

CYBERCRIME LAW:

THE CONVENTION ON CYBERCRIME

Craig J. Blakeley

*The Qatar Information Security Forum
Doha, Qatar
June 19, 2008*



The Role of Cybercrime Law

- **Cybercrime law is not by itself sufficient to deter or address cybercrime. However, it is a critical component in:**
 - **Developing a National Strategy for Cybersecurity**
 - **Deterring Cybercrime; and**
 - **Promoting a National Culture of Cybersecurity**

Why Do We Need Cybercrime Law?

- **Conventional/Traditional Law is not sufficient to cover cybercrime.**
- **Cybercrime can be very costly and can seriously weaken confidence in ICT, thus disrupting economic growth and development.**
- **Cybercrime is increasingly international in scope.**

Conventional/Traditional Law Is Not Sufficient to Cover Cybercrime

- **What do we mean when we say “cybercrime?”**
- **In its broadest sense, we mean any type of misconduct or crime that can be committed or assisted through the use of a computer or the Internet.**

Cybercrime: What is it?

- **Use of a computer/Internet to do something that would be a crime in any case.**

Analogy: Murder is the taking of a human life without justification whether done with a rock, a sword, a gun electricity, poison, etc. The crime is defined in terms of the end result -- not how that result was brought about.

- **Fraud (credit card or identity theft)**
- **Child Pornography**
- **Intellectual Property Violations**
- **Stalking**

Cybercrime: What is it?

- **Use of a computer/Internet to commit a “traditional” crime in a different way or to dramatically increase the impact of a “traditional” crime.**
 - **Fraud (credit card or identity theft)**
 - **“Phishing” -- obtaining identity information or credit card numbers by masquerading as a legitimate business representative (such as a Web site or through e-mail)**
 - **Child Pornography & Intellectual Property Violations**
 - **Internet can be used to distribute on a worldwide basis & can be used to hide geographic location of crime or to escape jurisdiction**

Cyber Crime: What is it?

- **Use of a computer/Internet to commit a “traditional” crime in a different way or to dramatically increase the impact of a “traditional” crime. (*cont.*)**
 - **Cyberstalking -- Use of e-mail or other electronic communication by computer to threaten, harass, or put an individual in fear of harm.**



**ALLIANCE
LAW GROUP_{LLC}**

www.AllianceLawGroup.com

Cyber Crime: What is it?

- **Use of a computer/Internet to do something that we want to prohibit (i.e., make criminal) but which action (crime) would not be possible without a computer/Internet.**

Analogy: Drunk driving would not be a crime (i.e., would not be possible) without an automobile.

- **Computer viruses**
- **Spam**
- **Hacking**
- **Distributed Denial of Service Attacks**

A Cybercrime Law is Necessary Because Traditional Penal Laws Are Not Adequate.

- **Credit Card Fraud (for example):** Under existing law a fraudulent transaction does not lose its fraudulent (i.e., criminal) nature just because it takes place online rather than through a paper transaction. However, the impact may be significantly greater when it takes place online.
- **Hacking, Denial of Service Attacks, Viruses etc.:** Existing Laws are insufficient. There is not a physical entry or taking. And even if laws could be interpreted to cover such activity (a dubious proposition), the deterrence effect of a law of uncertain application would be very low.

Cybercrime Is Increasingly International in Scope

- **Cybercrime is increasingly decentralized, spread across numerous countries. In this way, perpetrators can avoid better avoid detection and enforcement efforts.**
- **The ITU and others have indicated that there is evidence that cybercriminals tend to locate where relevant law is weakest or non-existent.**



**ALLIANCE
LAW GROUP_{LLC}**

www.AllianceLawGroup.com

What Kind of Cybercrime Law is Needed?

- **Cybercrime law is needed in each country, which contains:**
 - **uniform and flexible definitions of illegal activity**
 - **procedures to allow the detection of cybercrimes and capture/preservation of relevant evidence**
 - **method for effective international collaboration**

Council of Europe Convention on Cybercrime

- **Opened for signature on Nov. 23, 2001**
- **Entered into force on Jan. 7, 2004**
- **Signed by 44 countries**
- **Ratified/acceded to by 23 countries including Canada, Costa Rica, Japan, Mexico, South Africa, and U.S.**



**ALLIANCE
LAW GROUP_{LLC}**

www.AllianceLawGroup.com

Convention on Cybercrime

(cont.)

- **The first international treaty focused on crimes committed on the Internet and using other computer networks**
- **Generally accepted as the international standard for cybercrime laws/legislation**
- **Aimed at fostering a common criminal policy against cybercrime, across multiple countries, and encouraging international co-operation against cybercrime**



Convention on Cybercrime

(cont.)

The Convention has three aims that are set forth in three chapters:

- **Harmonizing national substantive laws dealing with cybercrime**
- **Providing necessary power for the investigation and prosecution of cybercrime offenses**
- **Creating an effective means of international cooperation**

Convention on Cybercrime: Substantive Criminal Law Provisions

The Convention requires parties to adopt domestic laws and other measures that will make it a criminal offense to:

- **Illegal access.** (Chap. II, Sect. 1, Art. 2)
Intentionally access the whole or part of a computer system without legal right to do so
- **Illegal Interception.** (Chap. II, Sect. 1, Art. 3)
Intentionally intercept without right non-public transmissions of data to, from, or within a computer system
- **Data Interference.** (Chap. II, Sect. 1, Art. 4)
Intentionally damage, delete, deteriorate, alter, or suppress computer data without right



ALLIANCE
LAW GROUP_{LLC}

www.AllianceLawGroup.com

Convention on Cybercrime: Substantive Criminal Law Provisions

(cont.)

- **System Interference.** (Chap. II, Section 1, Art. 5)
Intentionally seriously hinder without right the functioning of a computer system by inputting transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.
- **Misuse of Devices.** (Chap. II, Sec. 1, Art. 6)
Intentionally and without right, produce, sell, procure for use, import, distribute, or otherwise make available:
 - a device designed or adapted for the purposes of committing any of the offenses specified in Articles 1 to 5 or



**ALLIANCE
LAW GROUP_{LLC}**

www.AllianceLawGroup.com

Convention on Cybercrime: Substantive Criminal Law Provisions

(cont.)

- a computer password, access code or similar data by which the whole or any part of a computer system is capable of being accessed
- Computer-related forgery.
(Chap. II, Sec. 1, Art. 7).
Intentionally and without right, input, alter, delete, or suppress 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 the data is directly readable and intelligible

Convention on Cybercrime: Substantive Criminal Law Provisions

(cont.)

- Computer-related fraud.

(Chap. II, Sec. 1, Art. 8)

Intentionally and without right, and with the fraudulent intent of procuring without right an economic benefit for oneself or for another person, cause a loss of property to any other person by:

- any input, alteration, deletion or suppression of computer data or
- any interference with the functioning of a computer system



Convention on Cybercrime: Substantive Criminal Law Provisions

(cont.)

Child Pornography (Chap. II, Sec. 1, Art. 9)

The Convention requires parties to adopt domestic laws and other measures that will make it a criminal offense with respect to child pornography to:

- **Produce it for the purpose of distributing it through a computer system**
- **Offer or make it available through a computer system**
- **Distribute or transmit it through a computer system**
- **Procure it through a computer system**



Convention on Cybercrime: Substantive Criminal Law Provisions

(cont.)

Child Pornography *(cont.)*

- Possess it in a computer system or on a computer data storage medium

Convention on Cybercrime: Substantive Criminal Law Provisions

(cont.)

Infringement of copyright & related rights

Chap. II, Sec. 1, Art. 10

The Convention requires parties to adopt domestic laws and other measures that will make it a criminal offense to violate the Agreement on Trade-Related Aspects of Intellectual Property Rights (“TRIPS”), the WIPO Copyright and Performances and Phonograms Treaties, and related international agreements (the Bern & Rome Conventions) where such acts “are committed willfully, on a commercial scale, and by means of a computer system.”



www.AllianceLawGroup.com

Convention on Cybercrime: Substantive Criminal Law Provisions

(cont.)

Attempt & Aiding and Abetting

Chap. II, Sec. 1, Art. 11

The Convention requires parties to adopt domestic laws and other measures that will make it a criminal offense to intentionally aid, abet, or attempt, the commission of any of the offenses, established under Articles 2 - 10 of the Convention.



**ALLIANCE
LAW GROUP_{LLC}**

www.AllianceLawGroup.com

Convention on Cybercrime: Substantive Criminal Law Provisions

(cont.)

Corporate Liability

Chap. II, Sec. 1, Art. 12

The Convention requires parties to adopt domestic laws and other measures to ensure that legal persons can be held liable in appropriate instances when actions prohibited by laws under the Convention are taken by by natural persons on their behalf.



**ALLIANCE
LAW GROUP_{LLC}**

www.AllianceLawGroup.com

Convention on Cybercrime: Substantive Criminal Law Provisions

(cont.)

Penalties

Chap. II, Sec. 1, Art. 13

The Convention requires parties to adopt domestic laws and other measures to ensure that violations by natural persons of offenses established in accordance with the Convention’s substantive provisions are punishable by “effective, proportionate, and dissuasive sanctions,” including imprisonment.

Similar requirements are imposed with respect to legal persons (i.e. corporations), except that imprisonment is not specified.

Convention on Cybercrime: Procedural Provisions

Section 2 of the Convention specifies procedural requirements to be applied to:

- **The criminal offenses established pursuant to the Convention**
- **Other criminal offenses committed by means of a computer system**
- **The collection of evidence in electronic form concerning a criminal offense**



**ALLIANCE
LAW GROUP_{LLC}**

www.AllianceLawGroup.com

Why Are Procedural Issues Important?

- **The Internet makes cybercrime activity possible anywhere in the world, directed at any area of the world.**
- **Cybercriminals often mask their location and their activity by using “third party” computers that they control without the owner’s knowledge or consent.**
- **Digital evidence is ephemeral and can quickly disappear or be erased. Thus, it is critical to detect and capture it very quickly.**



**ALLIANCE
LAW GROUP_{LLC}**

www.AllianceLawGroup.com

Convention on Cybercrime: Procedural Provisions

Parties must adopt domestic law and other provisions necessary to require:

- Expeditious preservation of data stored on a computer system**
- Submission of specified computer data under a person's control and subscriber information within the possession or control of a service provider**
- Search of a computer system and the data on it and seizure of relevant data**
- Collection or recording of real-time traffic data (including compelling a service provider to do so)**



Convention on Cybercrime: Procedural Provisions (*cont.*)

- **Collection or recording of real-time communications content (including compelling service providers to do so or to assist)**

Convention on Cybercrime: Jurisdictional Provisions

The Convention requires that parties adopt domestic law and other measures necessary to establish jurisdiction over any substantive offense under the Convention and that occurs in:

- The Party's territory**
- On board a ship flying the flag of the Party**
- On board an aircraft registered under the laws of that Party or**
- In a State where the offense was committed by a Party's nationals and is punishable by criminal law in that State or if the offense is committed by one of that Party's nationals in an area outside the territorial jurisdiction of any State**



**ALLIANCE
LAW GROUP^{LLC}**

www.AllianceLawGroup.com

Why is Jurisdiction Important?

- **Cybercriminals try to avoid detection and prosecution by operating outside of the territory that they are targeting.**
- **Thus, it is important that the targeted country have broad jurisdiction to pursue them.**
- **In order to do this effectively, international cooperation and coordination is critical.**



**ALLIANCE
LAW GROUP^{LLC}**

www.AllianceLawGroup.com

Convention on Cybercrime: International Cooperation

Chapter III of the Convention establishes the general principle that parties shall cooperate with each other “to the widest extent possible” to conduct investigations or proceedings concerning criminal offenses related to computer systems and data and for the collection of evidence in electronic form of criminal offenses under laws established pursuant to the Convention.



**ALLIANCE
LAW GROUP^{LLC}**

www.AllianceLawGroup.com

Convention on Cybercrime: International Cooperation *(cont.)*

Chapter III of the Convention also sets forth general principles on:

- **Extradition (i.e., the removal of a person from one country to another in order to be subject to prosecution for one of the criminal offenses established in accordance with the Convention) and**
- **Mutual assistance between parties**



**ALLIANCE
LAW GROUP_{LLC}**

www.AllianceLawGroup.com

Convention on Cybercrime: International Cooperation *(cont.)*

Chapter III of the Convention provides specific provisions on certain aspects of mutual assistance requests, where the data is within the territory of another party including:

- **Expedited preservation of stored computer data**
- **Expedited disclosure of traffic data**
- **Accessing stored computer data**
- **Real-time collection of traffic data**
- **Interception of communications content data**



**ALLIANCE
LAW GROUP_{LLC}**

www.AllianceLawGroup.com

Convention on Cybercrime: International Cooperation *(cont.)*

Finally, Title 3 of Chapter III of the Convention specifies that each party shall designate a point of contact available on a 24 hour by 7 day a week basis to assist in investigations or proceedings concerning criminal offenses related to computer systems and data. Such assistance shall include facilitation or performance of the following functions:

- Technical assistance**
- Preservation of data**
- Collection of evidence**
- Coordination and communication on an expedited basis with another Party's designated contact**

Convention on Cybercrime: Limitations (“Reservations”)

- **Reservations**

- **Many of the articles in the Convention specify that countries may limit the scope of the Convention through specific “reservations.”**

For example:

- **Countries may limit prohibition on data interference to conduct that “results in serious harm.”**
- **Countries can reserve the right not to impose criminal liability for copyright infringements so long as other effective remedies are available and this does not violate other international obligations.**



**ALLIANCE
LAW GROUP_{LLC}**

www.AllianceLawGroup.com

Convention on Cybercrime: Concerns

- **Privacy**

- **Some groups contend that its privacy protections (e.g., Article 15) do not provide adequate protection to individual privacy (Electronic Privacy Information Center <http://epic.org/privacy/intl/senateletter-072605.pdf>)**



**ALLIANCE
LAW GROUP_{LLC}**

www.AllianceLawGroup.com

Convention on Cybercrime: Concerns *(cont.)*

- **Dual Criminality**
 - **Concerns also have been raised that one country may be required to cooperate with another country in collecting evidence with respect to conduct that is not a crime in the second country.**
(American Civil Liberties Union
(<http://www.aclu.org/privacy/gen/15748leg20040616.html>)
However, the U.S. Dept. of Justice believes that this is not the case
(<http://www.usdoj.gov/criminal/cybercrime/COEFAQs.htm#QA10>)



**ALLIANCE
LAW GROUP_{LLC}**

www.AllianceLawGroup.com

Convention on Cybercrime: Implementation

- **Project on Cybercrime**
 - **Implementation project of Council of Europe focused on education and training concerning cybercrime and Convention on Cybercrime. Designed to encourage signing and ratification of Convention, use of Convention as model law, and training concerning implementing legislation.**
(http://www.coe.int/t/DG1/LEGALCOOPERATION/ECONOMICCRIME/cybercrime/default_en.asp)



**ALLIANCE
LAW GROUP_{LLC}**

www.AllianceLawGroup.com

On-Line Resources

- Convention on Cybercrime
(http://www.coe.int/t/DG1/LEGALCOOPERATION/ECONOMICCRIME/cybercrime/default_en.asp)
- ITU Global Security Agenda
(<http://www.itu.int/osg/csd/cybersecurity/gca/>)
- Computer Crime and Intellectual Property Section
U.S. Department of Justice
(<http://www.cybercrime.gov/>)
- News summaries concerning cybercrime laws and regulation and links to many national laws concerning cybercrime (<http://www.cybercrimelaw.net/>)

THANK YOU!



www.AllianceLawGroup.com

Craig J. Blakeley
Alliance Law Group LLC
7700 Leesburg Pike, Suite 410
Tysons Corner, VA 22043-2618
+1 703 848.8336
cblakeley@alliancelawgroup.com