

COMBATING CYBER CRIME: THE LEGAL (& PRACTICAL) CHALLENGES

Craig J. Blakeley



Cyber Crime

- **What is it?**
- **Why should we care?**
- **Are existing penal laws adequate to deal with it?
(Is there something unique or different about cyber crime that requires new laws to specifically address these issues?)**
- **What is the importance of international cooperation in addressing cyber crime?**
- **What preventative actions can be taken?**

Cyber Crime: 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**

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**
- **Denial of Service Attacks**

Cyber Crime: Why Should We Care?

- **Pervasive Nature and Growing Importance of the Internet and Computers**
- **Economic Importance of Computers & the Internet (Information & Communications Technology -- “ICT”)**
- **Potential Economic or Other Costs (e.g., e-government & e-commerce)**



**ALLIANCE
LAW GROUP_{LLC}**

www.AllianceLawGroup.com

Are Existing Penal Laws Adequate?

- **Some Are; Some Are Not**
- **Credit Card Fraud (for example): Existing Laws generally OK. A fraudulent transaction does not lose its fraudulent (i.e., criminal) nature just because it takes place online rather than through a paper transaction.**
- **Hacking, Denial of Service Attacks, etc. Existing Laws probably 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.**



But There Are Other Problems

- **Proof; evidence**
 - **Where the criminal conduct is digital, so is the evidence. As a result, there are associated problems of finding the evidence (it can be more easily hidden, changed or destroyed) and presenting the evidence (what is an acceptable physical version of a piece of digital evidence -- sort of a reverse e-signature/e-contract problem).**



**ALLIANCE
LAW GROUP_{LLC}**

www.AllianceLawGroup.com

But There Are Other Problems

- **Location; Jurisdiction**
 - **The Internet makes it possible for a cyber criminal**
 - **to be located anywhere in the world**
 - **to hide his or her location**
 - **Even where the location can be determined, it may be difficult or impossible for the country which was victimized to get jurisdiction of the criminal**



**ALLIANCE
LAW GROUP_{LLC}**

www.AllianceLawGroup.com

How to Deal With the Problem

- **Specific Laws to Cover New Crimes**
 - **E.g., U.S. Computer Fraud & Abuse Act prohibits unauthorized access to computer or computer networks which causes damage in a 1-year period of \$5,000 or more; prohibits transmission of viruses and other intentionally destructive code; both civil & criminal penalties are provided.**



**ALLIANCE
LAW GROUP_{LLC}**

www.AllianceLawGroup.com

How to Deal With the Problem

- **Broad Jurisdictional Provisions**
 - **E.g., Virginia: Virginia Computer Crimes Act**

Broad jurisdictional provision. Law defines using a computer or computer network within Virginia as conferring jurisdiction in Virginia. Given that the bulk of U.S. (and perhaps the world's) Internet traffic passes through Virginia, this gives Virginia broad authority. Both criminal and civil actions may be brought under the law, including by individual recipients.



**ALLIANCE
LAW GROUP_{LLC}**

www.AllianceLawGroup.com

How to Deal With the Problem

- **Broad Jurisdictional Provisions (cont.)**
 - **E.g., Australia: THE SPAM ACT OF 2003**

Prohibits the sending of commercial e-mail to recipients without their consent. Requires that the e-mail contain accurate information about the sender & a functional way for the recipients to unsubscribe. Use of electronic address harvesting software or lists which have been generated using such software is prohibited for the purpose of generating unsolicited e-mail messages. Applies to e-mail sent from Australia & to e-mails sent to an address

How to Deal With the Problem

- **International Agreements & Cooperation -- Essential Due to the Worldwide Nature of the Internet**
 - **E.g, Council of Europe Convention on Cybercrime**
 - **Requires Members and other signatory states to adopt legislative and other measures necessary to establish as a criminal offense:**
 - **accessing a computer system without right;**
 - **intercepting without right non-public transmissions to or from a computer system**
 - **damaging, deletion, etc. of computer data without right**
 - **serious hindering without right of the functioning of a computer system by inputting, damaging, deleting, etc. computer data**

How to Deal With the Problem

- **International Agreements & Cooperation -- Essential Due to the Worldwide Nature of the Internet**
 - **E.g, Council of Europe Convention on Cybercrime (cont.)**
 - **producing, selling, importing, etc. devices that make it possible to conduct one of the activities otherwise prohibited by the law**
 - **the input, alteration or deletion without right of computer data resulting in inauthentic data with the intent that it be acted upon for legal purposes as if it were authentic (i.e., forgery) transmissions to or from a computer system**



**ALLIANCE
LAW GROUP_{LLC}**

www.AllianceLawGroup.com

How to Deal With the Problem

- **International Agreements & Cooperation -- Essential Due to the Worldwide Nature of the Internet**
 - **E.g, Council of Europe Convention on Cybercrime (cont.)**
 - **the causing of loss of property to another by input, alteration, deletion, etc. of computer data or interference with computer system with fraudulent or dishonest intent of producing without right economic benefit for oneself of another**



**ALLIANCE
LAW GROUP_{LLC}**

www.AllianceLawGroup.com

How to Deal With the Problem

- **International Agreements & Cooperation -- Essential Due to the Worldwide Nature of the Internet**
 - **E.g, Interpol Regional Working Parties on Information Technology Crime**
 - **Computer Crime Manual -- best practices guide for investigators**
 - **Computer Crimes Training Courses for investigators and enforcement authorities**
 - **Rapid Information Exchange System to quick notification of computer crimes to appropriate in various countries**



**ALLIANCE
LAW GROUP_{LLC}**

www.AllianceLawGroup.com

How to Deal With the Problem

- **Other Practical Steps**
- **Governmental & Private Sector**
 - **Security Policies** (*not common in the Middle East -- Daily Star, Oct. 7, 2004*)
 - **Software and Hardware Defenses** (e.g., antispam, antivirus software, firewalls)

Next Steps in Lebanon

- **Legal Advisory Committee of Ecomleb (advising Ministry of Economy & Trade) at work on recommendations, which will include measure on data privacy, security, etc.**
- **Cyber crime can remove or destroy substantial amounts of economic value from the Internet, thus increasing costs, consuming resources, discouraging new investment, or causing a loss of confidence in the Internet. Thus it's important to move forward on such things as the initiatives at the Ministry of Economy & Trade.**



**ALLIANCE
LAW GROUP_{LLC}**

www.AllianceLawGroup.com