

## LEGAL FRAMEWORKS FOR COMBATING CYBERCRIME

### **Components of Substantive Network Crimes Laws: How to Criminalize Attacks on Computer Networks and Information**<sup>1</sup>

#### **I. Introduction**

#### **II. Definitions**

#### **III. Defining Computer Crime**

- A. *Computer as a Tool*
- B. *Computer as a Storage Device*
- C. *Computer as a Target*

#### **IV. Components of a substantive network crimes law**

- \_\_\_\_\_ A. *Who is the Victim?*
- B. *What is the wrongful activity?*
  - 1. Computer Intrusion
    - a. \_\_\_\_\_ Damaging Computers During an Intrusion
    - b. Theft of Information
    - c. Intent to Commit Fraud or Other Crime
    - d. Cause Physical Harm or Threat to Public Safety
  - 2. \_\_\_\_\_ Transmit Command or Program to Commit Offense
  - 3. \_\_\_\_\_ Interception of Data in Transmission
  - 4. \_\_\_\_\_ Trafficking in Passwords or Other Access Information
- C. *What is the State of Mind?*
- D. *Where are the Crime and the Criminal: Issues of Jurisdiction?*
- E. *What is the Punishment?*

#### **V. Conclusion**

---

<sup>1</sup> An earlier version of this paper was presented at the “Legal Frameworks for Combating Cybercrime” workshop in Moscow, August 17-18, 2002, in connection with the APEC TEL 26 meeting. It was prepared by Miriam Smolen, Computer Crime and Intellectual Property Section, Department of Justice, United States of America.

## **I. Introduction**

Today, the exploding use of information systems and networks has caused countries to become increasingly interconnected, and these connections cross geographic borders. Computer networks support critical infrastructures such as energy, transportation, and banking and finance, and they play a major part in how companies do business, how governments provide services to citizens and enterprises, and how people communicate and exchange information. The number and nature of technologies has multiplied and will continue to grow, and so has the nature, volume, and sensitivity of information that is moving from place to place. Information systems and networks are now exposed to a growing number and a wider variety of threats. Electronic commerce and the marketplace cannot thrive without strong and safe information systems and networks on which the public can trust. One element of assuring secure networks is a comprehensive legal framework to deter, identify, and prosecute attacks on computer networks and information.

This white paper seeks to provide a catalogue of elements of substantive network crime laws and to suggest the components necessary to create a powerful and effective statute to deter and punish attacks on computer networks and information. It draws upon many different countries' existing cybercrime laws, each of which is unique. This presentation also presents articles from the Council of Europe Cybercrime Convention (2001), where relevant, because many countries have agreed that the Cybercrime Convention provides the necessary standards for an effective legal framework. Of course, countries are encouraged to develop legal frameworks that go beyond the Cybercrime Convention to provide more comprehensive protection against attacks on computer networks and information.

## **II. Definitions**

The following definitions, taken from the Council of Europe Cybercrime Convention, apply to the discussion that follows:

- a.* "computer system" means any device or a group of inter-connected or related devices, one or more of which, pursuant to a program, performs automatic processing of data.
- b.* "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function.
- c.* "service provider" means:
  - i.* any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and

- ii. any other entity that processes or stores computer data on behalf of such communication service or users of such service.
  
- d. "*traffic data*" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

(Council of Europe, Convention on Cybercrime, 2001).

### **III. Defining Computer Crime**

Terms such as "cybercrime," "computer crime," and "network crime" have no universally accepted definitions. Part of the confusion arising from their use comes from the fact that today criminals use computers in the course of committing almost any crime. The computer's role in an offense can, however, be characterized in one of three ways:

#### *A. Computer as a Tool*

A computer can be used as a tool for committing criminal activity. This category includes those crimes that criminals have traditionally committed in the physical world but that are now occurring with increasing frequency on the Internet. These crimes include fraud, the distribution of child pornography, intellectual property violations, stalking, money laundering, and the sale of illegal substances and goods online. However, online facilities may be used in the furtherance of a broad range of other traditional unlawful activity as well. E-mail and chat sessions, for example, can be used to plan or coordinate almost any type of unlawful act, or even communicate threats or extortion demands to victims. For the most part, existing "physical world" laws already govern these kinds of unlawful conduct.

Lawmakers should, however, consider reviewing traditional criminal laws to ensure that what is prohibited in the physical world is likewise prohibited in the virtual world. Traditional crimes may be committed in new ways using computer networks. For example, certain types of communications on the Internet are point-to-point like the telephone, while others disseminate information to a vast, unknown audience, like a newspaper. Prohibitions should be technology neutral so that laws do not become outdated as technology evolves.

#### *B. Computer as a Storage Device*

Criminals, like businesses, governments, and individuals can take advantage of computers' ability to store large amounts of information. Criminals store information when committing a wide

variety of traditional crimes, and that information becomes electronic evidence<sup>2</sup> relevant to the investigation of that crime. For example, a drug dealer may store his customer list on his Palm Pilot or laptop. A kidnapper may type a ransom note on her computer, potentially allowing investigators to link her to the crime. In addition, information stored on a computer may be relevant to solving a crime even where the criminal did not create that information. For example, an investigation into the submission of false invoices may depend on the contents of an electronic database maintained by a victim corporation that contains the firm's bills and payments. Use of computers as storage devices generally does not require the creation of new substantive laws, but the growth of electronic evidence may require a country to consider amendments to laws regulating law enforcement access to such evidence.

### C. *Computer as a Target*

A computer can be the target of criminal activity. Commonly called “network crimes,” this activity involves attacks on the confidentiality, integrity, or availability of computer systems or information.<sup>3</sup> Criminals undertake these attacks to acquire information stored on the target system, to control the target system without authorization or payment, to delete or modify data, or to interfere with the availability of a computer or information. Often these attacks result in theft of information or monetary loss to the owner of the victim computer. Criminal activities included in this category are computer intrusions, the release of viruses and other malicious code, website defacements, and denial-of-service attacks that impair the availability of computer systems or data. The following discussion will explore the legal framework necessary to address those situations where the computer is the target of the crime.

---

<sup>2</sup> Electronic evidence is information relevant to a criminal investigation that is created or stored in digital form. Electronic evidence may be created when, for example, a person sends an email or enters data into a database. Electronic evidence may also be generated by the computer itself. This occurs when computer programs generate output. Examples of this type of evidence include bank statements where the software used by the bank calculates sums; phone logs recording phone numbers called or received; and the addressing logs for electronic communications. In addition, electronic evidence may be the contraband itself – images of child pornography or pirated software. Electronic evidence can be easily destroyed, deleted, or modified. For example, digital photographs can be altered in ways that may be difficult to detect. As a result, law enforcement officials must be cognizant of how to gather, preserve, and authenticate electronic evidence.

<sup>3</sup> A network is any collection of connected computers. A network may be as simple as two computers joined on a LAN (local area network), or have hundreds or thousands of computers connected by common servers and routers. The Internet is an interconnected “network” of millions of computers.

#### IV. Components of substantive network crimes law

\_\_\_\_\_ Although there are a wide variety of network crimes laws in existence, each of them addresses certain core components. These are:

- A. Who is the victim?
- B. What is the wrongful activity?
- C. What state of mind is required?
- D. Where are the crime and the criminal?
- E. What is the punishment?

##### A. *Who is the Victim?*

Many countries' network crimes laws do not separate victims into categories; instead they simply use the term "any computer," to define the victim of specified offenses. However, the identity of the victim may influence what type of activity is criminalized, and the severity of the punishment.

The distinction may be between government and non-government computers. The category of government computers often includes government departments and agencies, military systems, systems related to national security, and private entities operating as government contractors. The non-government computer category then becomes a catch-all for all computers not identified with the government.

There are other victims that may fall in the non-government category that need specialized attention in a network crimes law because they are critical to the day to day functioning and the safety and well-being of society. These victims are part of what is called the Critical Infrastructure and include systems controlling: telecommunications, banking and financial systems, electrical or other energy supply systems, transportation, water, emergency operations, medical and health care, and food supply. Also, facilities through which an electronic communication service is provided, such as public or private Internet Service Providers (ISP), may warrant special focus in a law.

Protecting this critical infrastructure is imperative but difficult for a host of reasons: the number of different systems involved, the interdependency of these systems, the varied nature of the threats (physical and cyber, military, intelligence, criminal, natural), and the fact that many of these infrastructures are maintained primarily by the commercial sector. Addressing cyberthreats to the infrastructure is particularly difficult, because of the need to balance interests relating to privacy,

economic competitiveness, commercial risk, national security, and law enforcement; and the overlapping authorities within governments for dealing with infrastructure issues.

*B. What is the wrongful activity?*

1. Computer Intrusion

A computer intrusion, also called a hack, is a trespass into a computer or computer system by a person not entitled to be there. These intruders may be divided into two categories -- persons who attack from the outside and wrongfully access a computer “without authorization,” and persons who are insiders and thus have authorization for access to specific portions of the computer but intrude into other parts of the computer or network by “exceeding authorized access.” Prohibiting computer intrusions is the heart of any network crimes law.

Obtaining access to a computer “without authorization” may be defined as intrusions into a computer by an “outsider” who has no legitimate purpose in using the system. The anatomy of this type of intrusion may look like this: a hacker locates a victim system by scanning the Internet with hacker tools and finding an open port or other hole in the operating system security. The hacker breaks in to exploit the operating system. He gains “superuser” status and then may alter logging or accounting systems to hide his tracks. Once inside, he has free rein to read, alter, or damage any files or the computer, including communications and other records. He may use the compromised system as a platform to attack other systems. Finally, a hacker will often advertise the compromised site and its vulnerabilities on hacker websites or in chat rooms.

Obtaining access to a computer by “exceeding authorized access,” refers to intrusions by insiders – persons who, by employment or some other relationship, have authority to access certain areas of a network, but who then use that authorized access to increase their status to “superuser,” and access areas they are not allowed to visit. Once this insider is where they are not allowed to be, they might read, alter, or damage information to which they are not entitled to have access.

A network crimes statute may use the distinctions of “accessing a computer without authorization,” and “exceeding authorized access,” to treat insiders and outsiders differently. Some network crimes laws do not make this distinction, and treat all hackers similarly. Some of the other commonly seen phrases used to describe a hacker’s lack of authority to have access to the computer include: illegal access; access without color of law; fraudulently obtaining or maintaining access; and unlawfully intruding into a computer.

The Council of Europe Convention on Cybercrime addressed this area in:

*Article 2 – **Illegal access***

*Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may*

*require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.*

a. Damaging Computers During an Intrusion

An effective network crimes law must prohibit access without authorization, or access that exceeds authorization, where the intruder causes damage to information or systems. If, as a result of an intrusion, the information in the database is changed, the data does not possess the integrity or availability it did before, and “damage” has therefore been caused. Similarly, where an intrusion causes a shutdown or slowdown in a computer system, either as a result of the attack, or as a result of the steps taken to discover and repair the attack, the system integrity and availability has been damaged.

In a network crimes law, the words “causes damage,” should mean impairing the availability and integrity of systems or information. If a statute chooses to further describe how damage is caused, words commonly used include: deletion, addition, modification, alteration, suppression (so that legitimate users may not gain view or use data), deterioration, rendering data unusable, obstruct, interfere or deny access, and also inputting or transmitting a program, information, code or command, and as a result of such conduct, causing damage. The last conduct – inputting or transmitting a program etc. – is important to include in a statute because damage can be caused even without an illegal intrusion. For example, a denial of service attack can flood a computer with so much information or communications that the computer slows or shuts down.

When drafting sections of network crimes laws dealing with causing damage, make sure the same terminology is used throughout. Defining causing damage differently when discussing damage to information than when discussing damage to systems, for example, leads to confusion and holes in the law. Whatever specific terminology is used, the statute should make clear that the terminology is not exclusive. Also, ensure that the language used is technology neutral. For example, avoid naming attacks such as “virus” and “worm.” New attacks are created all the time and statutory language drafted today must be broad enough to anticipate what the future may bring.

The Council of Europe Convention on Cybercrime provisions relating to this area are:

*Article 4 – Data interference*

*1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.*

*2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.*

*Article 5 – System interference*

*Each Party shall adopt such legislative and other measures as maybe necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.*

b. \_\_\_Theft of Information

Prohibitions against stealing information via obtaining unauthorized access to a computer serve to protect the confidentiality, integrity and availability of data contained in computers. There is an individual privacy interest in ensuring that certain types of information, such as financial information, credit cards, and banking information, remain private. There is a corporate or organizational interest in ensuring that business related data – customer lists, trade secrets, internal databases - also remain private.

It should be noted that the concept of obtaining or stealing data should include the act of merely viewing the data, regardless of whether an intruder copies or downloads the information. Indeed, by merely “viewing” data, a copy of it is transferred to the hacker’s computer screen. The confidentiality and integrity of the data is vitiated by the act of viewing it and the prohibition needs to take effect at that moment.

Criminalizing the obtaining of any data stored in a computer by means of unlawful access would cover whatever type of information was stolen. However, many statutory schemes distinguish between types of stolen data, or the uses to which it may be put, for purposes of intent requirements or severity of punishment.

Theft of certain types of data, such as certain government records or national security information, pose such a danger that those types of theft may be punished more severely, regardless of whether the information has inherent value, or to what use the information is put. Thus, a criminal code might punish such thefts more severely. The category of financial or personal information, about which individuals are particularly concerned includes: banking records, credit card numbers and records, credit reports and other types of uniquely identifying personal information such as full names date of birth, identity number (i.e. Social Security number in the United States). The prevalence of the crime of identity theft, where a person appropriates the identity of another and proceeds to open lines of credit, and make other transactions in the stolen name, makes the protection of this type of data particularly important.

Another category of data that may require increased punishment if stolen, is business information or trade secrets. This data may be valuable in and of itself, such as websites that sell access to a certain database for a price, or data which is valuable because it contains trade secrets or other proprietary information. Finally, network crimes law may contemplate additional penalties for stealing information and using it to facilitate a separate crime.

c. \_\_\_\_ Intent to Commit Fraud or Other Crime

\_\_\_\_\_ To the extent that computers are prevalent in a sector of an economy, computers will be the targets of persons who are intent on hacking in order to further a different crime. These persons may be hacking in order to obtain information contained in a computer that they can use in another crime, such as theft of credit card numbers in order to make fraudulent purposes. Or, they may use the computer to further the offense itself, such as where a person uses email to entice someone into a fraud scheme, or sets up a “warez” website to distribute illegally copied copyrighted software. The list of offenses that may be facilitated through a hack is, unfortunately, extremely large. A network crimes statute that seeks to combat such wrongful use need not focus on individual crimes but rather on whether an unauthorized access was undertaken with the object of facilitating another crime.

The Council of Europe Convention on Cybercrime’s related provisions are:

*Title 1, Article 7 – Computer-related forgery*

*Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.*

*Title 1, Article 8 – Computer-related fraud*

*Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another by:*

- a. any input, alteration, deletion or suppression of computer data,*
  - b. any interference with the functioning of a computer system,*
- with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another.*

d. \_\_\_\_ Cause Physical Harm or Threat to Public Safety

When a computer intruder’s actions cause, or threaten to cause, physical harm to an individual or a threat to public safety, it may be appropriate to level more severe penalties on the perpetrator, or reduce the mental state required to show a crime.

An individual’s physical safety may be threatened if a hack, for instance, altered medical records in a hospital, or simply caused the hospital’s doctors to be unable to reach medical records. There are untold ways in which an unauthorized user could cause harm to a person, and such actions should be taken extremely seriously.

Moreover, when a hacker threatens, or causes, a harm to public safety, heightened scrutiny is also appropriate. Public safety may be threatened when any of the critical infrastructures are threatened. These include systems controlling: telecommunications, banking and financial systems, electrical or other energy supply systems, transportation, water, emergency operations, medical and health care and food supply. Damage to these infrastructures could cause terrible consequences: imagine the impact of an air traffic control system shut down or disruption of computerized flood gate controls of a large dam.

## 2. Transmit Command or Program to Commit Offense

A person can harm a computer, data, program or system without gaining unlawful access to the computer itself by sending through electronic communications various types of attacks that damage the computer which receives it. These attacks are often self-multiplying and infected computers often pass on the infection to other systems connected to them. Computer users have suffered attacks of several types over the last few years that have caused untold millions in damage to computers and lost business. Therefore, effective network crimes laws must prohibit the transmission of a program, information, code, or command that would cause damage or harm, without a requirement of unauthorized access.

These attacks have a number of different names, but include viruses, worms, logic bombs, trojan horses, and denial of service attacks. The common features among these attacks is that the attack is sent via electronic communication, and that the attacker need not access the computer to cause extreme harm.

Viruses infect a file or program and can make the computer damage its system and those of others. If one of the infected programs is passed to another user, such as by being attached to e-mail, the virus continues to spread. Many of the anti-virus software packages available do a good job at blocking viruses, but the effectiveness depends largely on the user updating the software so that it knows the “signatures” of the viruses on the loose. Even then, some viruses can morph into a new look with each time they infect different systems. These so-called polymorphic viruses, make it very difficult for anti-virus programmers to find a single signature that works to detect the ever-changing viruses. Viruses are also appearing in other technologies, such as wireless devices and hand-held computers.

The Worm thrives on networked computers. Its distinguishing characteristic is that it multiplies across networked systems without the need for human action. A worm does not rely on being carried by other files or programs as does the virus. Rather, it is its own free-standing program, designed to replicate itself on to as many systems as it can. Like a virus, a worm may be able to do a myriad of tasks. The first worm to become famous was the Morris worm, which crashed thousands of computers by simply replicating itself with exponential growth. Some of the recent examples of worms include the I Love You worm and Nimda.

The Trojan Horse is designed to trick users into installing a malicious program by making the program appear to be something useful, entertaining, or at least innocent, but which is actually something entirely different (usually damaging). Users are fooled into installing the payload because the Trojan horse disguises the true contents. If it replicates itself, the Trojan is also a worm or virus.

The Logic Bomb resides within otherwise legitimate code, and is invoked upon the happening of some event, or series of events. When the triggering event occurs, the logic bomb deletes information, crashes the operating system, or causes some other malicious activity on the computer.

A denial of service attack is an attempt to keep legitimate users from using a system. Sometimes such attacks work by consuming scarce, limited, or non-renewable resources such as disk space, network bandwidth, or processor time, so that none of these resources is available to the legitimate users. Another technique is to destroy or alter configuration information to render a computer unreachable. Like so many other attacks on networks, denial of service attacks are often automated, remote and anonymous.

### 3. Interception of Data in Transmission

A person may take steps to capture data and communications while they are in transit without the knowledge or permission of the people communicating. This type of activity may take place inside a computer system, where a person could be present either wrongfully, or with authorization. Network crimes laws that desire to prohibit this type of behavior must not limit their scope to activity inside a particular computer or system, but rather focus on the wrongful activity itself, wherever it may take place.

The Council of Europe Convention on Cybercrime (2001) discusses this prohibition in Title 1, Article 3:

*Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.*

### 4. Trafficking in Passwords or Other Access Information

Access devices are passwords, codes, account numbers, or other telecommunications service, that allow access to a computer, computer system or to the data in transmission. The word “device” is a misnomer; often the device is information that will unlock the gate for the computer user. Network crimes statutes should prohibit the unauthorized transfer of such devices, as well as the

possession with the intent to use wrongfully, because such devices facilitate computer abuse and fraud. Prohibitions sometimes require that a certain number of devices be sold or at a certain value.

The definition of access device should be broad enough to cover all the means for obtaining unauthorized access. Indeed, it should cover information about a system's vulnerabilities that, if used, allows the user to find the unauthorized "back door" into a system.

The Council of Europe Convention on Cybercrime discusses this prohibition in:

*Article 6 – Misuse of devices*

*1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:*

*a. the production, sale, procurement for use, import, distribution or otherwise making available of:*

*i. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the [hacking] offences;*

*ii. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed with intent that it be used for the purpose of committing any of the [hacking] offences*

*b. the possession of an item referred to in [earlier] paragraphs, with intent that it be used for the purpose of committing any of the offences [established in earlier Articles]. A Party may require by law that a number of such items be possessed before criminal liability attaches.*

*C. What is the State of Mind?*

Existing network crimes statutes tend to compartmentalize actions into three possible mental state categories; some statutes use these mental states as a means of determining the severity of the punishment. These mental states are acting with intention, acting recklessly, and actions that do not have a mental state requirement. It must be mentioned that the definitions and use of these descriptions of mental states are specific to each country. Identical terms do not have identical meanings in every country.

Intentional acts are those where it can be said that a person had the purpose to do a thing. He acted, or failed to act, consciously and voluntarily, and not inadvertently or accidentally. A law may use the term willfully instead of intentionally; generally, the definition of a willful act is one which is done knowingly, intentionally, and deliberately.

Reckless acts are those taken carelessly and in willful disregard of the rights or safety of others, or without regard to the impact of those actions.

Statutes that criminalize actions without regard to mental state do not require that there be a showing that a person knew the result of his actions; merely that he take those actions and a result occurs.

Where a statute requires that a defendant act with intent, the intent requirement should be limited to showing that the defendant intended to do the actions he took, rather than that he intended to cause the actual consequences which resulted. For example, the requirement should go to showing the defendant's intent to do the thing which caused the intrusion, rather than showing that the defendant intended to cause a specific type of damage. Also, where there is an intent to cause damage, whether a person is inside the system legally or illegally should not be relevant.

*D. Where are the Crime and the Criminal: Issues of Jurisdiction?*

The borderless nature of global networks means that a single criminal act using the computer may touch several countries. Increasingly, computer attacks come from outside a country's borders. Even where an attack comes from within an country's borders, the hacker tools used to commit the offense, may reside on a server outside those borders.

Domestic laws should cover attacks against a computer inside a country's borders regardless of the location of the attacker — inside the country's borders or outside. Also, the law should allow for prosecuting, or making available for prosecution, an individual located domestically, who attacks a computer outside the country's borders. Moreover, laws need to be capable of supporting prosecutions of individuals who use tools or computers located outside the borders of where they are located, to conduct the attack or crime. Of course, because of the borderless nature of network crimes, countries need to be supportive and cooperative with other countries with regard to the protection of networks and information, and where a country is not able to assume jurisdiction, it should be prepared to cooperate in the prosecution of an individual by the prosecuting country.

The Council of Europe Convention on Cybercrime (2001), set forth the following with regard to jurisdiction:

*Section 3, Article 22 – Jurisdiction*

- 1. Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence . . . , when the offence is committed :*
  - a. in its territory; or*
  - b. on board a ship flying the flag of that Party; or*
  - c. on board an aircraft registered under the laws of that Party; or*
  - d. by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State. . . .*

2. *Each party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down [in the Convention].*

3. *Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph (1) of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him/her to another Party, solely on the basis of his/her nationality, after a request for extradition.*

4. *This Convention does not exclude any criminal jurisdiction exercised in accordance with domestic law.*

5. *When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.*

E. *What is the Punishment?*

Existing network crimes laws present as many different frameworks for punishment of computer offenses as there are countries with network crimes laws. While there is obviously no correct answer as to how severe punishment should be for the various offenses described above, it is clear that the punishment should be severe enough to act as a deterrent for those persons who believe that hacking and network attacks are not crimes that governments take seriously. This usually means meaningful periods of incarceration, restitution to the victim, and sometimes, fines.

As described above there are a number of variables that might be taken into account when determining which offenses merit heavier punishments:

Who is the victim? Does the network attack threaten an individual's personal safety or the safety of a critical infrastructure system?

Was the information stolen of such importance it deserves extra protection?

Was the action intentional or reckless?

What other crimes were facilitated by the network attack crime?

What was the damage suffered by the system or information?

What was the loss suffered by the victim or other enterprises and people who were harmed by the wrongful activity?

An additional factor to be taken into account is what benefit, economic or otherwise, the defendant gained. However, that a defendant did not personally benefit should never be determinative because, unlike many conventional crimes, often a person who is committing crimes against, or on, a network, is not doing it for a personal benefit. There have been numerous network attacks which are committed by individuals simply because they could do it. The motivation is often to raise the actor's personal reputation as someone who is capable of these technological escapades, rather than to obtain a financial benefit.

If a statutory framework uses the level of damage or amount of loss as a criteria for punishment distinctions, or even for determining the nature of the offense, the framework must take into account a number of factors, starting with how the level of damage, and the total of amount of the loss is calculated.

The term loss typically refers to the harms caused by an intrusion to a computer, data, program or system. The financial calculator for this harm should include the costs associated with discovering the intrusion, determining the scope of the harms, and the time and material spent repairing the harm, including any computer “fixes” necessary to close the door through which the hacker entered. Time spent in discovery, assessment, and repairs may be calculated by using the employees’ hourly rate with, or without benefits, the computer time lost, and other administrative overhead costs. Where an intruder impairs a program, system, or data, by for example deleting or modifying a program or data, or adding program code or data that alters the systems operations, the damage would be the costs to discover what was done, the “fix,” and securing the system from future similar attacks.

The amount of loss must also include any financial losses due to interruption of service, either because the intrusion shut or slowed the system, or because the system was shut down for repair purposes. Business interruption losses may be difficult to quantify depending on the nature of the business. Where a number can be attributed to loss of goodwill or reputation, that may be included as well.

Where the purpose of the intrusion was to gain use of the computer itself, as where an intruder hacks into a powerful computer to use its computing power to run his own programs, the loss would be the value of the computer time used, as well as any discovery and repair costs.

If an intruder steals information, the value of that information should be included in the loss amount. This number may be calculated by the value of the stolen information where the information has an inherent value, as where the information is itself for sale. Or, if the information is of a proprietary nature, such as certain business information, the value may need to be determined by calculating its value to the business.

There are scenarios where an intrusion does not cause permanent alteration of the system or data, and thus, it could be argued there is no financial impact. For example, suppose an intruder alters existing security programs and obtains information, such as user passwords, but then fixes his alterations to leave the computer as he found it. Arguably, in such a situation, neither the computer nor its information is permanently damaged. Nonetheless, the intrusion itself did impair the confidentiality and integrity of the data, and thus damage has occurred which can be quantified. In this case, patches to fix the security hole would need to be applied, and also the breach of the security of the passwords would require that resources be devoted to changing the compromised passwords.

Laws should also take into account the fact that a single intrusion, or a series of intrusions by one hacker, may affect multiple computers causing damage and loss at each site. Aggregating the total loss from all the affected computers provides a truer total figure of harm caused by the hacker.

Thus, statute that uses damage amounts as a criteria for a certain crime or level of punishment should ensure that the language takes into account damage from all affected computers from an attack or series of related attacks.

Finally, determining the “actual loss” is often difficult for a number of reasons. For example, the actual effects of a network intrusion may reach far beyond the network itself. The downstream harm, or ripple effect, of the loss of service on the network may be severe, yet difficult to quantify in dollar terms. Consider the case of an intrusion into a computer that controls air traffic at a small airport. It may only cost a small amount of money to have a computer technician reset the computer, but even a short outage may have an enormous impact on air safety and flight schedules. Similarly, disruption of a military logistics computer may not cause any loss in business revenue and cost a relatively small amount to restore service, yet temporarily cause grave harm to the country’s security or prevent the military from fulfilling an important mission. Moreover, “actual loss” may not capture the true extent of the harm where the computer intrusion causes a loss in privacy. For example, if hackers break into a health care provider’s data base and steal medical records and identification numbers, the harm to personal privacy is great even though their actions cause little or no financial loss. Where there is no way easily to calculate that harm in financial terms, the criminal activity may not be properly punished.

## **V. Conclusion**

This presentation has focused on criminal frameworks for fighting network crimes. Although not addressed here, the world of civil remedies is another strong avenue for combating networks attacks as well.

This presentation has attempted to describe all the various network crimes activities that could be addressed in a network crimes statute. This presentation drew from many countries’ laws, and the Council of Europe Cybercrime Convention, and none of these sources encompasses all the points made above. Obviously, any country’s law must fit within its own legal framework. Much can be learned from reviewing the network crimes laws currently in existence and their amendments, which usually cure flaws in the earlier versions.