THE CONVENTION ON CYBERCRIME

- Gianluca Esposito
- Head of the Economic Crime Section
- Council of Europe

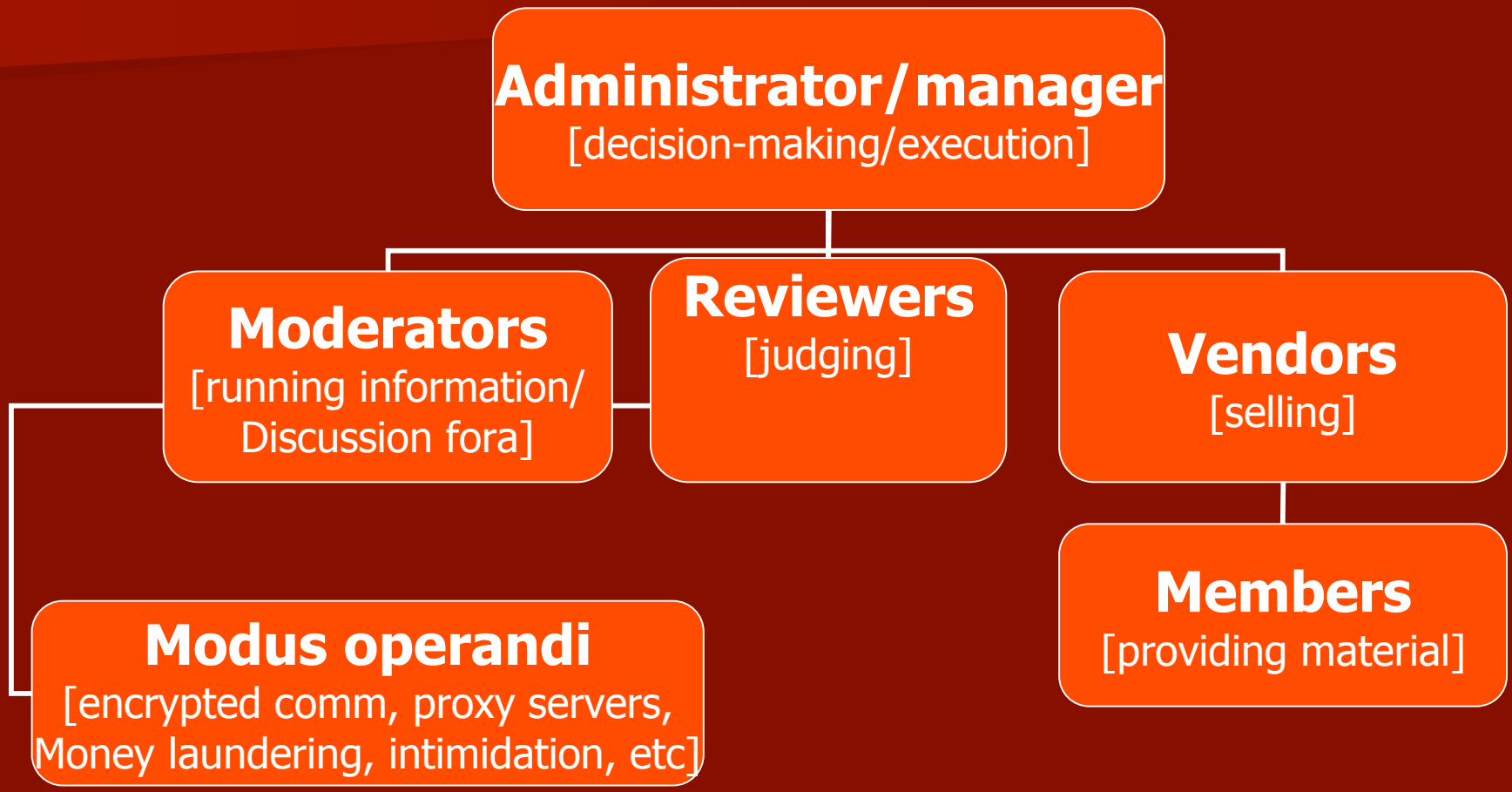
The extent of the problem

- Global economic damage from digital risks doubled from 2003 to 2004 (500 billion US$)
- In 2004, 71% of private & public organisations in Australia and 64% of companies in the US reported incidents
- By July 2004, 16% of attacks aimed at e-commerce
- Web site aiming at racism and xenophobia increased by 300% from 2000 to 2004
- Share of pirate software in 46 CoE member States ranged from 25% in Austria to 91% in Ukraine
- Child pornography on the Internet has an annual business volume of 20 billion US$ annually
- Symantec reports that the number of attacks blocked by their filters in December 2004 is 33 million per week

Characteristics of cybercrime

- The assumption that cyber offenders are usually acting individually and are juvenile and young adults is still valid
- However, we are increasing assisting to the development of organised forms of cybercrime, which are not structured and which co-operate on an *ad hoc* basis (eg. extorsion, attackers using botnets, identity thefts, physhing, etc…)

Structure of organised cybercriminals



Objectives of the Convention

- to lay down common definitions of certain criminal offences;
- to define common types of investigative powers better suited to the information technology environment;
- to determine both traditional and new types of international co-operation.

« State of affairs »

- 31 States have signed the Convention
- 11 States have ratified it
- Entered into force on 1 July 2004
- Many States are joining the Convention (eg. France, Kazakhstan)

Who can become a Party ?

- Every country around the globe may become a Party to the Convention.
- It is currently the only binding international treaty in this field.

And how ?

- For accession, a country may contact the Secretariat of the Council of Europe (eg. the Council of Europe Treaty Office or the Department of crime problems). Upon the request of the interested State, the Secretariat of the Council of Europe will bring the matter to the Committee of Ministers of the Council of Europe, who is responsible for inviting this country to become a Party to the Convention.

The Offences

- offences against the confidentiality, integrity and availability of data or computer systems (eg. "hacking", "cracking" or "computer trespass “);
- computer-related offences (eg. fraud and forgery);
- content-related offences;
- offences involving the infringement of intellectual property and related rights.

Investigative tools

- Cover both the offences contained in the Convention and any other offence committed through, on and/or against computer systems.
- Investigative tools can be used in cases where an offence is committed by means of a computer system or in which evidence of a crime is electronic.

Investigative tool N° 1

- Expedited preservation of stored computer data: this applies to stored data which has already been collected and retained by a data holder, eg. an ISP. This tool only applies where computer data already exist and is being stored.
- This is an important new investigative tool, especially for crimes committed through the Internet, owing to the the volatility and possible manipulation of computer data and the potential risk of loosing evidence.

Investigative tool N° 2

- Production order: This enables the competent authorities to compel a person to provide specified stored computer data or an ISP to provide subscriber information. PO only applies to data which are stored and already exist.

Investigative tool N° 3

- Search and seizure of computer systems: this aims at modernising and harmonising legislation in the area of search and seizure of stored computer data with respect to specific criminal investigation or prosecution.
- Search and seizure in the net environment require special care as (i) data are in an intangible form and (ii) while data can be read in a computer, they can not be seized and taken away in the same sense as in the real world.

Investigative tool N° 4

- Real-time collection of computer data:
  - *real-time collection of traffic data*: data relating to a communication made by means of a computer system;
  - *interception of content data*: interception of the content of the communication, of the message or the information conveyed.

International co-operation

- Need for rapid action to gather evidence (volatile in the net environment)
- Legal basis for the 24/7 Network
- No need to create a new contact point: it can also be built in existing structures at a national level
- Needs for capability to provide investigative, as well as judicial, assistance around the clock

Monitoring

- ART. 46 -> Consultations of the Parties
  - Effective use and implementation of the Convention
  - Exchange of information on significant legal, policy or technological developments;
  - Consideration of possible supplementations or amendments to the Convention

Towards a global accession to the Convention on cybercrime

- **Europe** (CoE & EU)
- **OAS** (2004): "to evaluate the advisability of implementing the principles of the Council of Europe Convention on cybercrime (2001), and consider the possibility of acceding to that Convention".
- **Asia-Pacific**: Lima Ministerial Declaration of 3 June 2005: « enact…laws….consistent with the Convention on cybercrime …»
- **Africa**: 5th Interpol meeting of the WP on IT crime in Africa (May 2005): « All African countries shall be encouraged to consider joining the Convention on cybercrime ».
- **Commonwealth**: « …support the idea of joining existing 24/7 networks such as the one set up under the 2001 Convention on cybercrime ».
- **G8**: « encourage the adoption of the standards contained in the Convention on cybercrime on a broad basis… »
- **UN**: « …reaffirm the fundamental importance of implementing existing instruments….in particular against cybercrime… » (2005 Bangkok Declaration)

Conclusions

- Creating more then one international treaty against cybercrime with the same provisions risks to jeopardize the effectiveness of the existing treaty and to lower its standards
- WSIS should encourage global accession to the Convention on cybercrime

A global commitment