INVESTIGATION OF CRIMES COMMITTED VIA ICT by the National Police Force.

National Police Force (CNP)
The Judicial Police Department
UDEF CENTRAL
Technological Investigation Brigade (BIT)

In 1995 the IT Crime Group was launched as part of the Economic and Financial Delinquency Brigade, of the General Judicial Police Department, in an attempt to provide a response to the attacks and infringement of rights arising from software piracy and a number of internet banking frauds.

In 2000 considerable impetus was given to this type of investigation into offences, in which new technologies were being employed to perpetrate crimes, thus the department grew from a small operations group to become a fully fledged unit with a more specifically defined remit, fulfilling the need to increase its scope of activity and coordinate investigations between the various departments of the National Police Force, relating to this specific criminal activity.

Thus in March 2000, within the framework of the Speciality matters of the Programme 2000, in an act presided over by the Ministry of the Interior, the Information Technologies Crime Investigation Unit was created (a rather long title which is not easy to remember). By 2002 it had developed into its current form as the Technological Investigation Brigade (BIT).

The Technological Investigation Brigade currently comes under the auspices of the Central Unit for Economic and Fiscal Crime (UDEF) and it is structured as follows: A Brigade Office headed by a Commissioner which is responsible for two Operational Sections led by two Chief Inspectors, each with various Operational Groups and a Technical Section led by an Inspector with technical departments.

Its specific duties include the following:

- Direct responsibility for particularly complex operations, either because they require special technical resources, or because they involve various Senior Departments.
- Carrying out and coordinating investigations originating abroad.
- International representation of the National Police Force in Matters of Technological Crime.
- Design and development and provision of training courses for members of the National Police Force and foreign Police Forces.
- National and international representation in various specialist Forums on Information and Communications Technologies and Cybercrime.
- The study of new strategies and protocols for investigation and action in matters of technological crime.
- Systematic internet tracing for crime prevention and investigation of crimes committed.

The chief objective of BIT members, as part of a central service like the UDEF is to strengthen the scope of investigation into organised crime as much as possible in all the areas and concerning the Brigade, which are as follows:

OPERATIONAL SECTION I:

1.1 – Child Protection Groups

These carry out investigations into the location of child pornography production centres which sell, distribute or exhibit or facilitate material using almost all the internet applications available including:

- Web pages with illegal content
- Peer to peer applications
- Grooming of children through chat rooms (messenger) or social networks
- Specific exchanges in FTP servers
- IRC
- E-mail
- Social Network Exhanges

The work of this group is based on prosecution of crimes relating to sexual exploitation of children when the medium is internet.

1.2 – Telecommunications use Fraud Group

This group deals basically with investigation into:

- Mobile and fixed line telephone fraud.
- Digital platform fraud (Cable TV decoders, Websites where passwords are published for access to content).
- Threats, calumny and slander from mobile to mobile telephone making use of internet servers and usurpation of civil status.

1.3 – Open Networks Group

This group is responsible for the following duties and tasks through continuous web browsing.

- DETECTING new “modus operandi”.
- COMPILATION of reports on activities which, though not criminal offences in themselves, may be harmful or dangerous particularly to children.
- COLLABORATION with C.N.P. units carrying out other investigations.

The content investigated includes specific violence, racism and xenophobia, brutal aggression and attacks on the moral integrity of individuals, particularly the incapacitated and minors.

Contents which contravene road traffic regulations, such as illegal racing on urban

circuits, where the races pose a serious and life threatening risk to citizens.

Those sites concerned with anorexia and bulimia which have no scientific basis and which can endanger lives.

Other content in general such as collective suicides, mistreatment of animals, and techniques for stealing from department stores and a long list of similar offences.

OPERATIONAL SECTION II:

2.1- Internet Fraud Groups

The type of crime investigated by these groups concerns fraud perpetrated on private individuals, companies or entities. As part of their fight against fraud they investigate other crimes such as falsification of documents, usurpation of civil status, money laundering etc. Some of the most well known offences prosecuted and dealt with by the internet fraud groups include:

- FRAUDULENT SALES AND ILLEGAL AUCTIONS ONLINE in which goods or products are purchased online, are paid for but are not received, or are delivered and the seller is not remunerated.
- EXECUTION OF FRAUDULENT ELECTRONIC TRANSFERS (EFT). In general this criminal activity which covers other complex issues that are individually considered, ranges from the discovery of passwords to online banking services (using techniques based on “Phishing”, “Pharming” or malicious programmes such as “Malware”); it continues with the control of other computers and their lines in order to access financial institutions, claiming to be clients, the withdrawal and transfer of money to “intermediate accounts” or ”mule” accounts and the placing in circulation of illegally obtained financial amounts.
- In the case of PHISHING activities are based on massive mailing simulating a financial institution. In the case of PHARMING computer programmes are used to alter domain name servers (DNS) which transform domain names into IP addresses so that they redirect users to the computer of the hacker, who is then able to discover their passwords. And in the case of MALWARE computers are taken over in an attempt to gain the users’ personal and financial information, and the hackers make fraudulent purchases or electronic transfers. Work and investigation of these illegal procedures are carried out jointly with the Logical Security Group.
- JOB OFFERS: these are designed to move money resulting from fraudulent transactions (using intermediaries captured through these fake job offers, who are known as mules) or either by requesting money in advance as the first steps to obtaining a good job.
- BANK CARDING is the fraudulent use of valid card numbers in e-commerce. The numbers are obtained in various ways (programmes which generate numbers, sales points, sale of batches of cards through the web

etc).
- OTHER FRAUDULENT PRACTICES: financial pyramids through internet.

2.2 – Logical Security Group

This Group investigates any action leading to the infringement of security measures in computer systems. These offences are commonly known as “hacker crimes". They include:

- Computer intrusion – attacks on computers in order to cause harm or discover or obtain protected data (crimes of damage or discover and disclosure of secrets).
- Dissemination of Viruses or malicious programmes in general.
- Denial of Service Attacks (DDOS) consisting of saturating a server with multiple requests in order to prevent it from functioning properly.

2.3 – Anti- piracy Group

Investigation into crimes against Intellectual and Industrial Property through internet.

INTELLECTUAL PROPERTY crimes online include those which are known as P2P downloads that is, downloads through file exchange programmes such as EMULE, TORRENT etc. This type of investigation is carried out on the orders of a court or public prosecutor.

As part of this procedure, investigations that have been carried out in the Brigade concentrated on those who run websites which facilitate downloading of illegal copies in exchange for considerable financial profits, based mainly on advertising placed on the web pages. Investigations are not directed against users, or against the file exchange applications.

Internet (through forums) sales of pirate copies, as well as unlawful installation of illegal software by commercial establishments are also investigated.

In respect of INDUSTRIAL PROPERTY counterfeit goods are also sold illegally through websites and forums.

This group also investigates a third criminal activity which is often closely linked to infringement of industrial property in the imitation of trademarks etc. – these are offences against public health (sale of medicines and health products) online. This activity is on the increase.

Furthermore, the new trend in Intellectual Property crime through internet and telecommunications is that of committing fraud through "Cardsharing" deals, defrauding the European Platforms which provide paid digital TV signals This criminal activity is investigated jointly by this group and the telecommunications fraud squad.

TECHNICAL SECTION:

The Technical Section carries out the following duties:

- Technical support to the other BIT groups and other Units (transferred technical reports of an operational nature, as the expert reports are carried out by the Computer Forensics section of the General Forensic Police Service).
- Training of National Police Force personnel and other national and foreign Police Forces.
- Participation in international forums (Interpol, Europol, Council of Europe etc).
- R+D+I into the tools and techniques of technological investigation.