Crime, Law & Social Change **34:** 259–273, 2000.
© 2000 *Kluwer Academic Publishers. Printed in the Netherlands.*

Redefining borders: The challenges of cybercrime [*]

DAVID L. SPEER
Marquette University, Political Science Department, Milwankee, WI 53201-1881, USA
(e-mail: david.speer@marquette.edu)

Abstract. Cybercrime is the newest security threat in the world today, and is distinct from any other threat facing the world. This paper attempts to place cybercrime in relation to other security threats, as well as illustrate the unique characteristics of cybercrime. First, an investigation of the major elements of cybercrime will be conducted. After the parameters of cybercrime have been laid out, cybercrime will be analyzed as a security threat on both domestic and international levels. Finally, current security structures will be examined for their effectiveness in controlling the threat posed by cybercrime.

Introduction

In the aftermath of the Cold War, domestic and international security agencies began to retool their focus towards transnational criminal threats such as drug trafficking and organized crime. However, none of their efforts have prepared the security structures and enforcement agencies to deal with the challenges posed by cybercrime. The instituationalized focus of security and law enforcement agencies on tracking the physical location and sources of security threats is a major impediment towards successfully combating cybercrime. More important, the exact nature of cybercrime remains underspecified in the policy and scholarly debates over the magnitude of the problem and its solutions.

Recently, the United States has taken steps to establish new security structures and upgrade existing structures, but these steps are just the beginning of what needs to be done. The impetus for this initiative has come from President Clinton, Janet Reno, and individuals that have witnessed the destructive power of cybercrime. Agencies involved in fighting cybercrime must look at three major factors. First, the nature of the cybercrime must be understood, as there are many different classifications of the crimes depending on the offender and the victim. Next, the crimes need to be understood in relation to how they fit into current means of analyzing a security threat. The final area is how security structures can best counter cybercrimes.

[*] I would like to thank my mentor Dr H. Richard Friman for his comments and support on this paper.

The nature of cybercrimes

Cybercrimes are activities in which computers, telephones, cellular equipment, and other technological devices are used for illicit purposes such as fraud, theft, electronic vandalism, violating intellectual properties rights, and breaking and entering into computer systems and networks. A term that is related to cybercrime is information warfare, which includes war-related activities carried out by individuals, organizations, and governments. These activities are implemented against the infrastructure and computer systems of other organizations and governments using the same skills and equipment that are used in cybercrimes (Cilluffo, Berkowitz, and Lanz 8, 1998). These two terms are often used synonymously, but are quite different. More importantly, applying the term information warfare to cybercrimes, often sensationalizes crimes that are unimportant on the levels of national or international security.

With these definitions in mind, it is necessary to examine the nature of the cybercrime. This section examines four major elements of cybercrime: the location of the criminal in relation to the crime, the victim, the offender, and what is being done to eliminate the threat. Addressing the nature of cybercrime is the first step towards comparing this issue to other security threats.

Location

The location of the offender in relation to the scene of the crime is the characteristic of cybercrime that differentiates itself most from others. In more traditional threats, the criminal is physically present at the crime scene. Therefore, enforcement officials can apprehend the criminal and bring him or her to justice. This is not the case with cybercrimes, as the criminal usually is not present at the crime scene thus making apprehension difficult. Not only are the offenders not present, but many times they are in another state or country. As a result cooperation between various enforcement officials is necessary. Recently, efforts have been made toward cooperation as illustrated by the apprehension of an Israeli hacker with the alias of “analyzer” who helped two teenagers in California interfere with military deployments in the Persian Gulf (Cilluffo, Berkowitz, and Lanz XV, 1998). However, cooperation can be inhibited by problems of jurisdiction and whether an enforcement agency will be able to cross borders in order to apprehend a criminal. Again the “analyzer” example illustrates this point because Israeli, not United States, authorities arrested this hacker (“Ehud Tenebaum” 1, 18 Mar. 1998).

Victims

Beyond the cooperation and jurisdictional difficulties faced by enforcement agencies is the problem of dealing with a large variety of victims of cybercrimes. The primary victims are governments and their various agencies, corporations, and organizations. These institutions each have different agendas that often times are opposed to each other, which hinders progress toward the common goal of elimination of cybercrime. Additionally, a large percentage of cybercrime is committed against individuals, but there has been limited emphasis on the individuals in conferences and summits, due to the fact that they have limited power and influence over governments.

Cybercrime legislation has been slowed by competing demands of the victims' lobbies. For example, the United States government has established the Federal Intrusion Detection Network or FIDNET which is an agency designed to fight cybercrime by monitoring government computers for security breaches. There have been attempts to centralize FIDNET under the Federal Bureau of Investigation (FBI). Organizations, corporations, and individuals are all very opposed to this type of control because they feel it would be an invasion of their privacy and has great potential for abuse. The reason these groups feel this way is because the access would be regulated by the FBI, which would "create a de facto 'desktop surveillance' network" (Markoff 1, 1 Oct. 1999). As a result of these strong feelings, many lobbyists are working against this type of law enforcement.

Additionally, each of these potential targets has internal protection and security enforcement measures already in place. For example, Sun Microsystems Incorporated has a company rule about their employees not having modems attached to their computers, to prevent hackers from breaking into the company network using an idle modem. This is such a serious threat that Sun will immediately fire anyone that breaks the rule ("Modem" 1, 18 Mar 1998).

Some firms are taking more drastic action against hackers by employing vigilante tactics. Many institutions, including major corporations and the Pentagon have installed counteroffensive computer programs. These programs will attack a hacker's computer once a breach of security has occurred. These types of programs fall into a gray area of legislation because they are not illegal, yet many law enforcement officials feel that these programs can cause more problems than they prevent. According to Schwartau, many law enforcement agencies unofficially say to these institutions, "We can't handle the problem. It's too big. If you take care of things yourself, we will look in the other direction. Just be careful." (8, 11 Jan 1999) Unfortunately, many hackers that fall victim to these programs often want revenge and will work even harder to destroy an institution's computer systems.

On an international level, the countries that are the most vulnerable to these threats are the United States, Japan, and member states of the European Union. At the time of this writing, very little data is available on the number of cybercrimes committed in these countries. An interesting paradox exists in these cases. These are the countries in the world that are the most reliant on computers and technological devices to support and control their infrastructures. This makes them the most vulnerable to cybercrime threats and information warfare. Yet because these countries have invested the most into their technological equipment, they also have the best security for these systems. Therefore, the less technological equipment a country has, the less vulnerable it is to this type of threat. Unfortunately, without this equipment it is virtually impossible to compete in the international economy.

Offender

The other part of the threat equation is the offender and his or her motives and intentions. This is one of the most unique areas of cybercrime. In some instances the criminal is a teenager trespassing on someone else's computer for fun or to prove themselves in the face of their peers. In other cases, the offender is an adult looking to vandalize computers or steal sensitive information and sell it. Conversely, the offenders in information warfare are governments or individuals acting against other governments and the target country's infrastructure. The intent of information warfare is national defense, or to weaken the opponent by disabling key computer systems.

Beyond clear examples of crimes such as these, there are many gray areas in cybercrime. For example, individuals and groups commit crimes that they may not know are crimes or may not understand the potential consequences of their actions. An example of this is people pirating software from a friend, this is particularly true with people that are new to the computer world. This illegal transfer of software occurs both over the telephone with the use of a modem or physically by exchanging diskettes. In this type of cybercrime, there is a very definite overlap with intellectual property rights and laws governing these rights. Therefore many new legal precedents must be set as well as new legislation to determine the proper punishment for these various crimes. Additionally, the international community needs to set standards for dealing with these crimes and how an offender in one country will be punished by the legal system in the victims' countries.

A related issue to the offender is the dual-use skills and abilities that are pocessed by many individuals that work for corporations and governments. The same skills are used to program a new and useful program as to program a virus designed to ruin entire computer networks. Therefore, it is very difficult to monitor individuals with the potential to commit cybercrimes. This is an area that many corporations and governments are extremely concerned about, because they employ individuals with these skills. Furthermore, a large portion of cybercrimes are committed by people inside an organization because it is easier to gain access to the system.

Eliminating the threat

These aspects of cybercrime have lead to discussions of the threat at a number of conferences dealing with transnational crime. Both the G8 and European Union have held conferences about international crime with cybercrime as an area of focus. These conferences have been surprisingly similar in the manner in which cybercrime is being discussed as well as the measures to prevent it. The most recent conference with cybercrime as a topic was the 1998 G8 summit in Birmingham, United Kingdom. This conference took most of its initiative from the 1997 G8 summit in Denver, Colorado. At the 1997 summit, many calls to action were primarily placed by the United States, but no treaty or agreement was signed (G8 Denver Summit, 1997). Once again, in the 1998 summit, nothing binding was signed by the participating countries because most of the participants were unwilling to delegate the authority of their domestic security structures (G8 Birmingham Summit, 1998). In both of these summits, the United States was the country arguing most strongly for a prohibition regime on cybercrime. These summits generated a list of ten steps that needed to be carried out by the participants, including modifying existing domestic regulations and working toward international standards and cooperation (Communiqué Annex Action Plan, 1, 1997). The United States is not the only country that is concerned about the new threats from technology. In 1995, the European Union held its own conference about setting up standards for dealing with cybercrime threats. These talks had obvious influence on the 1997 and 1998 summits, as the topics were very similar with cooperation internationally and among the member states being extremely important (EU Recommendation, 1995). In addition to the conferences held by countries are those held by corporations and organizations. The impetus for the conferences is the feeling that governments are not dealing with these threats in a timely manner. For example, the annual RSA Data Security, Inc. data security conference and expo is a forum for corporations, organizations, individuals, and government agencies to discuss security and encryption. Here, these actors attempt to initiate standards and develop norms for the security world (RSA Conference, 1999).

As a result of these conferences, new legislation is developing, as is a classification system for the various crimes. In the United States, the classification system consists of four classifications of cybercrimes and computer crimes. The first category is that of “computer as target”, here computers are the targets of crimes such as vandalism, trespassing, and information theft (Carter 1, 4 Nov. 1999). The information theft is the biggest concern for most corporations, as thefts of detailed plans about a new product's design or marketing campaign could ruin the company. Next is that of "Computer As the Instrumentality of the Crime", where the offender modifies the processes of a system or piece of equipment or alters a device's primary licit use to something illicit (Carter 2, 4 Nov. 1999). This type of crime mostly consists of fraud, and stealing information such as credit card numbers or cellular phone billing codes. Third are crimes that occur when the "Computer Is Incidental to Other Crime" (Carter 3, 4 Nov. 1999). In these cases, the computer is not necessary to commit the crime, but facilitates the process of committing the crime. Examples of this type of crime are money-laundering or the spread of child pornography over the internet. The final category of cybercrime, "Crimes Associated With the Prevalence of Computers", are crimes that are related to the computer and its peripheral equipment. This category covers software piracy, copyright violations, and counterfeiting of both software and hardware (Carter 4, 4 Nov. 1999).

With this new set of classifications, the United States has begun to establish an international prohibition regime which is a set of "norms and the processes by which they are enforced" on a global scale (Nadelmann 479, 1990). Nadelmann further argues that prohibition regimes are established only when crimes exhibit a "strong transnational dimension", excluding many types of crime which are left to the domestic enforcement agencies to handle (Nadelmann 481, 1990). Cybercrime fits quite well into the framework established by Nadelmann because it is a threat that exists in every country of the world that relies on computers. Furthermore, the perpetrators of these crimes are often in other countries than the scene of the crime creating a "transnational dimension". Nadelmann developed a set of five stages through which a prohibition regime must go through to be successful at eliminating a given problem or threat. Cybercrime falls into the third stage of this process. At this point the regime proponents, which include governments and moral entrepreneurs, begin to push for the "suppression and criminalization of the activity by all states and the formation of international conventions" (Nadelmann 485, 1990). Usually, the moral entrepreneurs, or the people that try to establish a prohibition regime, are individuals or members of nongovernment organizations. In the case of cybercrime, corporations join the list of moral entrepreneurs fighting against cybercrime because of the high level of risk that the corporations face. With corporations supporting the prohibition regime, it is likely that the regime will be established, if not succeed at its goal of eliminating cybercrime.

Analysis of the security threat

The single biggest factor in determining what does and what does not constitute a security threat are boundaries. These boundaries serve as indicators of what is secure or needs to be made secure. According to Lipschutz, these "boundaries are always under challenge and they must always be reestablished, not only on the ground but also in the mind" (224, 1995). Nowhere is this more true than in the realm of cyberspace, where new threats are constantly emerging and pushing boundaries of security. Until recently, many people did not consider cybercrimes a major threat, and as a result very little was modified in the security structures of the domestic and international complexes. Additionally, during the Cold War period the threats and their origins were known and understood (Lipschutz, 2, 1995). Now the problem lies in the fact that the source of the threat is unknown, as is the reasoning of the instigating actors.

For the analysis of cybercrimes and information warfare as a security threat, the pattern established by Buzan, Wæver, and de Wilde (1998) is useful. First, the cybercrime threat is a heterogeneous complex, that is a number of different actors are interacting in many different sectors. By comparison, in a homogeneous complex, the threat is confined to a few actors in one or two sectors. As a result, the dangers of cybercrime can come from any number of actors in numerous sectors ranging from military to societal sectors. Beyond the heterogeneous nature of the cybercrime complex, there is both an objective and a subjective threat embodied in this area. The objective threat has already been demonstrated by the numerous incidents of hackers breaking into the computers of governments, corporations, and organizations. The subjective threat is the basis for the information warfare arguments: that the potential for attack on key government and infrastructure systems is quite real.

The information warfare complex also has an objective side that has been demonstrated through tests conducted by governments working with hackers to test their computer systems. That hackers were able to enter the government and infrastructure systems suggests the potential to plant viruses or shut down the system entirely (Cilluffo, Berkowitz, and Lanz, 20, 1998). To this date, there has been very little information warfare, with the first incidents being practiced against the United States in the Persian Gulf, by the two teenagers in California in the "analyzer" example above. The number of information warfare attacks like this are growing. During the air raids on Kosovo, the United States "cyberwarriors" were trying to "drain the assets or alter banking records" of Slobodan Milosevic and other top officials. During this period the United States also detected many attempts to break into United States' computers (Becker 1, 1 Oct. 1999).

Beyond the heterogeneous versus homogeneous and objective versus subjective arguments there are the three major pieces of a security complex: referent objects, securitizing actors, and functional actors. The cybercrime threat fits into these three pieces, but there are some areas that are not fully covered by this typology. For Buzan, Wæver and de Wilde the referent objects, or the "things that are being existentially threatened", are generally states or nations (Buzan, Wæver, and de Wilde 36, 1998). In some cases the economy or the environment fit into their referent object category, but the authors fail to discuss the place of corporations and organizations. Corporations and organizations are frequent targets of cybercrimals, particularly from competing entities stealing research secrets and confidential information. This is a very clear example of an existential threat, therefore, the referent object category needs to be expanded to include more than just states, economies, and the environment.

Securitizing actors are "actors who securitize issues by declaring something – a referent object" (Buzan, Wæver, and de Wilde 36, 1998). Buzan, Wæver, and de Wilde's argument that government officials, lobbyists, bureaucracies, and other individuals are generally the securitizing actors fits well with cybercrimes. These actors usually have to speak in terms of international, national, or social security to have their message accepted, even if the threat would only affect a small portion of that population (Buzan, Wæver, and de Wilde 40, 1998). The terms international, national, and social security have to be used by some securitizing actors to amplify small threats. The threat may not affect the majority of the population, which would result in the issue not receiving the attention that the actor feels it deserves. This pattern extends itself into cybercrimes because these are the same actors that are trying to securitize computers, the internet, and the users of these devices. Lastly functional actors "affect the dynamics of a sector" (Buzan, Wæver, and de Wilde 36, 1998). This category includes those who try to enforce the laws and those that break the laws. This is the category that truly distinguishes the cybercrime threat from other possible security violations. Functional actors can be identified by their actions within a given sector. For example, in the drug threat, the movement of Pablo Escobar up through the ranks to kingpin of the Medellín cartel has been traced by many law enforcement officials and scholars. The functional actors in cybercrimes are not as easily identified. Obviously the control and enforcement officials and the victims of cybercrimes can be identified. The perpetrators of these crimes are very difficult to distinguish because they have many false identities that they use online. Therefore, when they are offline, the perpetrators have no connection to their online identities or crimes. Thus it is very difficult to identify, arrest, and prosecute these criminals. Additionally, many times the criminals act from areas outside the jurisdiction of many enforcement officials. This makes arresting the offender very difficult, especially given the fact that no international treaties have been signed to facilitate the capture of these criminals.

Security structures

Most law enforcement and security structures are directed toward physical security threats with very little, if any, focus on cybercrime or information warfare threats. This problem is occurring at domestic and international levels, with most existing governments and enforcement agencies being slow to react to the threat. On a domestic level, most governments have been slow to pass legislation specifically targeting cybercrimes. Currently, the governments of developed countries throughout the world have passed some legislation dealing with cybercrime, but this legislation is slow and this threat is very dynamic. For example, one of the most important pieces of legislation dealing with cybercrime in the United States is the Computer Fraud and Abuse Act of 1986, now fourteen years old. Furthermore, this act deals primarily with federal computers, leaving out privately owned computers and networks. Another is example is the Computer Misuse Act of 1990 in the United Kingdom. This piece of legislation is more comprehensive than the United States act above because it applies to all computers, rather than just federal computers. Unfortunately, this document is almost ten years old and speaks in generalities about computers. The crimes are moving faster than the legislation, thus loopholes in the legislation can be found, because the laws do not exactly apply to many of the crimes.

Beyond the slow and somewhat ineffective legislation are problems with the enforcement agencies. Many local police do not have the knowledge nor the equipment necessary to enforce laws against cybercrimes. In many national enforcement agencies the cybercrime department has just recently been started or does not exist at all. The United States Federal Bureau of Investigation has a cybercrime unit that has been growing continuously since its inception. Recently, the FBI asked for $74 million to improve their information technology equipment as well as train more agents to effectively fight cybercrime (Tillett, 1, 24 March 1999). In Great Britain, the National Crime Intelligence Service is launching a cybercrime squad, that will be assisted by the MI5 Intelligence service and the GCHQ, the British spy center. This squad will fight against computer aided money laundering, fraud, and will share information about hacking, pedophilia, and counterfeiting (NCIS, 1, 17 Jan 2000). Cybercrime departments in enforcement agencies are not only occurring in developed nations, but also in developing nations. For example, in India the Central Bureau of Investigation (CBI) is introducing the Information Technology bill to “help check computer crime and legalize electronic transactions” (India, 1, 25 Feb 1999). Moreover, Indian officials realize that they are behind in adopting computer systems, but want Indian enforcement agents to be able to effectively use a computer and fight cybercrime in the future. Furthermore, these organizations have limited staffs that cannot track all the cybercrimes that have been committed. To avoid this problem the United States Securities Exchange Commission (SEC) has obtained the help of 125 volunteer agents that will help investigate potentially fraudulent activities. Additionally, the SEC relies on other individuals and institutions to provide approximately 120 tips per day about activities and individuals that need to be investigated (Woody, 1, 16 Nov 1998).

Internationally, the security structures to combat cybercrime are worse than those at the domestic level. The international security structures are virtually non-existent because the high levels of cooperation between countries necessary have not been forthcoming. To apprehend many of the more dangerous criminals, international cooperation is vital. Countries around the world see that this cooperation is necessary, and, as mentioned above, have been holding conferences. Loose agreements are the only thing that have come of these conferences thus far because cooperation infringes upon state power and sovereignty. Governments realize that as the world becomes more interdependent, they will lose more of their sovereignty to international organizations and treaties. Therefore, opposition to cooperation is prevalent, but as the cybercrime threat continues to grow, more agreements and cooperation will occur. One of the few examples of international cooperation is between the United States and India. The United States has been helping India establish a cybercrime division in the CBI (“India”, 1, 25 Feb 1999).

At this point in time, cybercrime is seen as a lesser threat on the international level, much like the threats presented by money laundering and trafficking in women for the international sex trade. These three types of transnational crime, all are growing in importance and the level of attention that they command, yet are still not on the same level of importance as arms trafficking and the drug trade. When cybercrime becomes a greater threat, most likely due to a major incident or attack, the level of cooperation will increase. Cybercrime will then be more comparable to the drug trade or trafficking arms, both of which command much greater levels of international cooperation.

Many things need to be done in order to improve the security structures so that they will be effective in combating cybercrime. Domestically, the most necessary improvement to the system would be funding. With additional funding security agencies and local police would be able to buy new equipment and train officers to handle cybercrime threats. This necessary funding is now just beginning to be provided as the number of cybercrimes continues to increase at a rapid rate. For example, the United States is now giving scholarships for students studying information technology and computer security. In exchange for the scholarships, the students will work for the federal government in the Federal Cyber Services division for a set period of time (Brewin, 1, 17 Jan 2000).

When increasing enforcement agencies, the potential for corruption also increases. The number of officers fighting cybercrime that will become corrupt is much lower than with other criminal activities, such as drug trafficking, because there is much less money involved in cybercrime. Furthermore, education of the civilian population about what is and is not legal when dealing with computers is necessary. With an educated population, less ordinary people would commit cybercrimes, thus reducing the work load for the national agencies. Not only would the work load be reduced, but the gray areas surrounding cybercrimes would also be lessened.

Internationally, the single biggest improvement to the security structure would be working multilateral agreements, particularly between the developed nations. These multilateral agreements would allow for high levels of cooperation between countries and their enforcement agencies. Additionally, many of the jurisdiction difficulties between countries would be eliminated. The first example of a multilateral agreement is beginning to take shape in the European Union with the data privacy directive. This directive is designed to establish “a common regulatory framework for data transmission, to ensure both a high level of privacy for the individual and free movement of data within the EU (de Bony, 1, 17 Jan 2000).” By October 1998 all fifteen member nations were to have implemented this directive, but only six of the nations met this deadline. Another four nations complied by August 1999. France, Germany, Ireland, Luxembourg, and the Netherlands all have yet to implement the directive, as a result, the European Commission is taking these countries to the European Court of Justice to have the matter resolved. The lack of implementation by some of the most powerful countries in the European Union illustrates some of the difficulties with establishing multilateral agreements dealing with cybercrime.

Another possibility to enhance the security structure would be an international organization dealing specifically with cybercrimes. This type of organization would possibly be an extension of the United Nations (UN), the North Atlantic Treaty Organization (NATO), Interpol, or would be independent. Such an organization would help facilitate cooperation in the apprehension of cybercriminals and building secure computer networks. If the organization was part of the United Nations, it would often be bogged down by the politics of competing nations within the UN, and not be as effective as possible.

Additionally, this organization does not seem as though it would have a place within the UN. A more positive aspect of being part of the UN would be the jurisdictional reach the structure would have in all parts of the world. If such a security structure was part of NATO, it would be much more limited in jurisdictional reach given fewer countries are NATO members. Additionally, many governments might be concerned about the fact that NATO is a military organization and the potential for abuse of sensitive information and power for military or other purposes would exist. If the concerns about abuse could be overcome, this structure could become quite effective because of the resources available to it through NATO. Interpol would be the best choice for the structure because the jurisdictional reach would be large and the concerns about military abuse of information would not be an issue. If such a security structure was independent, it would face many difficulties because few governments would trust a new organization. Therefore, much of the organization's initial years would be spent building political trust and clout rather than serving as a means to deter cybercrime.

The CERT® Coordination Center at Carnegie Mellon University has been working with the United States government and many corporations since 1988 after a cybercrime has been committed. This organization was initially a computer incident response unit. An incident is defined by the organization as "the act of violating an explicit or implied security policy" (CERT (4) 6 Dec. 1999). The CERT® Coordination Center has now branched out beyond this task to help start other incident response teams and coordinate large scale operations between many teams. Additionally, this team has been researching the causes and prevention methods of security vulnerabilities, as well as improvement of security systems. This organization could be an example from which to build an international security complex. Furthermore, the need for such an organization is very evident by looking at statistics produced by the CERT® Coordination Team. In 1988, the team handled six incidents, ten years later in 1998 they dealt with 3,734 incidents. This number has almost doubled in the first three quarters of 1999, with 6,844 incidents handled (CERT (3) 6 Dec. 1999).

Conclusion

Unfortunately, most of the necessary modifications and additions to the cybercrime security structure will not occur until after a major attack on a government system takes place. A large number of attacks on critical corporations and industries within a country also could trigger support. If these attacks occur, it would be very difficult to build an effective defense because many new perpetrators would attack after seeing that there is a poor defense system. The damage that would have to be done to the government or corporations of a country would have to be devastating, causing a shut down in the computer systems of the victim to generate the support to build a security structure. The necessary levels of destruction, damage, and loss of valuable resources to bring cybercrime to the forefront of security threats is nearing. In 1999 spending on eradication and protection against computer viruses as well as lost productivity around the world totaled $12.1 billion (Fonseca, 1, 18 Jan 2000). As figures like these continue to grow, more countries will take notice and start taking more action against cybercrime. Additionally, once one or two developed nations establish strong security structures, many other countries will follow their lead and develop their own structures. Again, this would further assist cooperation between nations. After a major attack has transpired, funding will become readily available for building a strong security structure. Until that time, funding will continue to be limited, as will support for the agencies currently fighting the cybercrime threat.

The new threats of cybercrime and information warfare have not yet become a major security issue in most countries. In the near future, as the threat grows and more examples of cybercrime and information warfare are seen, this will become a major security issue. When governments and corporations take this threat seriously, many resources will be directed toward eliminating it. These resources should be used to modify existing security structures and create new ones. Additionally, the resources must be used on an international level to create multilateral agreements between nations about cooperation and jurisdiction issues. Not only must these areas be addressed, but efforts must be put forth to understand why these criminals commit these crimes, and what measures can be taken to stop them. Overall, the threat of cybercrime is very large now, and will only continue to grow as more of the world becomes knowledgeable about computers and other technological equipment. This threat can be curbed now in its early phase, or later when the threat is much larger. This depends on what actions the governments and corporations of the world decide to take now.

References

Becker, Elizabeth, “Pentagon Sets Up New Center for Waging Cyberwarfare,” *New York Times* 1 Oct 1999.

Brewin, Bob, “Government Wooing Best and Brightest for Cyberdefense Mission,” *Federal Computer Week* 17 Jan 1999.

Buzan, Barry, Wæver, Ole, and de Wilde, Jaap, *Security: A New Framework for Analysis* (Boulder, CO: Lynne Rienner Publishers, 1998).

Carter, David L., *Computer Crime Categories: How Techno-criminals Operate*. Accessed 4 Nov. 1999. http://nsi.org/Library/Compsec/crimecom.html.

CERT® Coordination Center, Homepage and other pages. Accessed 6 Dec. 1999. (1) http://www.cert.org, (2) www.cert.org/nav/aboutcert.html, (3) www.cert.org/stats/cert_stats.html, (4) www.cert.org/tech_tips/incident_response.html.

Cilluffo, Frank J., Berkowitz, Bruce D., Lanz, Stephanie, *Cybercrime . . . Cyberterrorism . . . Cyberwarfare . . .: Averting an Electronic Waterloo* (Washington, D.C.: The CSIS Press, 1998).

Computer Fraud and Abuse Act 1986 (US) 18 USC 1030. Accessed 7 Dec. 1999. http://www.austlii.edu.au/au/other/crime/123.html.

Computer Misuse Act 1990 (UK) Accessed 7 Dec. 1999. http://www.austlli.edu.au/au/other/crime/125.html.

de Bony, Elizabeth, *EC Takes Countries to Court on Data Privacy* 17 Jan 1999. Accessed 18 Jan. 1999. http://www.idg.net.

Denning, Dorothy E., *Information Warfare and Security* (New York: ACM Press; Reading, MA: Addison-Wesley, 1999).

Ehud Tenebaum (AKA "analyzer") Arrested in Israel Associated Press 18 Mar 1998.

European Union, Committee of Ministers to the Member States. "Recommendation No. R (95) 13" 11 Sept 1995. http://www.usdoj.gov/criminal/cybercrime/cryoe.htm .

Federal Bureau of Investigation Nation Computer Crime Squad. Home Page. Accessed 4 Nov. 1999. http://www.fbi.gov.

Fijnaut, Cyrille, Marx, Gary T. *Undercover: Police Surveillance in Comparative Perspective* (The Hague: Kluwer Law International, 1995).

Friman, Richard H., Andreas, Peter, *The Illicit Global Economy and State Power* (Lanham: Rowman & Littlefield Publishers Inc., 1999).

Fonseca, Brian. "$12.1 billion reportedly spent to ward off computer viruses in 1999," *InfoWorld* 18 Jan 1999.

G8 Birmingham Summit 1998. Homepage. Accessed 4 Nov 1999. http://www.g8summit.gov.uk/

G8 Denver Summit 1997 document, *Communiqué Annex: Action Plan to Combat High-Tech Crime* Accessed 4 Nov 1999. http://www.usdoj.gov/criminal/cybercrime/action.htm.

G8 Denver Summit 1997 document, *Communiqué Annex: Principles to Combat High-Tech Crime* Accessed 4 Nov 1999. http://www.usdoj.gov/criminal/cybercrime/principles.htm.

"India to Police Internet Abuse, Cyber Crimes," *Reuters* 25 Feb 1999.

Joubert, Chantal, Bevers, Hans, *Schengen Investigated* (The Hague: Kluwer Law International, 1996).

Lipschitz, Ronnie D., *On Security* (New York: Colombia University Press, 1995).

Markoff, John "New Center Will Combat Computer Security Threats," *New York Times* 1 Oct 1999.

Meeting of the Justice and Interior Ministers of the Eight December 9–10, 1997, *Communiqué* Accessed 4 Nov 1999. http://www.usdoj.gov/criminal/cybercrime/communique.htm.

"Modem on the Desk Earns a Pink Slip at Sun," *Network Week* 18 Mar 1998.

Nadelmann, Ethan A, *Cops Across Borders: the Internationalization or US Criminal Law Enforcement* (University Park, PA: Pennsylvania State University Press, 1993).

Nadelmann, Ethan A, "Global Prohibition Regimes: the Evolution of Norms in International Security," *International Organization* Autumn 1990, 479–526.

Platt, Charles, *Anarchy Online: Net Crime/Net Sex* (New York: HaperPaperbacks, 1996).

RSA convention, Homepage. Accessed 4 Nov 1999. http://www.rsa.com/conf99/overview.html.

Schwartau, Winn, "Striking Back Corporate Vigilantes go on the Offensive to Hunt Down Hackers," *Network World* 11 Jan 1999.

Tillett, L. Scott, "IT Key to FBI's Future," *Federal Computer Week* 24 Mar 1999. http://www.idg.net accessed 19 Jan 2000.

"UK Reportedly to Launch National Cybercrime Squad," *Reuters* 17 Jan 1999.

Woody, Todd, "The SEC's Internet Ranger John Reed Stark, Internet Enforcement Chief, Surfs the Web for Scams," www.thestandard.com 16 Nov. 1998. Accessed 18 Jan. 1999.