Bahrain’s Draft Law on Computer Crimes

Dr. Jameel Al Alawi
Economic Development Board
Jameel.alalawi@bahrainedb.com

Law is based on Cyber Crime Convention

- Based on Cyber-Crime Convention
- Advantages of modeling the law on the convention: conciseness, more consensus, Assistance from member countries in Investigating and Prosecuting Cybercrimes after (hopefully) acceding to the convention
- No extensive introduction of criminal offences as in some other countries in ESCWA Region
- Provisions of the convention’s Additional Protocol concerning the criminalization of acts of a racist and xenophobic nature committed through computer system (2003) not incorporated in the draft
Main Sources

- Convention on Cybercrime 2001
- US Federal Act on Computer Fraud and Abuse Act 1986 (Modified in 1994, 1996, 2001, 2006)- The latest modifications were through the infamous Patriot Act

Approach.... 1

Offences:
Criminalize certain acts where:

- The computer is the subject of a crime (e.g. viruses, wars, trojan horses, logic bombs, denial of services attacks, hacking)
- The Computer is the object of a crime
<table>
<thead>
<tr>
<th>Approach …..2</th>
</tr>
</thead>
<tbody>
<tr>
<td>- No Copyright Related Offences under proposed Computer Crimes Law</td>
</tr>
<tr>
<td>- Copyright Related Offences are covered under Copyright and Neighboring Rights Law (2006)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Approach …..3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Procedural Matters :</td>
</tr>
<tr>
<td>- Introduce suitable procedural provisions &amp; ensure words within the procedural law that are unsuitable for computer crimes are appropriately adapted.</td>
</tr>
<tr>
<td>- No effect to the provision on international cooperation as Bahrain is not yet party to the convention.</td>
</tr>
<tr>
<td>Offences</td>
</tr>
<tr>
<td>----------</td>
</tr>
</tbody>
</table>
| - Unauthorized access  
- Interference with data or system causing damage (include damaging, altering, rendering useless, obstructing, denying access, ...etc)  
- Interference with data or system causing serious damage (e.g. health, public utilities, physical injury, medical diagnosis or tests)  
- Unauthorized interception of data |

<table>
<thead>
<tr>
<th>Offences.....Cont.</th>
</tr>
</thead>
</table>
| - Threatening to cause damage to computer data or system (extortion)  
- Misuses of devices (e.g. program or password) used to commit any of the computer crimes. The offence extends to possession, production and procuring.  
- Child pornography (Why only child pornography?)  
- Forgery  
- Fraud   
**Mens Rea: Always intentional & without authority.** |
### Special Procedural Provisions

**Applicable to:**
- Computer crimes prescribed in the Computer Crimes Law
- Any other crime committed using a computer system

### What are the Special Procedural Provisions?

- Power to order expedited preservation of stored computer data (includes ordering any person who can do so and demand confidentiality under criminal sanction)
- Power to order production of data (including subscriber's information)
- Search and Seizure of computer data (includes access to another computer system where lawfully possible through the original system, order any person to assist in facilitating access)
- Preserve traffic data and partial disclosure thereof (to identify the route and ISP involved)
### Procedural Matters ...Cont.

- Real time collection and recording of traffic & content data
- Provide information to enable access to a system, search and preserve.
- Power to compel person directed to execute the order to maintain its security (under criminal sanction)
- Special powers to Attorney General under other laws on collection/monitoring are intact (counter-terrorism law)

### The Penalties

- Can be substantial
- Corporate liability
- Half the penalty for attempt
- Full penalty for aiding and abetting
E-Evidence & Crimes

- Current situation not very satisfactory (probably all ESCWA Region)
- What is Caffrey Case (UK)?
- Jurists and Law Enforcement Agencies should look into this issue and consider the experience of other developed counties
- Examples: Good Practice Guide for Computer-Based E-Evidence (UK Police)
- & Searching and Seizing Computers and Obtaining E-Evidence in Criminal Investigation (USA DOJ)

Investigatory/procedural matters

- how to seize evidence on computers without contaminating it.
- how to preserve data in case the owner had sent out a kill program to destroy it.
- how to track down the originators of a message, particularly when encrypted or using anonymizers.