Cyber crime and international law

- At the international level two new treaty instruments provide a sound basis for the essential cross-border law enforcement cooperation required to combat cyber-crime. The first of these instruments, the Council of Europe's (CoEs) Cyber-crime Convention, is purpose built and although designed as a regional mechanism has global significance. The second is the United Nations (UN) Convention against transnational organized crime, which is global in scope but indirectly deals with cyber-crime when carried out by criminal networks in relation to serious crime.

- a UN draft resolution in 2003 at the 58th session of the General Assembly (GA) on "Cybersecurity and the protection of critical information infrastructures“.
- The passage of the CoE's Cyber-crime Convention in December 2001 and its activation in July 2004 provides for the first time an international legal mechanism for cooperation in law enforcement and harmonisation of laws

International treaties

- Forty-two states have signed the Convention (including non-council member states: Canada, South Africa, Japan and the USA) but as of 2005 only 11 states had ratified the convention.
- The cumbersome nature of treaty ascension processes the ratification and activation (a minimum of five ratifications are necessary) of this Convention in less than three years has been extraordinarily rapid.
- The Convention's "First Additional Protocol to the Convention on Cyber-crime on the criminalisation of acts of a racist or xenophobic nature committed through computer systems" that extends "content" cyber-crime to include "hate speech" as well as child pornography has been signed by 25 states and awaits the ratification process.

- The Convention, apart from enhancing MLA, provides comprehensive powers to expedite preservation of stored computer data and partial disclosure of traffic data;
- to make production orders; to search computer systems;
- to seize stored computer data;
- to enable real-time collection of traffic data;
- and to intercept the content of questionable electronic data.

- Beginning with the Eighth UN Congress on the Prevention of Crime and the Treatment of Offenders in 1990, the UN, with its network of institutes on crime prevention and criminal justice, has been actively involved in addressing problems of transnational crime and cyber-crime.

United Nations Convention against transnational organized crime

- The TOC Convention significantly extends the reach of the 1988 Vienna Convention against illicit traffic in narcotics and psychotropic substances.
- The TOC Convention enables establishes several offence categories:
- participation in an organised criminal group, money laundering, corruption and obstruction of justice as well as protocols in respect to trafficking in women and children (117 states and 64 parties with effect from 25 December 2003);
- illicit manufacturing and trafficking in firearms (52 states and 22 parties but not yet in force);
- and smuggling of migrants (112 states and 57 parties with effect 28 January 2004).
- Serious crime is defined broadly (conduct attracting punishment of four or more years' imprisonment).

TOC

- The TOC Convention, defines an offence as "transnational" if it is:
- " committed in more than one state;
- " committed in a single state but planned, prepared, directed or controlled in another state";
- committed in one state but involving an organised group whose activities cross national boundaries;
- committed in a single state but has "substantial effects" in another state.

“serious crime”

- "serious crime" (as defined in the Convention), "where the offence is transnational in nature and involves an organized criminal group“.
- Every cyber crime is "serious crime" because such offences usually affect more than a single jurisdiction, often involve at least three or more actors, and are committed with the aim of achieving some financial or material benefit.

The Council of Europe Cyber-crime Convention (1949)

- The CoE, founded in 1949, comprises 45 countries, including the members of the EU (a separate entity), as well as countries from Central and Eastern Europe. Headquartered in Strasbourg, France, the CoE was formed as a vehicle for integration in Europe, and its aims include agreements and common actions in economic, social, cultural, legal and administrative matters.
- As one of the two principal supranational organisations in Europe (the other being the EU), the CoE is responsible for creating and implementing a wide variety of measures aimed at international crime and has adopted a number of widely used conventions on interstate cooperation in penal matters.
- In 1996, the CoE's European Committee on Crime Problems established a committee of experts to address cyber-crime, which completed its work late in 2001.

- The resulting Cyber-crime Convention has three aims: to lay down common definitions of certain criminal offences - nine are mentioned in the Convention - thus enabling relevant legislation to be harmonised at national level;
- to define common types of investigative powers better suited to the information technology environment, thus enabling criminal procedures to be brought into line between countries; and
- to determine both traditional and new types of international cooperation, thus enabling cooperating countries to rapidly implement the arrangements for investigation and prosecution advocated by the Convention in concert, for example, by using a network of permanent contacts.

- The Convention, has received strong support from lawmakers and practitioners throughout Europe and beyond. But both the Convention and its additional protocol have been criticised on various grounds by a number of associations, particularly those active in the protection of freedom of expression, and also by industry elements.
- The CoE Convention on Cyber-crime (the "Convention") obligates signatories to criminalise a minimum list of specific offences where there was consensus and thus harmonised offences to eliminate problems of dual criminality.
- The basic structure and content of the convention is outlined below. The CoE Convention on Cyber-crime (the "Convention") obligates signatories to criminalise a minimum list of specific offences where there was consensus and thus harmonised offences to eliminate problems of dual criminality.
- The basic structure and content of the convention is outlined below.

Computer-related offences: Title 1

- addresses offences against the confidentiality, integrity and availability of computer data such as:
- * illegal access of a computer system;
- * interception of non-public transmissions of computer data to, from, or within a computer system;
- * interference with computer data;
- * interference with computer systems, such as computer sabotage; and
- * the misuse of computer-related devices (e.g. "hacker tools"), including the production, sale, procurement for use, import or distribution of such devices.

- Title 2 covers the traditional offences of fraud and forgery when carried out through a computer system. For forgery, the intent of this provision is to protect computer data in the same manner as tangible documents, where such data may be acted upon or used for legal purposes.
- Title 3 seeks to control the use of computer systems as a vehicle for the sexual exploitation of children and acts of racists or xenophobic nature. This category of offences concerns the subject or contents of computer communications and focuses on offences related to children. The Convention makes various acts (from the possession to the intentional distribution of child pornography) criminal offences, thus covering all links in the chain. This provision criminalises various aspects of the electronic production, possession and distribution of child pornography.

- **Title 4** criminalises wilful infringements of copyright and related rights when such infringements have been committed by means of a computer system and on a commercial scale. This section targets the large-scale distribution of illegal copies of works protected by intellectual property rights (TPR). Infringements of IPR, in particular of copyright, are among the most commonly committed offences on the internet, and cause concern both.

- Jurisdiction Among the various important matters addressed by the Convention, was the question of jurisdiction in relation to information technology offences, for example, to determine the place where the offence was committed and which law should accordingly apply, including the case of multiple jurisdictions and the question of how to solve jurisdictional conflicts. This provision establishes criteria under which contracting parties are obliged to establish jurisdiction over the criminal offences in the Convention. The provision concerning jurisdiction also requires states exercising jurisdiction to coordinate when victims are located in different countries.

- The Convention also creates the legal basis for an international computer crime assistance network, a network of national contact points permanently available (the "24/7 network").
- The network established by the Convention is based on experience gained from the network created by the G8 and co-ordinated by the US Department of Justice.
- Under the Convention, states are obligated to designate a point of contact available 24 hours a day, seven days a week, in order to ensure immediate assistance to investigations within the scope of the Convention. The establishment of this network is one of the most important provided by the Convention to ensure states can respond effectively to the law enforcement challenges posed by computer crime. This network will supplement the more traditional channels of cooperation. Each national 24/7 contact point is to either facilitate or directly carry out technical or legal advice, preservation of data, collection of evidence, and locating of suspects. The Convention also requires that national network team be properly trained to respond to computer-related crime.

Budapest Convention: scope

Criminalising conduct

- Illegal access
- Illegal interception
- Data interference
- System interference
- Misuse of devices
- Fraud and forgery
- Child pornography
- IPR-offences

Procedural tools

- Expedited preservation
- Search and seizure
- Interception of computer data

+

International cooperation

- Extradition
- MLA
- Spontaneous information
- Expedited preservation
- MLA for accessing computer data
- MLA for interception
- 24/7 points of contact

Harmonisation

The only binding international instrument and guiding legislative tool in the fight against Cybercrime

Budapest Convention: The role of the Cybercrime Convention Committee (T-CY)

(Committee of Parties to the Budapest Convention)

Established under Article 46 Budapest Convention

Membership (November 2016):

- 50 Members (State Parties)
- 17 Observer States
- 12 organisations (African Union Commission, Commonwealth Secretariat, ENISA, European Union, Eurojust, Europol, INTERPOL, ITU, OAS, OECD, OSCE, UNODC)

Functions:

- Assessments of the implementation of the Convention by the Parties
- Guidance Notes
- Draft legal instruments

Two plenaries/year as well as Bureau and working group meetings

- ► An effective follow-up mechanism;
- ► The T-CY appears to be the main inter-governmental body on cybercrime matters internationally

2013: Need to enhance capacities at the Council of Europe for capacity building on cybercrime and electronic evidence

- **Decision by Committee of Ministers (October 2013) to establish a dedicated Programme Office in Bucharest, Romania**
- **Operational as from April 2014**
- **Currently 19 staff**
- **Task: Support to countries worldwide to strengthen criminal justice capacities on cybercrime and electronic evidence**

- Apart from widespread global efforts to suppress child pornography (De Schrijver et aL, 2004) little progress outside of Europe may be expected in relation to the kinds of hate crimes captured by the additional protocol.

HKSAR v Sum Cheuk Wa, FLS 700017/2003

- A 14-year-old Hong Kong boy was arrested for creating a false web site, purportedly authorised by a well-regarded local newspaper. He posted on that web site false information concerning the SARS epidemic, stating that Hong Kong would be declared a closed port. This caused widespread panic in the Hong Kong community. One consequence was supermarkets were over-run by fearful citizens stocking up on foodstuffs to tide them over the quarantine of Hong Kong. Calm was only restored some hours later when the government issued repeated public announcements denying the rumour. The 14-year-old was convicted and placed under welfare care for 12 months. With these risks has come the awareness that "information security" is no longer a matter for the technical and computer specialist, but for millions of people who now engage these new media every day for business, communications and leisure.

- The "digital divide" between nation-states is growing rapidly and the role of "advanced" IT-based economies in bridging this divide is essential.