UN ISPAC Conference on the Evolving Challenge of Identity-related Crime
(Courmayeur , Italy, 30 Nov – 2 Dec 2007)

Identity theft and the Convention on Cybercrime

Presentation by Alexander Seger[1]

As societies worldwide are becoming highly dependent on information and communication technologies they are also increasingly vulnerable to cybercrime. This includes:

- Malware, that is, malicious codes and programmes including viruses, worms, trojan horses, spyware, bots and botnets
- Botnets which are one of the central tools of criminal enterprises (DDOS, extortion, placing of adware and spyware)
- Spam not only as a nuisance but also as carriers of malware
- The use of the internet for terrorist purposes (attacks against infrastructure, logistics, recruitment, finances, propaganda)
- The growing risk of cyber-attacks against critical infrastructure
- Child pornography and the increasingly commercial sexual exploitation of children on the internet
- Offenders who are increasingly organising for crime aimed at generating illicit profits
- A shift in the threat landscape from broad, mass, multi-purpose attacks to specific attacks on specific users, groups, organisations or industries, increasingly for economic criminal purposes.

Many forms of cybercrimes are related to identity theft in one way or the other, whether ID theft is defined as "the misuse of the identity (name, date of birth, address, financial information or other personal details) of another person without knowledge or consent" or as "assuming the identity of another person by stealing personally identifiable information (PII) to commit fraud" or as "the theft or assumption of a pre-existing identity (or significant part of it), with or without consent, and regardless of whether the person is dead or alive".

Conceptionally, ID theft can be separated into three distinct phases:

1. The obtaining of identity information, for example, through physical theft, through search engines, insider attacks, attacks from the outside (illegal access to computer systems, trojans, key-loggers, spyware and other malware), or phishing and other social engineering techniques
2. The possession and disposal of ID information, which includes the sale of such information that now plays an important role in the e-underground economy where credit card information, bank account details, passwords or full identities are among the most offered goods
3. The use of ID information in order to commit fraud or other crimes, for example by assuming another person's identity to exploit bank accounts and credit cards, create new account, take out loans and credit, order goods and services or disseminate malware.

[1] Head of Economic Crime Division, Council of Europe, Strasbourg, France. The views in this paper do not necessarily reflect official positions of the Council of Europe. For further information see www.coe.int/cybercrime.

Action against identity theft in connection with cybercrime requires a multi-pronged approach involving:

- prevention (measures to be taken by individuals, data security in the public sector and in the private sector, measures to protect privacy and personal data)
- legislation (to criminalise illegal access, interception, data and system interference, misuse of devices, computer-related forgery and fraud; but also liability for data security and civil remedies)
- enforcement (facilitating reporting of ID theft, the investigation and prosecution of ID theft, the building of law enforcement capacities, coordination, intelligence and analysis, and public-private cooperation)
- extensive international cooperation, including the full implementation and accession to the Convention on Cybercrime of the Council of Europe.

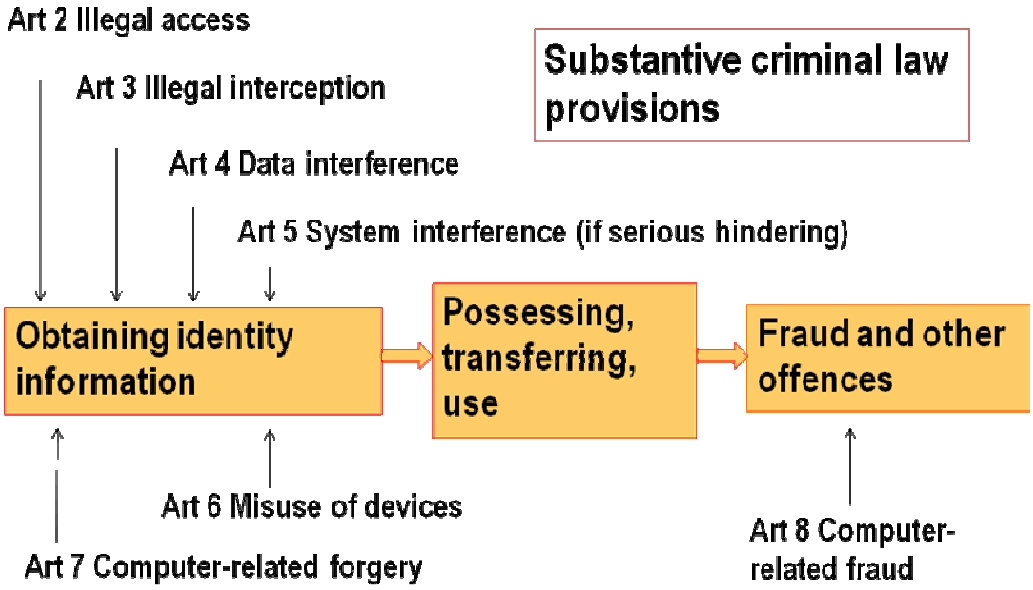
The Convention on Cybercrime is the only binding international treaty in this field. It was elaborated by the Council of Europe with the participation of Canada, Japan, South Africa and the USA, and opened for signature in Budapest in November 2001 (thus also known as the "Budapest Convention"). It is in force since July 2004 and has become a treaty with a global scope in that it serves countries worldwide as a guideline for the development of national laws against cybercrime, in that an increasing number of countries are moving towards accession and in that it serves the Parties to the Convention as a framework for international cooperation.

The Convention requires countries to criminalise certain conduct such as the illegal access to a computer system ("hacking", circumventing password protection, key-logging, exploiting software loopholes etc), the illegal interception (that is, violating the privacy of data communication), data interference (malicious codes, viruses, trojan horses etc), system interference (such as denial of service attacks through botnets and other means of hindering the lawful use of computer systems), the misuse of devices (including the development of tools to commit cyber-offences), computer-related forgery (including phishing attacks), computer-related fraud, child pornography, the infringement of copyright and related rights, and – in a separate protocol – hate speech, xenophobia and racism.

It asks countries to introduce a range of procedural law measures to give law enforcement and other criminal justice authorities the means to investigate, prosecute and adjudicate cybercrimes more effectively. Among other things this should allow for the possibility to take immediate action to preserve electronic evidence, to search and seize computer data or to intercept communications, while putting the necessary safeguards in place to prevent abuse of such powers and unnecessary infringements of privacy, freedom of expression or other civil rights.

Finally, it provides for a range of measures for more effective international cooperation against cybercrime.

The Convention is focusing on criminal conduct and not on specific techniques or technologies. There are thus no specific provisions on identity theft. However, the full implementation of its substantive law provisions will allow States to criminalise conduct related to the first and third stages of the ID theft process:



With regard to substantive criminal law, the question that remains is whether the possession, disposal, sale or other use of ID information, that is, stage two of the process, is to be made a separate criminal offence, such as for example in the USA. In Europe, this question was also raised by the European Commission in a Communication in May 2007[2]. This will certainly trigger further discussions and possibly actions.

In addition to the substantive law provisions, the Convention offers further tools to facilitate criminal justice measures against ID theft committed through computer systems. The scope of the procedural provisions mentioned above is very broad and applies to any criminal offence involving a computer system. This means they can e used for the investigation of any conduct related to ID theft which is made a criminal offence in a country even if this conduct is not specifically mentioned in the Convention.

Finally, the chapter of the Convention on international cooperation is highly relevant as cybercrime is probably the most transnational of all crimes.

In conclusion, countries that are determined to take action against ID theft in relation to cybercrime should make every effort to implement the Convention on Cybercrime. This will help cover many needs in terms of substantive law, procedural law and international cooperation.

It is nevertheless worthwhile to continue the discussion as to whether in addition it is necessary to criminalise identity-theft as a separate offence or to develop a separate international instrument on the criminalisation of identity theft in general (that is not limited to the internet or computer systems), or whether the full use of the existing legal framework and a stronger emphasis on prevention would serve the purpose.

_____

[2] Communication from the Commission to the European Parliament, the Council and the Committee of the Regions towards a general policy on the fight against cyber crime, COM (2007) 267