GLOBAL NATURE OF COMPUTER CRIMES
AND THE CONVENTION ON CYBERCRIME

Dr. M. Yasin ASLAN*

ABSTRACT

This article explains the global nature of computer crime and the “Council of Europe Convention on Cybercrime.” The nature of computer crime makes it too difficult for law enforcement to effectively combat the problem. Traditional model of law enforcement is not an effective strategy for dealing with computer crime. While “cyber crime” alters assumptions about the relationship between internal order and external threats, it is important to examine the computer crimes and international approaches to computer crime enforcement.

ÖZET


Keywords: Cybercrime, computer crime, Council of Europe Convention on Cybercrime, law enforcement.

* Hâkim Binbaş, Genelkurmay Başkanlığı Adli Müşaviriği, Uluslararası Hukuk İşleri Ş.Md. (Judge (Major), International Law Department, Office of the Legal Advisor to the Turkish General Staff).
I. INTRODUCTION

Computer crimes present unique problems due to the global nature of the Internet. On the Internet, where borders are meaningless, we are vulnerable to criminals from all over the world.¹ The Internet’s disregard of national borders poses significant difficulties for law enforcement officials who must operate within national borders while attempting to prosecute computer crimes.² It is apparent that an adequate global uniformity cannot be achieved in national laws because computer crime laws are still lacking in many countries in Africa and Asia. Many developing countries lack the necessary technical infrastructure and subsequent computer use among their populations.³ Computer crime simply cannot be a priority issue because it is not considered a problem or even a potential problem particularly in those countries.

It sometimes may be beneficial for a nation to become a computer crime haven. For example, many of the former Soviet Republics are already major de facto computer crime havens.⁴ Criminals may capture the political process with threats or bribes, making the local national government unable to pass the appropriate legislation. A country may also choose to become a computer crime haven in order to secure large aid awards from the United States and other industrialized nations. A nation with such aims could hope to receive millions in aid to wage a war on computer crime.⁵

Cyberspace makes physical location irrelevant.⁶ It is as easy to victimize someone who is halfway around the world as it is your next-door neighbor. There is currently no effective way to police cyberspace because our experience

³ AMERICAN BAR ASSOCIATION, INTERNATIONAL GUIDE TO COMBATING CYBERCRIME 5 (2003) (noting that, high-income countries averaged just over three Internet users per ten people in their population, while low-income countries averaged far below one in twenty).
⁵ Id. (mentioning Colombia which receives considerable aid in the United States’ war on drugs).
with computer crime is still very low. Given the nature of the cyberspace, computer crime requires developing a new model of law enforcement.

This article discusses the global nature of computer crime and the “Council of Europe Convention on Cybercrime.” The nature of computer crime makes it too difficult for law enforcement to effectively combat the problem. The traditional model of law enforcement is not an effective strategy for dealing with computer crime. While “cyber crime” alters assumptions about the relationship between internal order and external threats, it is important to examine the computer crimes and international approaches to computer crime enforcement.

II. GLOBAL NATURE OF COMPUTER CRIME

A. Defining Computer Crime

In general, “computer crime” is a crime where a computer system itself is the target. Computer crime can be defined as any violation of criminal law that involves knowledge of computer technology for its perpetration, investigation, or prosecution. Because of the diversity of computer-related offenses, a narrower definition would not be adequate. Most countries have not defined what computer crime is and how it differs from real-world crime. However, there has been a dramatic increase in specialized legislation to combat these new criminal behaviors. Computer crimes can be charged under at least forty different federal statutes in the United States.

The traditional model of law enforcement assumes real-world crime. One characteristic of real-world crime is that the victim and the perpetrator must be

---


9 For the purposes of this paper, the term “computer crime” will be used to include both “computer crime” and the interchangeable term “cyber crime.”


12 Id. at 301.

in relatively close physical proximity when the crime is committed. However, in cyberspace there is no crime scene in the traditional sense. For most computer crimes, evidence is scattered over several locations, including the computer the perpetrator used, the victim’s computer and the intervening computers and computer servers the perpetrator used to accomplish the offense.

Computer crime is not a distinct type of crime, such as rape or murder. Computer crime denotes the use of computer technology to achieve illegal ends. The term “computer crime” includes traditional crimes committed with the use of a computer. The rapid emergence of computer technologies and the exponential expansion of the Internet have spawned a variety of new, technology-specific criminal behaviors that must also be included in the category of “computer crimes.”

Computer crime is a borderless crime. It can be committed against a victim who is in another city, another state, or another country. All a perpetrator needs is access to a computer that is linked to the Internet. The perpetrator needs no passport and passes through no checkpoints as he commits his crime. Automation gives perpetrators the ability to commit many computer crimes very quickly. The constraints that govern action in the physical world do not restrict the perpetrators of computer crime.

**B. Types of Computer Crime**

Computer crime essentially encompasses two types of unlawful activity. First, computer-related crime consists of conduct that targets a computer or a computer system. Attacks on networks, including hacking, denial of service

---

15 Smith, supra note 2, at 46.
16 Brenner, supra note 7, at 75.
17 Ferrera, supra note 11, at 302.
19 Smith, supra note 2, at 48.
20 Brenner, supra note 7, at 65.
21 Id. at 66.
attacks, and virus dissemination, fall into this category. In this category, the computer is akin to the pedestrian who is mugged or the house that is robbed - it is the subject of the attack and the site of any damage caused. Second, computer-enabled crime is a traditional crime like fraud or theft that is facilitated by a computer. A computer may be an “instrument” used to commit traditional crimes such as identity theft, child pornography, copyright infringement, and mail or wire fraud.

1. Computer-related Crimes

a. Hacking

“Hacking” can be defined as gaining unauthorized access to a computer system either for the purpose of exploration or for causing damage once inside. This involves using technology to gain unauthorized access to a computer system, program, or data.

b. Viruses, Worms, Trojan Horses, Logic Bombs, and Sniffers

A “virus” is computer code, generally disseminated by email, which causes a computer to perform certain functions that range from annoying to very destructive. A virus modifies other computer programs, causing them to perform the task for which the virus was designed. It is usually spread from one host to another when a user transmits an infected file by e-mail, over the internet, across a company’s network, or by disk. For example, the “Melissa virus” disrupted e-mail service around the world when it was posted to an Internet newsgroup on March 26, 1999.

“Worms” are similar to viruses, but, whereas viruses require human action in order to spread from one computer to the next, worms use computer networks or the Internet to self-replicate and “send themselves” to other users, generally

---

22 Lewis, supra note 4, at 1355.
23 American Bar Association, supra note 3, at 34.
24 Carter & Perry, supra note 13, at 314-18.
25 Brenner, supra note 7, at 73.
26 Lewis, supra note 4, at 1354.
27 Id. at 1355.
28 Loundy, supra note 14, at 55.
29 Smith, supra note 2, at 54.
via e-mail. worms have far more destructive potential than viruses; the “iloveyou” worm spread nine times faster than the “melissa virus” as a result of its self-replication capability.

“trojan horses” are programs that have legitimate functions but that also contain hidden malicious code. like its namesake, a trojan horse dupes a user into installing the seemingly innocent program on his or her computer system. then it activates the hidden code, which may release a virus or allow an unauthorized user access to the system. the “iloveyou” worm was delivered by trojan horses in the form of seemingly innocent e-mail attachments.

“logic bombs” are programs that are activated by a specific event, such as the arrival of a particular date or time. they can be destructive, but are also commonly used by software companies to protect against violation of licensing agreements by disabling the program upon detection of a violation.

“sniffers,” also known as network analyzers, are used to monitor networks and troubleshoot network connections. sniffers can help network administrators find and resolve network problems. however, a hacker can break into a network and install a sniffer that logs all activity across a network including the exchange of passwords, credit card information, and other personal information.

c. denial of service attacks

these attacks generally involve swamping a computer system’s servers with millions of false authentication requests in order to use up the available capacity of the target system, thus denying legitimate users access to the site. distributed denial of service attacks are designed to “crash” websites by

30 loundy, supra note 14, at 55.
31 american bar association, supra note 3, at 13.
32 id.
33 id.
34 id.
35 loundy, supra note 14, at 55.
36 steven branigan, high-tech crimes revealed 292 (2005).
37 id.
38 ferrera, supra note 11, at 306.
preventing them from communicating with other computers and use the networks of innocent third parties to achieve this goal.39

d. Cyberterrorism

Cyberterrorism involves a politically-motivated attack against a computer system in order to directly inflict harm upon a civilian population or indirectly aid the carrying out of a terrorist plan.40 For example, a cyberterrorist might break into the computer system of a power company and shut down a power grid and may use Internet technology to obtain illegal money or documentation in furtherance of a terrorist act against the United States.41

2. Computer-Enabled Crimes

a. Fraud and Theft

Fraud and identity theft are common types of computer-enabled crime, but are only some of the threats posed by computer crime and computer-enabled crime.42 The tempting volume of information stored on the Internet makes the networked computer a natural fit for identity theft.43

b. Child Pornography

This category of computer crime may be committed in two ways: by disseminating child pornography over the Internet44 or by using a computer to entice children into meetings for illicit sexual encounters.45

III. Lack of Efficient Law Enforcement Models

Computer crimes are difficult to prosecute due to both the nature of the technology itself and the relative unfamiliarity of law enforcement with the technology. The nature of the Internet allows people to engage in criminal conduct on-line with virtual anonymity. With respect to computer crimes such

39 CLIFFORD, supra note 10, at 7.
40 FERRERA, supra note 11, at 307.
41 MARTIN C. LIBICKI, WHAT IS INFORMATION WARFARE 78 (1996).
42 FERRERA, supra note 11, at 304.
43 Lewis, supra note 4, at 1372.
44 Id. at 1356.
45 SMITH, supra note 2, at 136.
as hacking, a victim may never even realize that she was a victim of a computer crime. Further impeding law enforcement, many private and commercial entities who do detect an intrusion are fearful to report offenses due to potential negative publicity.46

Computer crimes can be committed instantaneously and therefore require a rapid response. However, law enforcement agencies are burdened with cumbersome mechanisms and are accustomed to dealing with real-world crimes, “the investigation of which proceeds at a more deliberate pace.”47 The transborder nature of computer crime further enhances the difficulties officers face when they attempt to react to a computer crime because “traditional assumptions about a perpetrator’s being observed preparing for, committing and/or fleeing from an offense no longer hold.”48

Cyberspace also lets perpetrators conceal or disguise their identities in a way that is not possible in the real world.49 Even if police can identify a perpetrator, gathering evidence of the computer crime can be difficult because the country that hosts the cybercriminal and his activities may not define what he did as illegal and may therefore be unable to prosecute him or cooperate in his extradition to prosecute elsewhere.50 The host nation also may not have agreements in effect with the victim nation which obligate it to assist in gathering evidence that can be used against the perpetrator.51 The evidence may have been destroyed advertently or may have not retained by the “Internet Service Provider (ISP)” which the offender used to commit his crime.52

All nations continue to struggle with defining computer crimes and developing computer crime legislation that is applicable to both domestic and international audiences.53 Worldwide, national governments are adopting computer-specific criminal codes that address unauthorized access and

46 Carter & Perry, supra note 13, at 327 (noting that the FBI uses a device called Carnivore, which is a special filtering tool that may be used to gather the information authorized by a court order, and no other additional information, to intercept Internet communications).

47 Brenner, supra note 7, at 69.

48 Id.


50 AMERICAN BAR ASSOCIATION, supra note 3, at 88.

51 Brenner, supra note 7, at 70.

52 EOGHAN CASEY, DIGITAL EVIDENCE AND COMPUTER CRIME 15 (2nd ed. 2004).

53 LOUNDY, supra note 14, at 690.
manipulation of data similar to the “Computer Fraud and Abuse Act of 1996” in the United States. In addition to the criminalization of new computer offenses, many nations are facing the problem of the “computerization” of traditional offenses. Every country has enacted some form of computer-specific legislation. However, jurisdictional problems arise for domestic prosecutors when the acts are committed outside of a country because the jurisdictional rules of criminal law require the prosecutor to prove that the defendant intended to cause harm within his country.

The rapid evolution of computer networks and information technology poses the first obstacle to efforts to globally harmonize domestic computer crime laws. Differences in certain substantive values pose a potential impediment to enacting harmonized domestic laws on computer crime. Furthermore, even if nations pass laws harmonizing their criminalization of certain computer activities, they may still utilize different standards for conviction and impose different punishments upon conviction. This discord is foreseeable because computer crimes in a more industrialized nation will have greater ramifications than in a less industrialized nation.

Another difficulty impeding solutions that rely on international coordination is the failure of many countries to commit adequate resources to fighting computer crimes. It is not enough to get the laws on the books; there must be adequate domestic resources within each nation to enforce those laws. Law enforcement agencies often have been reluctant to marshal adequate resources to fight the rising threat of computer crime.

54 FERRERA, supra note 11, at 308.
55 Id. at 327.
56 Id. at 322.
57 Carter & Perry, supra note 13, at 359.
58 CLIFFORD, supra note 10, at 174.
59 SMITH, supra note 2, at 105.
60 Lewis, supra note 4, at 1360.
61 AMERICAN BAR ASSOCIATION, supra note 3, at 48.
62 Id. at 87.
63 Lewis, supra note 4, at 1361.
Given the global nature of computer technology, purely domestic solutions are inadequate because cyberspace has no geographic or political boundaries and many computer systems can be easily accessed from anywhere in the world. In addition, the development of sophisticated computer technology has enabled organized crime and terrorist groups to bypass government detection and carry out destructive acts of violence.

It is already apparent that the traditional model of law enforcement cannot deal effectively with computer crime. Prosecution is not always an effective solution for computer crimes because of the difficulties involved in apprehending cybercriminals. Law enforcement is also less effective in maintaining order in cyberspace than it is in real-world. The justice system’s inability to prosecute computer crimes indicates that it is not functioning effectively in this area. The cyberperpetrator does not risk identification and apprehension since he is able to act remotely and anonymously.

IV. Council of Europe Convention on Cybercrime

A. Background

The global interconnection of vulnerable computer systems requires a uniform transnational legal framework for addressing multinational computer crimes. There have been two significant steps towards achieving this framework. First, in December 1997, representatives from eight major industrialized nations (the G-8) agreed on a ten-point plan to fight international computer crime. The United States participates actively in the Subgroup on High-tech Crime at G-8’s Lyon Group.

Second, in November 2001, the Council of Europe approved a convention to deal with the rising problem of computer crime and its global implications. The United States and thirty-three other countries have signed the “Council of

\[\text{SMITH, supra note 2, at 155.}\]
\[\text{CLIFFORD, supra note 10, at 168.}\]
\[\text{Lewis, supra note 4, at 1369 (suggesting hack-in contests as a creative approach to preventing computer crime).}\]
\[\text{Brenner, supra note 7, at 88.}\]
\[\text{Id. at 103.}\]
\[\text{CLIFFORD, supra note 10, at 183.}\]
The Convention on Cybercrime was developed in response to a growing concern about the adequacy of legislation criminalizing certain activities occurring over computer networks. The Convention is a multilateral agreement geared at facilitating international cooperation in the prosecution of cyber criminals. It is the first international treaty on crimes committed via the Internet and other computer networks.

As set out in the preamble, the Convention's main objective is to pursue a common criminal policy to protect society from computer crime. The Council's solution requires parties to adopt appropriate legislation to counter computer crime, to ensure that their law enforcement officials have the requisite authority and procedural tools to effectively investigate and prosecute computer crimes, and to provide international cooperation to other parties engaged in such efforts. The Convention requires participating parties to adopt national measures that move towards establishing international uniformity in the area of computer crimes by amending the relevant substantive criminal law, procedural law, and jurisdictional provisions. In addition, the Convention obliges parties to cooperate with each other to the widest extent possible for the purposes of

---

70 Convention on Cybercrime, supra note 8, art. 1. While the United States has already signed the treaty, the Senate still must ratify the treaty in order to give it effect in the United States.

71 SMITH, supra note 2, at 101.


73 CLIFFORD, supra note 10, at 187.

74 Weber, supra note 72, at 430.

75 Convention on Cybercrime, supra note 8, art. 14.

76 Id. art. 2.
investigations or proceedings relating to computer crime.\textsuperscript{77} The Convention makes all computer crimes extraditable offenses.\textsuperscript{78}

The Convention requires parties to (a) establish substantive laws against computer crime; (b) ensure that their law enforcement officials have the necessary procedural authorities to investigate and prosecute computer crime effectively; and (c) provide international cooperation to other parties in the fight against computer crime.\textsuperscript{79} The Convention was created to address the jurisdictional issues posed by the evolution of the Internet.\textsuperscript{80} Its solution was to harmonize computer crime laws and assure the existence of procedural mechanisms to assist in the successful prosecution of cybercriminals. International cooperation on computer crime has traditionally been the exception rather than the rule and prosecution is frustrated by a lack of enforceable cooperation.\textsuperscript{81}

B. Offenses and Jurisdiction

The Convention requires the criminalization of nine offenses in four categories: the first category targets “offenses against the confidentiality, integrity and availability of computer data and system;” these include illegal access, illegal interception, data interference, system interference, and misuse of devices.\textsuperscript{82} The second category, “computer-related offenses,” includes provisions calling for the criminalization of computer-related forgery and computer-related fraud.\textsuperscript{83} The third category, “content-related offences,” requires criminalizing offences related to child pornography.\textsuperscript{84} The fourth category, “offenses related to infringements of copyright and related rights,” criminalizes copyright violations.\textsuperscript{85} This section of the Convention also

\textsuperscript{77} Id. art. 23.
\textsuperscript{78} Id. art. 24.
\textsuperscript{79} Id. art. 13.
\textsuperscript{80} Weber, \textit{supra} note 72, at 426.
\textsuperscript{81} Carter & Perry, \textit{supra} note 13, at 364.
\textsuperscript{82} Convention on Cybercrime, \textit{supra} note 8, art. 2.
\textsuperscript{83} Id. art. 7-8.
\textsuperscript{84} Id. art. 9. This third category is ostensibly supplemented by a new protocol, adopted November 7, 2002, making any dissemination of racist or xenophobic material through computer systems a criminal offense. However, the new protocol is a separate legal instrument from the treaty, and parties agreeing to the treaty are not obliged adopt it.
\textsuperscript{85} Id. art. 10.
includes ancillary provisions that require the establishment of laws against attempting, aiding or abetting in the aforementioned crimes, as well as the establishment of a standard for corporate liability.86

The Convention also addresses procedural legal issues. It requires states to establish a minimum set of procedural tools at the national level whereby the appropriate law enforcement authorities within a state have authority to conduct certain types of investigations specific to computer crimes.87 The Convention also includes a provision granting a participating state jurisdiction over offenses committed within that state’s territory. This allows a state to assert jurisdiction in a computer crime involving a computer system within its territory, even if the perpetrator committed the offense from a remote location outside of the state.88 Further, the Convention grants a state jurisdiction over a citizen of that state who commits a covered offense outside of the state’s boundaries, so long as the offense is also punishable by criminal law in the jurisdiction where it was committed, or if the offence occurred outside of the territorial jurisdiction of any state.89

The Convention provides three general principles of international cooperation. First, international cooperation will be provided among states “to the widest extent possible.”90 Second, the obligation to cooperate extends not only to the crimes established in the treaty, but also to the collection of electronic evidence whenever it relates to a criminal offense.91 Third, the provisions for international cooperation do not supersede preexisting provisions of international agreements on these issues.92 However, the Convention still has some flaws. Widespread adoption of the Convention could stunt the development of computer crime legislation. Treaties are more difficult to amend than domestic legislation. The Convention does not resolve the extraterritorial jurisdictional issue because it ultimately fails to articulate a common set of crimes.93 The Convention is further hampered by the lack of universal participation.94

---

86 Id. art. 11.
87 Id. art. 14.
88 Id. art. 22.
89 Weber, supra note 72, at 432.
90 Convention on Cybercrime, supra note 8, art. 23.
91 Id. art. 25.
92 Id. art. 27.
93 Weber, supra note 72, at 445.
94 Convention on Cybercrime, supra note 8, art. 39, 42.
V. Conclusion

Despite its flaws, the Convention on Cybercrime aspires to meet the challenges of computer crimes. Computer criminals are increasingly located in places other than where their acts produce their effects. However, domestic laws are generally confined to a specific territory. Thus solutions to the problems posed must be addressed by international law. The adoption of adequate international legal instruments is necessary.

The development of law on computer crimes lags behind the development of technology. Therefore, solutions that rely solely on international coordination to investigate and prosecute computer criminals will not work. Due to different priorities and rapidly changing technology, countries are unlikely to adopt uniform laws dealing with computer crime. Countries may not be able to dedicate adequate resources to effectively investigate and prosecute computer crime. There is no international body with the capacity or competency to coordinate investigation and prosecution of computer crime.

Computer crime will increasingly be a challenge for all industrialized nations. Given the global nature of computer crimes, domestic law enforcement authorities must work together with many other countries to make progress in the prosecution of computer crimes. In addition to specialized task forces designed to prosecute computer crimes, advances in technology have also increased the efforts of law enforcement to combat computer crime. Computer security is enhanced because potential victims of computer crimes are more aware of specific possible violations. Potential violators are more likely to know which particular activities are unlawful. Prosecution is aided by eliminating the need for prosecutors, attorneys, and judges to rationalize the application of a traditional criminal law in a technical, computer-related context.