



Cyber Threats and Security Standards

Jody R. Westby, Esq.
St. Mary's Center on Terrorism
May 1, 2009

www.globalcyberrisk.com

The International Legal Landscape

- Cybercrime, Privacy & Cyber Security Are Global Issues
- 233 Countries Connected to Internet; 1.5 Billion Online Users
- Cybercrime, Privacy & Security of Information Infrastructure Important to National & Economic Security Interests & Public Safety
- Industrialized Countries Addressing; Developing Countries Lagging
- International Legal Framework Highly Inconsistent
- Cyber Security Investigations & Response Impacted by Legal Differences in Cybercrime Laws

2

WWW.GLOBALCYBERRISK.COM

© GLOBAL CYBER RISK LLC



Cybercrime is More Sophisticated

- Cybercrimes increasingly involve organized crime
- Hacking, Use of Botnets, Insider Theft/Sale of Data
- Government Activity Increasing
- Estonia and Georgian Incidents Raised Awareness

3

WWW.GLOBALCYBERRISK.COM

© GLOBAL CYBER RISK LLC



Terrorism is Flourishing

Terrorism is flourishing through terrorists' use of ICTs in a globally connected world with over 1 B online users and 233 countries connected to the Internet

Due To:

- Difficulties in tracking & tracing cyber communications
- Lack of globally-accepted processes & procedures for investigation of cyber communications
- Inadequate & ineffective information sharing systems between public and private sectors

4

WWW.GLOBALCYBERRISK.COM

© GLOBAL CYBER RISK LLC



Problems Associated With International Investigation & Cooperation

- **Disparities in legal frameworks**
 - Inadequate & inconsistent cybercrime laws
 - Inconsistent government access to communication traffic data
- **Borders & jurisdictional issues**
 - Letters rogatory v. multilateral assistance treaties (MLATs)
 - Dual criminality requirements
 - Conflicts of laws
 - Extradition hurdles
 - Procedural laws and evidentiary rules
- **Lack of expertise of law enforcement, prosecutors, judges**
 - Investigative and prosecutorial assistance
 - Search and seizure of electronic records
- **Inadequate mechanisms and procedures for international cooperation**
 - CoE Cybercrime Convention & EU Framework Decision created lethargy re closing legal gaps

5

WWW.GLOBALCYBERRISK.COM

© GLOBAL CYBER RISK LLC



Problems Associated With Information Sharing

Information sharing is crucial for detection, prevention, mitigation & response to cyber attacks and terrorist activities

Requires

Public/private sector commitment
 Systems & networks
 Security technologies & protocols
 Tested & trusted policies & procedures

methods

Problems

Cultural Issues
 Mutual recognition of clearances
 Reputational concerns
 Legal issues
 Protection of sources &

6

WWW.GLOBALCYBERRISK.COM

© GLOBAL CYBER RISK LLC



Cybercrime Laws Protect Citizens

- Help Protect Freedom of Expression, Human Rights, & Other International Rights
- Enhance Statutory & Constitutional Rights (rights to privacy, protections on search/seizure & self-incrimination)
- Help Ensure Citizen Use of ICTs, Access To & Exchange Of Information
- Strengthen Consumer Confidence Against Fraud

7

WWW.GLOBALCYBERRISK.COM

© GLOBAL CYBER RISK LLC



Cybercrime Laws Important to Developing Countries

- Confidentiality, Integrity, & Availability of Data & Networks Central to Attracting Investment and ICT Operations
- Protect Integrity of Government & Reputation of Country
- Instill Market Confidence & Certainty Regarding Business Operations
- Provide Protection for Protected Information & Facilitate Cross-Border Data Flows
- Protect Consumers & Assist Law Enforcement, Intelligence Gathering
- Deter Corruption & Fraud
- Increase National Security & Reduce Vulnerabilities
- Provide a Means for Prosecution and Civil Action for Cybercrimes
- Increase the Likelihood Electronic Evidence Will be Obtained

8

WWW.GLOBALCYBERRISK.COM

© GLOBAL CYBER RISK LLC



Cybercrime Laws Important to All

- Substantive Provisions Can Raise Conflict of Laws Issues
- Procedural Provisions Can Impede Investigations, Impair Use of Evidence
- Search & Seizure of Electronic Evidence Needs Consistency
- Mutual Assistance Needed for Tracking & Tracing, Investigations
- Jurisdictional and Extradition Issues Can Be Problematic

9

WWW.GLOBALCYBERRISK.COM

© GLOBAL CYBER RISK LLC



Consistent International Legal Framework is Emerging

- UN, G8, OECD, Council of Europe are Global Leaders
- CoE Convention on Cybercrime
- EU Ministers of Justice adopted the Proposal for a Council Framework Decision on attacks against information systems on March 4, 2003
- U.S., Other Developed Nations

10

WWW.GLOBALCYBERRISK.COM

© GLOBAL CYBER RISK LLC



Areas With Need for Harmonization

- Definitions
- Jurisdictional Provisions
- Substantive Provisions
- Procedural Provisions
- Mutual Assistance

11

WWW.GLOBALCYBERRISK.COM

© GLOBAL CYBER RISK LLC



Definition & Scope

- Vary in Definition, Form, and Penalties
- Industrialized Nations' Laws Protect Computer & Communication Systems and Data Transiting & Residing In These Systems
- Cybercrime Laws Generally Apply To:
 - Use of computers & Internet for illegal purposes (viruses, hacking, unauthorized acts)
 - Crimes against communication systems
 - Crimes facilitated by the use of a computer
 - Wiretap, pen register, and trap and trace laws to protect privacy and facilitate investigations

12

WWW.GLOBALCYBERRISK.COM

© GLOBAL CYBER RISK LLC



Jurisdictional Issues

- Possible for Cyber Criminal to be Physically Located in One Country, Weave an Attack Through Multiple Countries & Computers, and Store Evidence on Servers in yet Another Country
- Victims May be All Over Globe, Jurisdiction Questionable
- Internet Borderless but Law Enforcement Must Stop at Borders
- Substantive & Procedural Laws of Countries May Conflict, Creating Evidentiary Issues
- Letters Rogatory & Multilateral Assistance Treaties (MLATs)
- Dual Criminality Requirements Very Problematic
- Needs to be Way to Secure Extradition; Extradition Treaties One Method

13

WWW.GLOBALCYBERRISK.COM

© GLOBAL CYBER RISK LLC



Substantive Provisions

- Unauthorized Access to Computers, Networks, Data
- Interference and Disruption
- System Interference
- Interception of Traffic Data, Content
- Malware & Misuse of Computers, Programs, Passwords
- Digital Forgery & Digital Fraud
- Extortion
- Aiding, Abetting & Attempting
- Corporate Liability

14

WWW.GLOBALCYBERRISK.COM

© GLOBAL CYBER RISK LLC



Procedural Provisions

- Within Procedural Conditions & Safeguards
- Preservation of Stored Data, Traffic Data, Computers or Storage Media
- Production of Data
- Search and Seizure of Stored Data
- Interception of Traffic Data, Content Data
- Requirements May Vary: Upon Court Order, Search Warrant, Subpoena

15

WWW.GLOBALCYBERRISK.COM

© GLOBAL CYBER RISK LLC



Mutual Assistance

- Cyberspace Has No Borders, But Law Enforcement, Diplomats, & Investigators Do
- Interpol and Europol are Important Global Links
- Interpol & Europol Do Not Investigate: Passes Requests from Country to Country
- Interpol has National Central Bureaus in Each Country
- Investigation, Information Sharing, Search & Seizure

16

WWW.GLOBALCYBERRISK.COM

© GLOBAL CYBER RISK LLC



Judicial & Statutory Common Protections for Live Interceptions

- Approval Should Be Obtained from Independent Official (Judge) Based on Written Application and Manifested in Written Order
- Approval Should Be Granted Only Upon Strong Factual Showing of Reason to Believe That the Target of the Search is Engaged in Criminal Conduct & Less Intrusive Methods Not Adequate
- Each Surveillance Order Should Cover Only Specifically Designated Persons or Accounts; Generalized Monitoring Should Not Be Permitted
- Rules Should Be Technology Neutral
- Scope & Duration of Interception is Limited to Only What is Necessary to Obtain Evidence
- In Criminal Investigations, Those Who Have Been Subject of Interception Should be Notified When Investigation Concludes (Whether Charged or Not)
- Personal Redress or Suppression of Evidence at Trial is Provided for Violations

17

WWW.GLOBALCYBERRISK.COM

© GLOBAL CYBER RISK LLC



ITU Toolkit for Cybercrime Legislation Project

- American Bar Association Privacy & Computer Crime Committee (Section of Science & Technology Law)
- Produce Draft Law & Explanatory Comments
- Same/Similar Format as UNCITRAL Model Laws (Electronic Commerce & Electronic Signatures)
- ITU to Make Available to Developing Countries to Help Them Establish Legal Frameworks

18

WWW.GLOBALCYBERRISK.COM

© GLOBAL CYBER RISK LLC



Participants

- Multidisciplinary
 - Industry, Policy Experts, Academicians, Government Personnel, Technical Experts, Attorneys)
- International (Canada, Germany, India, Israel, Latvia, Japan, Mexico, Nigeria, Pakistan, Sri Lanka, UK, US)
- No Cost to Participate, Open to Interested Persons

19

WWW.GLOBALCYBERRISK.COM

© GLOBAL CYBER RISK LLC



Approach

- Develop Matrix of Provisions of Laws (Council of Europe + 10 Developed Nations)
- Comparative Analysis of Laws
- Working Groups by Topic Areas
- Teleconferences (Skype) & Email
- Drafting Toolkit & Explanatory Comments
- Review & Editing Across Working Groups
- Completion Date: February 2009

20

WWW.GLOBALCYBERRISK.COM

© GLOBAL CYBER RISK LLC



Overall Goal of ITU Toolkit

Develop Toolkit for Cybercrime Legislation that Will Promote Global Harmonization & Assist Developing Countries In Establishing Legal Frameworks for Cyber Security

21

WWW.GLOBALCYBERRISK.COM

© GLOBAL CYBER RISK LLC



Ability to Counter Threat Often Depends Upon Security Program

- Logging of System Activity May be Inadequate
- Lack of Key Personnel and/or Clear Roles & Responsibilities
- Inadequate Policies and Procedures
- Lack of Effective Controls and Enforcement
- Security Tools are Not Within Best Practices and Standards
- Inadequate Procedures for Incident Response
- Failure to Preserve Evidence
- Evidence Not Usable in Court

22

WWW.GLOBALCYBERRISK.COM

© GLOBAL CYBER RISK LLC



Security Standards

- ISO
 - 27001 – Information Security Management
 - 27002 – Information Security Techniques (formerly 17799)
 - 13569 – Financial Services Information Security
 - 38000 – IT Governance
 - 15408 – IT Security Evaluation (Common Criteria)
 - 18045 – Security Evaluation Techniques (for 15408)
 - 18014 – Security Techniques – Time Stamping Services
 - 11770 – Security Techniques – Key management asymmetric encryption
 - 9798 – Security Techniques – Entity authentication using symmetric algorithms
 - 19772 – Security Techniques – Authenticated encryption

23

WWW.GLOBALCYBERRISK.COM

© GLOBAL CYBER RISK LLC



Security Standards

- Information Security Forum – Standard of Good Practices in Information Security
- Payment Card Industry Standard
- COBIT (Control Objectives for Information & Related Technology)
- NIST (US National Institute of Standards & Technology)
- ENISA (European Network & Info Security Agency)
- ITIL (Information Technology Infrastructure Library – UK)
- ITU Standards Setting Bodies

24

WWW.GLOBALCYBERRISK.COM

© GLOBAL CYBER RISK LLC



ISO 27001 Security Standard

- ISO 27001 – Information Security Management
 - Issued in 2005
 - Specifies requirements for establishing, implementing, maintaining, and reviewing information security management system within the context of an organization's overall business risks
 - Can be used to manage risks, ensure compliance
 - Helps with implementation and management of controls to ensure security objectives are met
 - Defines information security management processes
 - Can be used to determine status, maturity of information security management program

25

WWW.GLOBALCYBERRISK.COM

© GLOBAL CYBER RISK LLC



ISO 27002 Security Standard

- ISO 27002 – Information Security Techniques
 - Issued in 2005; Former ISO 17799
 - Establishes guidelines and general principles for establishing, implementing, and maintaining information security program
 - Contains best practices and control objectives for
 - Security policy
 - Asset management
 - Communications and operations management
 - Access control
 - Incident management & business continuity
 - Information systems acquisition, development, and maintenance
 - Personnel and physical security

26

WWW.GLOBALCYBERRISK.COM

© GLOBAL CYBER RISK LLC



ISO 27005 Security Standard

- ISO 27002 – Information Security Risk Management
 - Issued in 2008
 - Supports 27001
 - Guidance on implementing information security based on risk management approach
 - Applicable to all types of organizations

27

WWW.GLOBALCYBERRISK.COM

© GLOBAL CYBER RISK LLC



ISO 27006 Security Standard

- ISO 27006 – Requirements for Bodies Providing Audit & Certification of Information Security Management Systems (ISMS)
 - Issued in 2007
 - Supports 27001
 - Requirements are to be demonstrated in terms of competence and reliability by any body providing ISMS certifications

28

WWW.GLOBALCYBERRISK.COM

© GLOBAL CYBER RISK LLC



ISO 38500 Security Standard

- ISO 38500 – IT Governance Standard
 - Issued in 2008
 - Provides guiding principles for directors of organizations and senior management on the effective, efficient, acceptable use of IT in their organizations
 - Applies to governance of management processes and decisions

29

WWW.GLOBALCYBERRISK.COM

© GLOBAL CYBER RISK LLC



Countering Threats: Need Harmonized Laws & Adherence to Best Practices & Standards

- Cyber Threats from Terrorist, Bad Actors & Nation States Require
 - Harmonized Legal Framework
 - International Mutual Assistance
 - Public and Private Sector Cooperation (Governments, Providers, Companies, Citizens)
 - Private Sector Security Programs Adhering to Internationally Accepted Best Practices & Standards
 - Ongoing Support in Multinational Organizations, Standards Bodies
 - Multidisciplinary Participation in Every Forum

30

WWW.GLOBALCYBERRISK.COM

© GLOBAL CYBER RISK LLC



More Information

- ITU Global Cybersecurity Agenda
 - www.itu.int/osg/csd/cybersecurity/gca/
- ITU-D ICT Applications and Cybersecurity Division
 - www.itu.int/itu-d/cyb/
- Cybersecurity Resources and Activities
 - www.itu.int/ITU-D/cyb/cybersecurity/
- Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection
 - www.itu.int/ITU-D/cyb/events/
- Cybersecurity Publications
 - www.itu.int/ITU-D/cyb/publications/

31

WWW.GLOBALCYBERRISK.COM

© GLOBAL CYBER RISK LLC



More Information cont'd

- ABA Privacy & Computer Crime Committee Publications
 - International Guide to Combating Cybercrime
 - International Guide to Privacy
 - International Guide to Cyber Security
 - Roadmap to an Enterprise Security Program
- FREE to people in developing countries: Send email to westby@mindspring.com
- ITU Toolkit for Cybercrime Legislation
 - www.itu.int/ITU-D/cyb/cybersecurity/projects/cyberlaw.html

32

WWW.GLOBALCYBERRISK.COM

© GLOBAL CYBER RISK LLC



THANK YOU!

Jody R. Westby
westby@globalcyberrisk.com
202.255.2700

