terrorism in general, noted that the collection of data may not be enough to counter cyberterrorists. Hoffman does support the idea of systematic terrorism research when stating that "an essential prerequisite to ensuring that our formidable resources are focused where they can have the most effect is a sober and empirical understanding of the threat coupled with a clear, comprehensive and coherent strategy" (p. 8). The lesson Hoffman was trying to impart is that data collection is not the be-all and end-all of counterterrorism.

Although the details above suggest the need for social scientific–based operationalization and systematic construction of an analytical typology to facilitate an empirical understanding, we agree with counterterrorism professionals and government reports that suggest that this effort will not be enough (Hoffman, 2001; U.S. General Accounting Offce, 2001). As suggested by these advocates, agencies interested in cyberterrorism need to pursue a coordinated and structured data collection and analysis process. These efforts need to be augmented by policies and laws designed to reduce the risk of attacks. In a similar fashion, researchers have noted that as a matter of economic survival, private business should also be involved in these efforts (Bridis, 2001).

Documenting and categorizing incidents, conducting longitudinal analysis of the scope of the problem and trends therein, and informing directed and coordinated cyberterrorism policies would not be enough to stop cyberterrorism. A comprehensive analysis of the cyberthreat should dovetail with a comprehensive national and international counterterrorism policy. Hoffman (2001) recently testified before Congress on the general terrorism threat and said,

> an effective counter terrorism policy is, however, no longer the question of more attention, bigger budgets and increased staffing that it once was: but of a need for greater focus, a better appreciation of the problem and firmer understanding of the threat. (p. 1)

The collection and analysis of data are important to assessing the risks and can provide a better appreciation of the issues. As demonstrated herein, those issues may be hard to define, have yet to be addressed in a legalistic manner, and can change as technology develops. Data sets can only act as guides for policy makers and counterterrorism professionals. Research, although important, is not a replacement for consistent and persistent vigilance by lawmakers, agency managers, and policy elites charged with countering the threats of terrorism. The data set managers who will run a cyberterrorism typology need this same level of vigilance to overcome the rapid changes in their analysis environment, to identify changes in the tactics used by those they study, and to help inform changes in the policy responses necessary to counteract cyberterrorism threats.

NOTES

1. Currently, the RAND organization continues to study terrorism, and several of its research fellows are focusing on *netwar*, their term for various activities including Internet-related acts of political opposition (Ronfelt, Arquilla, Fuller, & Fuller, 1998).

2. This definition includes the legalistic and definitional perspective generally promoted by the FBI.

3. References are given to document the history and technical aspects of cryptography, steganography, and watermarking. The discussion that follows was written for lay readers and designed to help them understand this technology.

4. *Digital watermarking* is also commonly used to describe the process of hiding information or security systems in a sound or image file.

5. As the casual reader will note, the lines of technological distinction between cryptography, steganography, and watermarking are not exactly clear. Likewise, legal authorities are having difficulty distinguishing these techniques from one another when enacting policies, and they generally legislate against encryption as a single technological method rather than against individual technologies.

6. Developments in digital watermarking or the legitimate hiding of verification information in the recording of music help illustrate several issues not discussed here. One recent challenge between a trade industry organization and Princeton researchers looking to hack into their "safely" guarded information is illustrative ("The RIAA's Low Watermark," 2001). Using reverse engineering techniques, the researchers were able to defeat the industry security systems. The point of this example is that technological innovations are open to misuse and abuse almost as quickly as products can be distributed by manufactures.

7. Bits and bytes are the basic building blocks of digital and computerized communications. Bits are a subset of bytes.

8. This technology does not work on every type of file one would encounter in a computerized environment.

9. Although the techniques are similar for audio and image files, the focus from here on will be on image files. Audio files will be mentioned only when relevant.

10. The GIF (graphics interchange format) format is commonly used to upload documents to the CompuServe Information Service and to pass files onto other types of computers. This highly compressed format, using Lempel-Ziv-Welsh compression, is designed to minimize file transfer times over phone lines. The GIF format supports only color-mapped images with fewer than eight bits. Although, not the most economical format available, GIF is the most common file format found on the Internet.

11. BMP (bitmap) is a file format commonly used on IBM-compatible PCs. BMP files can also refer to the IBM OS/2 bitmap format, which is a strict superset of the Microsoft Windows format.

12. Other techniques (e.g., direct sequence, frequency hopping, spread spectrum, etc.) represent major watermark embedding methods. These methods modify the noise value of a container. The direct-sequence technique adds noise to every element of a container. The frequency-hopping method selects a pseudorandom subset of a container's data to be watermarked (Zhao, Koch, & Luo, 1998).

13. For an excellent and comprehensive resource on cryptography, steganography, and watermarking, see Anderson and Petitcolas (1999).

14 JPEG (from Joint Photographic Experts Group) is a 24-bit graphic format. JPEG compression economizes the way data is stored and also identifies and discards "extra" data, that is, beyond what the human eye can see. Because the JPEG format discards data, the JPEG algorithm is referred to as lossy. This means that once a file is compressed and then decompressed, the result will not be identical to the original image. In most instances, the difference in an image is not distinguishable from the original.

15. Experts on steganography note that an image with large areas of solid colors is a poor choice because variations created from an embedded message will be more noticeable (Johnson, 1999).

16. The use of the United States as an example of the legal challenges posed by cyberterrorism reflects the fact that this country has a well-documented and ongoing legal debate on these subjects. Likewise, other countries are also engaging in similar legal debates, albeit with focuses on different civil liberty issues.

17. Incident tracking typologies often do not include these types of domestic events. This is a vestige of the era when terrorism was thought of as a threat only from abroad and not necessarily an internal problem. Events such as the Oklahoma City bombing forced researchers to recognize this as a problem and reconsider this operational choice.

REFERENCES

Allen, N., Meserve, J., & Arena, K. (2001, February 19). Law enforcement officials cite changes in types of domestic terrorism threats. *CNN Sunday* [Television broadcast]. Atlanta, GA: Cable News Network.

Anderson, R. J., & Petitcolas, F. A. (1999, August 13). *Information hiding: An annotated bibliography*. Retrieved June 7, 2001, from http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/Annotated_Bibliography.pdf

Appel, A. (2001, January 22). Police urge public caution in face of rising Internet crime. *The Jerusalem Post*, p. 4.

Arquilla, J., & Ronfeldt, D. (1996). *The advent of netwar.* Santa Monica, CA: RAND.

Associated Press. (2001, March 27). Teen is accused of making threat against school over Internet. *St. Louis Post-Dispatch*, p. A9.

Ballard, J. D. (1997). *Preliminary study of sabotage and terrorism as transportation risk factors associated with the proposed Yucca Mountain high-level nuclear waste facility.* Available from http:// www.state.nv.us

Ballard, J. D. (2000). *Terrorism and political policy: Crisis and policy making indicators in the media during legislative action*. Unpublished doctoral dissertation, University of Nevada, Las Vegas.

Barger, B. (1996, July 16). U.S. to prepare for cyber terrorism attacks, but is it necessary? *CNN.com*. Retrieved May 30, 2001, from http://www.cnn.com/US/9607/16/cyber.terrorism/

Becker, H. S. (1973). *Outsiders: Studies in the sociology of deviance*. New York: Free Press.

Bell, J. B. (1978). *A time of terror: How democratic societies respond to revolutionary violence*. New York: Basic Books.

Bernstein v. United States Department of State, 974 F. Supp 1288, 176 F.3d 1132 (9th Cir. 1999), *rev'd* 192 F.3d 1308 (9th Cir. 1999).

Beth, T., Frisch, M., Simmons, G. J., Goos, G. & Hartmanis, J. (Eds.). (1992). *Public-key cryptography: State of the art and future directions*. New York: Springer.

Brandenburg v. Ohio, 395 U.S. 444 (1969).

Brassard, G. (1988). *Modern cryptology: A tutorial*. New York: Springer.

Bridis, T. (2001, March 23). NSC chief urges US tech firms to protect computer networks. *The Wall Street Journal*, p. B2.

Bronskill, J. (2001, January 9). CSIS on alert for cyber saboteurs: Spy agency monitors threat to computer networks: Report. *Ottawa Citizen*, p. A3.

Collin, B. C. (1996). *The future of cyber terrorism*. Retrieved April 2000 from http://www.ascp.uic.edu/OICJ/CONFS/terror02.htm

Communications Assistance for Law Enforcement Act, 47 U.S.C. §§ 1001-1010 (1994).

Cooper, H.H.A. (1978). Terrorism: The problem of the problem of definition. *Chitty's Law Journal*, *26*, 105-108.

Currie, P. J., & Padian, K. (Eds.). (1997). *Encyclopedia of dinosaurs*. San Diego, CA: Academic Press.

Davern, P., & Scott, M. (1995). *Steganography: Its history and its application to computer based data files*. Unpublished manuscript, School of Computer Applications, Dublin City University, Ireland.

Denning, D. E. (2000). *Statement of Dorothy E. Denning*. Retrieved June 4, 2001, from http://www.house.gov/hasc/testimony/106thcongress/00-05-23denning.htm

Denning, D. E., & Denning, P. J. (1998). *Internet besieged: Countering cyberspace scofflaws*. Reading, MA: Addison-Wesley.

DiDio, L. (1998, April 27). Special FBI unit targets online fraud, gambling. *Computerworld*, 47-48.

Dreyfuss, R. (2000, September/October). The phantom menace. *Mother Jones*, 40-45, 88-91.

18 U.S.C. § 2518(1)(c) (1994).

Export Administration Regulations, 15 C.F.R. §§ 730-740 (1999).

Fowler, W. W. (1981). *Terrorism data bases: A comparison of missions, methods, and systems*. Santa Monica, CA: RAND.

Frazier, S. (2001a, April 27). Officials consider threat of cyberattack. *Daybreak* [Television broadcast]. Atlanta, GA: Cable News Network.

Frazier, S. (2001b, April 29). What can be done to prevent cyber terrorism. *CNN Sunday* [Television broadcast]. Atlanta, GA: Cable News Network.

Garland, D. (1990). *Punishment in modern society: A study in social theory.* Chicago: University of Chicago Press.

Glut, D. E. (1972). *The dinosaur dictionary.* Secaucus, NJ: Citadel.

Grier, P. (2001, February 16). A terrorist version of NATO? *The Christian Science Monitor*, p. 1.

Grossman, M. (1999, February 15). Cyber terrorism. *Computer Law Tip of the Week*. Retrieved May 30, 2001, from http://www.mgrossmanlaw.com/articles/1999/cyberterrorism.htm

Harris, L. (2001, February 7). Ben Venzke of iDefense discusses cyber terrorism. *Morning News* [Television broadcast]. Atlanta, GA: Cable News Network.

Herman, E. S., & Chomsky, N. (1988). *Manufacturing consent: The political economy of the mass media*. New York: Pantheon.

Hoffman, B. (1998). *Inside terrorism*. New York: Columbia University Press.

Hoffman, B. (2001). *Combating terrorism: In search of a national strategy.* Santa Monica, CA: RAND.

Hoffman, B., & Hoffman, D. K. (1996). Chronology of international terrorism 1995. *Terrorism and Political Violence*, *8*(3), 87-127.

Hunker, J. (2000, May 5). Jeffrey Hunker on cyberterrorists: The head of critical infrastructure at the National Security Council says the threat is real. *TechTV.* Retrieved May 19, 2001, from http://www.techtv.com/print/story/0,23102,2559742.00.html

Imai, H., & Zheng, Y. (2000). *Public key cryptography.* New York: Springer.

Johnson, N. F. (1999). *Steganography & digital watermarking: Information hiding*. Retrieved September 17, 1999, from http://ise.gmu.edu/~njohnson/Steganography

Johnson, N. F., Duric, Z., & Jajodia, S. (2000). *Information hiding: Steganography and watermarking—Attacks and countermeasures*. Boston: Kluwer Academic.

Johnson, N. F., & Jajodia, S. (1999). *Steganalysis: The investigation of hidden information*. Retrieved May 22, 2001, from http://www.ise.gmu.edu/~njohnson/pub/it98a.htm

Junger v. Daly, 8 F. Supp 2d 708 (N.D. Ohio 1998), *rev'd* 209 F.3d 481 (2000).

Kahn, D. (1996). *The codebreakers: The story of secret writing*. New York: Scribner.

Karn v. United States Department of State, 925 F. Supp 1 (D.D.C. 1996).

Katz v. United States, 389 U.S. 347 (1967).

Katzenbeisser, S., & Petitcolas, F. A. (2000). *Information hiding techniques for steganography and digital watermarking*. Norwood, MA: Artech House.

Kelley, J. (2001a, February 6). Terror groups hide behind Web encryption: Officials say sites disguise activities. *USA Today*, p. A7.

Kelley, J. (2001b, February 6). Terrorists use Web to mount attacks. *USA Today*, p. A9.

Kelley, J. (2001c, March 1). U.S. finds bin Laden an elusive target. *USA Today*, p. A1.

Kelley, J. (2001d, February 6). Web hosts terror traffic: Bin Laden linked to hidden messages. *USA Today*, p. 1A.

Kurak, E. & McHugh, J. (1992, November/December). *A cautionary note on image downloading*. Paper presented at the IEEE Computer Security Applications Conference.

Kwang, M. (2001, May 7). End hackers' war, urges China paper. *The Straits Times*, p. 4.

Lam, K. Y., Okamoto, E., & Xing, C. (Eds.). (1999). *Advances in cryptology.* New York: Springer.

Lemert, E. M. (1951). *Social pathology.* New York: McGraw-Hill

Lesce, T. (1999, September). Protecting critical infrastructures. *Law and Order*, 95-98.

Lesser, I. O., Hoffman B., Arquilla, J., Ronfeldt, D., & Zanini, D. (Eds.). (1999). *Countering the new terrorism*. Santa Monica, CA: RAND.

Lieberman, J. (2000, January 7). *Thompson/Lieberman—Authors of bill to protect against cyberterrorism comment on administration's plan protecting America from tech attacks*. Retrieved June 4, 2001, from http://lieberman.senate.gov/~lieberman/press/00/01/r011000a.html

Magid, L. J. (2001). *Kids' rules for online safety.* Retrieved June 10, 2001, from http://safekids.com/kidsrules.htm

McClure, D. (2000). Note: First Amendment freedoms and the encryption battle: Deciphering the importance of Bernstein v. United States Department of Justice, 176 F.3d 1132 (9th Cir. 1999). *Nebraska Law Review*, *79*(2), 465, 473.

McFeatters, A. (2001, March 21). Cyber enemy: America's newest threat is lurking behind computer screens. *Pittsburgh Post-Gazette*, p. E-3.

Mullendore, K., & White, J. R. (1996, March). *Legislating terrorism: Justice issues and the public forum*. Paper presented at the Academy of Criminal Justice Sciences, Las Vegas, NV.

Myers, L. J., & Beatty, P. T. (2001). Computer information systems and the high technology offender: The need for an interdisciplinary approach in higher education curricula. *ACJS Today*, *23*(1), 1, 4-6.

Nobel Foundation. (1972). *Nobel, the man and his prizes*. New York: Elsevier.

Omnibus Crime Control and Safe Streets Act, Title III, 42 U.S.C. § 3789(d) (1968).

Petitcolas, F. A., Anderson, R. J., & Kuhn, M. G. (1998). Attacks on copyright marking systems. In D. Aucsmith (Ed.), *Information hiding: Second international workshop* (pp. 219-239). New York: Springer.

Pfleeger, C. (1989). *Security in computing*. Upper Saddle River, NJ: Prentice Hall.

Piller, C. (2001, February 8). Terrorists taking up cyberspace: Web sites have become inexpensive, easily accessible tools for giving instructions to operatives and raising funds. *Los Angeles Times*, p. A1.

Pollitt, M. M. (2001). *Cyber terrorism—Fact or fancy?* Retrieved May 30, 2001, from http://www.cosc.georgetown.edu/~denning/infosec/pollitt.html

The RIAA's low watermark. (2001, July). *Wired*, 61-63.

Rice v. Paladin Enterprises, 128 F.3d 233 (4th Cir. 1997), *cert. denied* 523 U.S. 1074 (1998).

Ronfeldt, D., Arquilla, J., Fuller, G. E., & Fuller, M. (1998). *The Zapatista social netwar in Mexico*. Santa Monica, CA: RAND.

Roy, R. (2001, February 22). Letters to the editor. *The Statesman*.

Schlosberg, J. (2001, Winter). Judgment on "Nuremberg": An analysis of free speech and anti-abortion threats made on the Internet. *Journal of Science & Technology Law*, 52-78.

Schmid, A. P. (1988). *Political terrorism: A research guide to concepts, theories, data bases, and literature*. New Brunswick, NJ: Transaction.

Schneier, B. (1994). *Applied cryptography: Protocols, algorithms, and source code in C*. New York: John Wiley.

Schneier, B., & Banisar, D. (1997). *Electronic privacy papers: Documents on the battle for privacy in the age of surveillance*. New York: John Wiley.

Seberry, J. (1989). *Cryptography: An introduction*. Upper Saddle River, NJ: Prentice Hall.

Shea, V. (1994). *Netiquette*. San Francisco: Albion.

Sloan, W. (2001, February 9). Getting the message across: Hidden writing is a sensation. *Bangkok Post*.

Smith, C. (2000). Current U.S. encryption regulations: A federal law enforcement perspective. *New York University Journal of Legislation and Public Policy*, *3*, 11-20.

Spiegel, P. (2001, March 21). Terrorists plan havoc using Internet. *The Financial Times*, p. 11.

Steganography thumbprinting. (1998, January 26). *Phrack Magazine*, 23-26.

Tannenbaum, F. (1938). *Crime and the community.* New York: Ginn.

Tenet, G. J. (2001, February 8). *Interview transcript from the Cable News Network's (CNN)* Ahead of the Curve. Available from http://www.fdch.com

Thrasher, F. M. (1936). *The gang: A study of 1,313 gangs in Chicago* (2nd ed.). Chicago: University of Chicago Press.

United States v. Barnett, 667 F.2d 835 (9th Cir. 1982).

United States v. Giordano, 416 U.S. 505 (1974).

United States v. Mendelsohn, 896 F.2d 1183 (9th Cir. 1990).

United States v. O'Brien, 391 U.S. 367 (1968).

U.S. Department of Justice. (1995). *Terrorism in the United States*. Washington, DC: United States Department of Justice, Terrorism Research and Analytical Center, National Security Division.

U.S. Department of Justice. (1998). *Terrorism in the United States*. Washington, DC: U.S. Department of Justice Counterterrorism Threat and Assessment and Warning Unit, National Security Division.

U.S. Department of State. (1996). *Patterns of global terrorism*. Washington, DC: Author.

U.S. Department of State. (2000). *Patterns of global terrorism*. Washington, DC: Author.

U.S. General Accounting Office. (2001). *Comments on counter terrorism leadership and national strategy* (Document GAO-01-556T). Washington, DC: Author.

Van Der Leun, G., & Mandel, T. (1996). *Rules of the Net: On-line operating instructions for human beings*. New York: Hyperion.

Wayner, P. (1996). *Disappearing cryptography: Being and nothingness on the Net*. San Diego, CA: Academic Press.

White, J. R. (1998). *Terrorism: An introduction* (2nd ed.). Belmont, CA: Wadsworth.

Wieviorka, M. (1988). *The making of terrorism*. Chicago: University of Chicago Press.

Wilkinson, P. (1974). *Political terrorism*. New York: John Wiley.

Williams, H. C. (1986). *Advances in cryptology*. New York: Springer.

Woodcock, G. (1956). *Pierre Joseph Proudhon: A biography*. London: Routledge Kegan Paul.

Yahoo! Inc. (2001). *Terms of service*. Retrieved June 10, 2001, from http://docs/yahoo.com/info/terms

Zhao, J., Koch, E., & Luo, C. (1998, July). In business today and tomorrow. *Communications of the ACM*, *41*, 67-72.