Legal Foundation and Development: The Risk of Cybercrime and Its Impact on Africa

Joel Schwarz

Joel.schwarz@usdoj.gov

Computer Crime & Intellectual Property Section

Criminal Division, US Department of Justice

Some Facts and Figures

- March 31, 2006 report

Internet Users and Population Statistics for Africa

Africa	Population 2006 est.	Pop. % Global	Internet Users	Penetration %	% Users Globally	Use Growth 2000-2005
Total for Africa	915,210,928	14.1%	23,649,000	2.6%	2.3%	423.9%
Rest of the World	5,584,486,132	85.9%	999,214,307	17.9%	97.7%	180.3%
WORLD TOTAL	6,499,697,060	100.0%	1,022,863,307	15.7%	100.0%	183.4%

Economic Growth (and other societal benefits)

- Great potential for economic growth
  - e-Commerce
  - Attraction of foreign investment
  - Information processing industries
  - Development of small- and medium-sized enterprises
- All of these benefits rely on reliable and secure information networks
- All of these benefits are in danger if a country cannot provide
  - secure information networks for citizens and businesses
  - Ability to investigate abuse or misuse of those networks
  - Punishment of criminals who attack or exploit those networks

How Should Countries Respond To The Threat of Cybercrime?

- A Law Enforcement Perspective
  - How can we successfully investigate, prosecute, and convict people who use computers and the internet to commit crimes?
- **Best things to do to combat cybercrime**
  1. Adequate cybercrime and related laws
  2. Specialized law enforcement
  3. Connections with other countries

1. Creating and Improving Laws

- Every country needs effective laws, but how?
  - Laws that meet domestic demands
  - Drafting – New Law in a Vacuum; Adding the word “computer”
  - Global nature of cybercrime – need common framework and improved international cooperation
- Convention on Cybercrime
  - Sets forth a framework for states; substantive offenses, procedural laws, international cooperation
  - Adaptable to any legal system
  - Does not dictate particular statutory language or method of implementation
  - Instead, it sets out CAPABILITIES and allows maximum flexibility in implementation

An Overview of the Convention on Cybercrime (2001)

- Introduction
- Substantive Offenses
- Procedural Laws
- Enhanced Cooperation

- Caveat: this is an overview – for all the details, see the Convention itself

Substantive Offenses

- Attacks on Computers and Data
- Article 2 **- Accessing whole or part of a computer system, without right**
  - **hacking to steal credit card information**
- Article 3 - **Illegal Live Reading/Listening of Content: obtaining electronic communications, without right**
  - **E-mail or voice content**
- Article 4 - **Data Interference: deletion, modification or suppression of computer data, without right**
  - **hacking to delete company's customer database**
- Article 5 - **System Interference: serious hindering, without right, of the functioning of a computer system**
  - **"denial of service" attacks**
- Article 6 - **Misuse of Devices**

Substantive Offenses

- Computer Related Offenses
- Article 7 **- Computer-related Forgery: manipulating a computer without right resulting in inauthentic data, with intent it be acted upon**
- Article 8 - **Computer-related Fraud: manipulating computer data without right to cause loss of property to another**

Substantive Offenses

- Content Offenses
- Article 9 **- Offenses related to Child Pornography**
- Article 10 **- Offenses related to infringements of copyright and related rights**

Procedural Laws

- Article 16: **Expedited preservation of computer data for up to 90 day**
- Article 17 **- Expedited preservation and partial disclosure of traffic data**
- Article 18 **- Production Order for data stored by a provider**
- Article 19 **- Search and seizure of stored computer data**

Procedural Laws

- Article 20 **- Real-time collection of traffic data**
  - **IP Address, e-mail header information**
- Article 21 **– Real-time collection of the content of electronic communications**

Enhanced Cooperation: Providing Assistance

- Article 25: **Allows for emergency requests by phone, fax, email**
- Article 27: **Acts as a Mutual Legal Assistance Treaty (MLAT) where parties do not have an existing MLAT**

Enhanced Cooperation: Providing Assistance

- Article 29: **Expedited preservation of electronic data for foreign requests (with no dual criminality requirement)**
- Article 30: **Expedited disclosure of stored traffic data**
- Article 31: **Expedited seizure of stored content data**
- Article 35: **24/7 Network**

1. Creating and Improving Laws

- Review of draft legislation
  - In place with resources available to assist states
  - COE drafting/implementation assistance
  - CCIPS and other US efforts
  - Other countries (Europe and elsewhere)
- COE Open to accession by everyone
  - Increasing number of non-European countries have acceded to the Convention
- Communication, support and training is critical
  - Within government
  - With private sector
  - International

African Countries and the Convention on Cybercrime

- Botswana – In editing its draft law, Botswana used the Convention on Cybercrime as a model to compare against its own draft law, resulting in ways to improve the language/capabilities of the draft law (now pending in their legislature).
- Nigeria - Nigeria used the Convention on Cybercrime as a model for drafting and editing its own Cybercrime Act, ensuring that Nigeria's final draft included the substantive and procedural tools, and international cooperation capabilities, covered in the Convention. That Act which is now pending before Nigeria's legislature.

2. Specialized Law Enforcement

- Initial capability
- Building capacity
- Practical considerations – you can help!
  - Educating police, investigators, prosecutors, judges
  - Establishing procedures for preservation and collection of digital evidence
  - Working with service providers
  - Assisting investigators and prosecutors to successfully use digital evidence in trial

3. Connections with Other Countries

- Formal:
  - MLAT and Extradition Treaty
  - LE to LE (via LegAtt and RLA)
- Informal:
  - 24/7 Network
  - LE to LE cooperation (via direct networking/relationships)
  - ListServ's
  - Regional groups (e.g., Asia- APEC; Americas – OAS; Africa - ?)

In the interim, while formal mechanisms are worked out….

- **Begin to develop strategic alliances of all levels of law enforcement, private sector technical experts, prosecutors, academic institutions and private industry dedicated to confronting and suppressing technology-based criminal activity.**

U.S. Examples: USSS ECTF & FBI's Infragard

- Listserv – dialogue and assistance
- Quarterly meetings
- Time commitment – whatever you wish

What's going on in Africa… developing CC capability/laws?

- June 2006 -- 2 training workshops on cybercrime capacity-building
  - 20 sub-Saharan African nations attended
  - Each workshop was 1 week long (one in English/French)
  - attended by judges, policy-makers, senior LE officials and private sector

- Results of these workshops:
  - 2 additional African countries joined the 24/7 Network
  - CCIPS asked for legislative drafting assistance by workshop attendees
  - brought to light Sub-Saharan cybercrime-related legislative initiatives, a number of which are using the Convention as a drafting model
  - Increase in African region requests for case-related cooperation;
  - African-focused ListServ set up: AfricanCyberInfoNetwork@afrispa.org
    - allows people to share insights, seek help and guidance from each other, and update each other on in-country/region developments
    - you can join too! ListServ admin is at this workshop

Questions?