EUROPOL

HIGH TECH CRIMES WITHIN THE EU:

OLD CRIMES NEW TOOLS, NEW CRIMES NEW TOOLS

Threat Assessment 2007

High Tech Crime Centre

PUBLIC VERSION

File Number: #247781

August 2007

TABLE OF CONTENTS

Introduction

The rapid development of technology has, in parallel, improved the possibilities to commit crimes. The Europol threat assessment on computer crime describes the scenario in this arena giving an overview of the most common crimes committed through the use of technology.

Besides the trouble in defining computer crime, cyber crime, and high technology crime, the common denominator is the use of technology to carry out criminal activities. Technology means not only devices but also services offered by providers. Computers may be the target or the means to commit crimes.

Nowadays the main target in high tech crimes is the violation of privacy and the theft of data which may be done in several ways. Hacking, phreaking, cracking of passwords, copyright infringement, phishing, identity theft, pharming, the spread of malicious codes, and child pornography images are just a few examples of ways in which criminals may perpetrate using technology. The use of the internet is the main vehicle in easing this criminal process.

Essentially the main aim for criminals is to gain money. Financial gain is the most important driving factor for criminals regardless of their activity: financial gain is the most common motivator, regardless of the culture or mindset of the offender. It is essential to understand how new technologies may be illicitly exploited for financial gains: *cyber crime is more profitable than many other crimes such as drugs trafficking*[1].

Even in the production and dissemination of child abuse images over the internet cases, financial gain is often the final goal of the criminal. Nowadays, the criminal profile of the offenders is divided in two: the real child abuser and the child pornographer. The latter is keener to produce child pornography images and sell them than to be a child abuser.

The financial market, through the birth of new and anonymous electronic means of payment, is accelerating the speed of money transfers all over the world. "Old fashioned" means of payments such bank transfers are slowly disappearing, being replaced by new form of electronic payments over the internet. In the same direction, security is moving in order to make the transaction safer, Secure Socket Layer (SSL)[2] is a typical example.

1 http://www.bwc.com.au/forum/viewtopic.php?p=31&sid=3afec005c882d992d53c0b0364642591 published 4 Dec 2005.

2 http://en.wikipedia.org/wiki/Secure_Sockets_Layer

Technology e.g. using Virtual Private Networks (VPN)[3] eases cooperative communication in terms of 'global villages'. This technical convergence can also be seen in the profiling of criminal organisations and their structure across vast geographical areas.

The convergence of services and devices causes a huge impact in several areas: just taking in consideration the push and pull factors in terms of money transfer in cases of money laundering over the internet or in cases of child pornography.

New forms of organised crime are rising especially with the enlargement of the European Union (EU). New and additional issues are becoming urgent mainly: technology development is always faster than laws and regulations. Issues like data protection, data retention, and protection of privacy are highly debated in every country. International organisations are trying to address the issue at political level in order to find a solution.

3 http://en.wikipedia.org/wiki/Virtual_private_network

Assessment Objectives

The report will try to outline computer threats and the challenges to be likely faced in the near future or are currently dealt with by investigative bodies. Due to the breadth of these phenomena the report will focus on some areas in order to better assess the threat of some crimes using high technology. Therefore, new tools and techniques will be described to clarify the real threat.

With the collection of as much data as possible the report will try to assess the capability of criminal organisation in threatening the citizens. This is still a blurred area because one of the main difficulties is to exactly assess how organised crime groups are active on the internet, although the use of high technology by criminal organisations has already been confirmed.

Typology

In order to make the study relevant to new trends and threats or to look deeper into some old crimes, the report investigates the following main areas deemed the most significant at the present time:

- The involvement of criminal organisations in high tech crimes
- Botnets and crimewares[4]
- Phishing
- Identity Theft
- Pharming
- Vishing
- SMiShing
- Critical Information Infrastructures
- Cyber terrorism
- Trafficking of Child Pornography Images on the Internet
- Drugs Trafficking on the Internet

4 Crimewares is the new trend in defining malicious codes spread over the internet.

Constraints

There currently are some outstanding challenges when writing a computer crime threat assessment. These include issues such as:

A Common Definition of Computer Crimes

Despite the effort made by legislators, researchers, and LEA personnel, it is still impossible to define what cyber crime, computer crime or high technology crime are. This is due to various reasons, such as:

- Different domestic legislation which apply in the MS and result in diverse approaches. Although the cyber crime convention was launched in 2001, it has only actually been ratified by a few countries and therefore this act cannot be considered to be a global legal point of reference yet.

- In particular, the cyber crime convention raises the problem of distinguishing computer crimes into five main separate categories:

  - crimes against the Confidentiality, Integrity and Availability of computer data and systems

  - computer related traditional crimes

  - content-related offences

  - offences related to infringement of copyright and related rights

  - infringement of privacy

By the way, this approach would seem to be the most appropriate or at least the most accepted by "computer crime stakeholders" because it encompasses all kinds of criminal cases in point.

- As domestic laws still apply, the procedural codes for operational activities also differ across the different European countries. Intelligence that would be admissible as evidence in one country might not be accepted in another one which is still a considerable constraint.

Preponderance of US Sources

As compared to the United States (US) that has a significant reporting mechanism in place Europe lacks such a structure. It also has to be recognised that the US is much more advanced in terms of technological development and thus the US market influences, substantially, all the others.

Information gathered from open sources is greatly influenced by the US market as this is where most of the articles are written and European reports are often just a total or partial translation from American ones. Therefore, it makes it very difficult to have a reliable European point of view on the current threat.

Lack of Reporting by the Victims

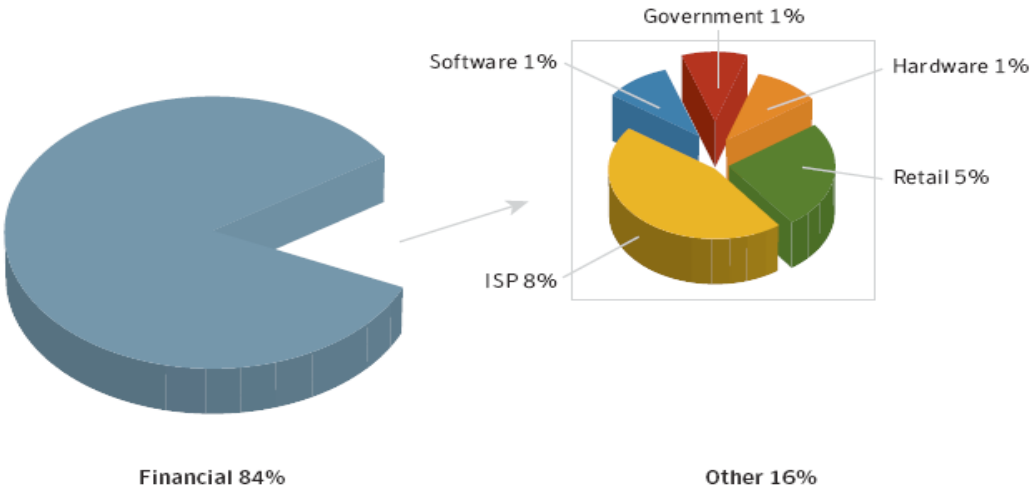
This is still one of the biggest constraints which impede a real assessment of computer crimes. Especially in cases of attacks to their computer systems, private companies are reluctant to report the crime to the police.

The reluctance is due to the likely damage to the reputation of the company resulting in a possible loss of market share. Therefore, private industry tends to internally absorb the losses by computer attacks without reporting the crime to LEA.

For example, being the main target of phishers, banks suffer mostly from this type of criminality. The main problem faced by police forces regarding this crime is that often the financial institutes or private sector in general do not report the crime, which makes it impossible to properly trace the suspects of these criminal activities. The reasons for not reporting reside in the fear of losing their reputation to their customers and, eventually, their market share, giving a competitive advantage to their rivals.

In the report produced by Symantec of last January-June 2006[5], the company underlines the worried statistics about the most targeted sectors for phishers:

5 http://www.symantec.com/enterprise/threatreport/index.jsp



Moreover there is a feeling with private industry that computer crime units do not respond quickly to their requests, in terms of:

- *Quick intervention as first responders*, as often the victim reports the incident at their local police station which does not have a specialist in computer crime; therefore an expert officer is needed in order to properly proceed.

- *Lack of understanding between the victim and the police*, as the first responder in the company is often not able to immediately provide the police with the evidences requested or simple does not understand what the investigator requires.

- *Discrepancy in goals*, as the victim, being a commercial entity, needs to re-state the computer system as soon as possible whilst the police look at it from a social aspect. This could cause tension as delay the process of recovery as some operational procedures have to be followed.

- *Lack of understanding in crime taxonomy*, as private companies do not care about the content of the penal code and which crime might have been committed as they just care about the consequences an attack may cause to their computer system in terms of disruptions and therefore economic loss.

In conclusion, companies actually prefer to set up a sort of internal investigation unit in order to immediately respond to the incident and avoid making their problems public.

Lack of Common Reporting System

The lack of common reporting system is an issue like the inconsistency of data about internet and its criminals' communities: it is very difficult to understand the interaction within hackers' communities unless an informant reveals information or an infiltration of LEA is possible within the group.

Moreover, the problem also lays down at the level of the collection of data: the Organised Crime is difficult to map because the Internet has no boundaries; information is too spread out and the collection of data is difficult: *unfortunately there is no standardised system of reporting computer crimes.*

Even at EU level the languages barrier should be taken in heavy consideration: currently there are 18 languages spoken. Eventually, this lack of common reporting system impedes the handling of information in an appropriate way both in terms of the content of the contribution and also the way the information is presented.

Methodology

In order to overcome the constraints mentioned above and to try to enrich the report with as much consistent information as possible, the following structure will be used:

- Questionnaire sent out to Member States
- Cases studies provided by HTCUs in EU
- Reports by LEA
- Reports by Europol
- Case studies by industry
- Reports by other international organisations
- Open-sources information

The Organised Crime in High Tech Crimes

When painting the picture of criminal organizations operating over the internet, difficulties arise for many reasons. A fundamental one is that the Internet has no boundaries and therefore catching all the relevant data is almost impossible. There is no unique reporting system or, even, one does not exist at all. Police forces, social scientists, security companies or other interested parties struggle to study the phenomena. Quantitative analysis is difficult to produce, with qualitative analysis being easier to come by.

For these reasons and for many others, the approach used to describe the threat from criminal groups over the internet follows the same concept as that of high tech crime already described: *vertical and horizontal uses of high technology*.

The vertical use of hi-tech occurs when the computer (or computer network) is the target of the criminal activity as the final goal. Spamming, hacking and crimewares are just some examples in which the presence of the machine is fundamental for the existence of the crime. The horizontal use of hi-tech is when the computer is instead utilized as a tool in order to facilitate criminals' goals.

The picture below depicts the scenarios:

In order to give some insights and to facilitate comprehension of the threat, this report aims to deal with the issue facing two parallel, but at many times convergent, subjects: *the communities of cyber criminals* and *the use of hi-tech by criminal organisations*.

In other words, one part will be dedicated to the organised groups who attack computer systems for various reasons in order to understand what kind of threats can be expected. The second part will focus on the use criminal organisations can make of high technology: utilising new tools and techniques or even using the skills of cyber criminals, recruiting or simply hiring them; in other words: *the horizontal use of hi-tech*.

Cyber Criminal Communities

There are many ways to define an 'intruder', all debatable. Blackhats, whitehats, crackers, samurai, lamers, script kiddies, newbies, hacktivists and many others can appear; these names have been given respecting different parameters such as meritocracy, status within the group, impact of their criminal actions, proven skills and so on.

The word "hacker" sometimes cannot even be strictly associated with a type of behaviour that clashes with an article mentioned in the penal code; but it can be linked to the concept of deviance that is just the credence in a society about the illegality of a certain behaviour categorised as illicit conduct.

Seeing the problem from the outside, there is only one common denominator in the whole issue: ***the impact caused by the criminal behaviour***. The public does not care very much about whether a hacker can steal a large amount of information from the computer system of commercial company, causing billions of Euros of damages in terms of security breaches and re-patching the system.

On the other hand, it is of public concern when, for example, just the website of a governmental institution is defaced, or when simply an attempt on a national information infrastructures' network is made by hackers. It seems that as long as we are not directly affected by the consequences of crimes, we do not much care about them.

It is very complicated to describe the culture (or at this point the subculture) of cyber criminal communities. When we study anthropological phenomena, we look for the origin of the groups and how they have evolved in order to make our conclusions.

Depicting the structure of these groups and their interactions is very difficult for many reasons, such as:

- the communities have not long been in existence
- there is little background information about them and even poorly recorded.

Points of reference could be the famous 'Jargon File'[6] or 'The Hacker's Dictionary'[7], freely accessible on the internet. But all the available data is nowhere near sufficiently exhaustive to give a true picture.

Hacker communities are difficult to analyse from inside unless we belong to them or we investigate them undercover, perusing the structure of the groups and their interactions. Externally, there is little chance to assess the effective potential of a criminal cyber group. The dynamics of a hackers' group are very complex and, of

6 See http://catb.org/jargon/

7 See http://www.outpost9.com/reference/jargon/jargon_toc.html

course, virtual. The groups have an unpredictable structure in the number of participants.

Some cyber criminals may participate in several groups depending, for instance, on how many languages they can speak or in how many technical areas they are specialised. In fact, Internet Relay Chats (IRC) are populated by thousands of users and the conversations are held in different idioms. It has been proven by investigators that, in some channels, a number of users were the same as in other forums.

Within these groups there is a strong hierarchy and a high sense of competition. Several reasons may drive these people to have criminal attitudes; as stated, competitiveness is one of the main motives, as is status within the community, a need for increased self-esteem and also probably just for the fun of it[8].

Moreover, details of successful attacks are often eventually shared amongst hacker communities during IRC sessions in order to rise through the ranks and to gain the respect of the other members. Exploits[9] might be shared within the entire group or just with some trusted friends who will not disseminate such valued information to others. *The main threat exists in the length of time the exploit is capable of harming the targets*. This can last several months or just a short period of time depending on how long it takes to detect and therefore neutralize the attack.

The chief target is usually the private sector; thus companies are the first responders to put in place, after the investigation, the necessary countermeasures to combat the potential activity.

Fundamentally, the main reason that leads criminals, either individuals or groups, into illicit conduct is *money*. The gain can be made directly through the theft of financial data (e.g. e-banking) or indirectly by extorting money from the victim through the threat of attacks.

The threat is ever-changing: today phishing or botnets are the most prevalent, tomorrow there is likely to be a new phenomenon coming through a breach of the satellite system. But the main motive is almost always economical gains. There is the term coined '*Hacking for Dollars*' that means intruders hack computer systems because 'making money is easy'.

Cyber criminals can be hired, not only by criminal organisations but also by business enterprises, with the intention of, for example, destroying a competitor or even of stealing confidential information to be sold for monetary gain (industrial espionage).

8 See also the theory called Money Ideology Competition Ego (MICE) especially within the study made by 'The Honey Net project' http://www.honeynet.org/

9 In computer security, an exploit is a piece of software, a chunk of data, or sequence of commands that take advantage of a bug, glitch or vulnerability in order to get unintended or unanticipated behaviour out of computer software, hardware, or something electronic (usually computerized). This frequently includes such things as gaining control of a computer system or allowing privilege escalation or a denial of service attack. Source: http://en.wikipedia.org/wiki/Exploit_%28computer_security%29

Revenues can be derived from extorting the money from the victim who prefers to pay instead of suffering computer attacks. This phenomenon is continuously increasing, as has been described by numerous reliable sources[10]. In addition, as previously explained, the latest generation of crime-wares have the special feature of extracting data rather than just destroying the network services.

Another driving principle might be an ideology as that can lead to criminal conduct. This is the case for hacktivists[11] who commit offences because of their beliefs. Terrorists, for instance, are a typical example; skilled members are part of the criminal organisation since they are the technicians needed to accomplish the aims of a subversive mission. Attacks to specific targets such as critical information infrastructures are perpetrated in order to destroy the enemy, make an impression on the public, keep the tension high, and create disorder.

Hacktivists are not always terrorists or do not always have subversive goals; they might simply be hackers that attack computer systems because these people are against the ideology of the current government, or are just defending a particular social interest, like the equality in society or even fighting for the free circulation of information on the internet.

10 FBI presentation at GOVCERT Symposium, The Hague (NL) 14-15 September 2006

11 Hacktivist is a combined word formed by hacker + activist.

The Use of Hi-Tech by Criminal Organisations

Organised crime groups are very difficult to trace over the internet. This is because there are deficiencies in a number of key areas, such as:

- global information about the internet itself
- a common reporting system
- reporting system for the victims
- the spread of information
- data retained by Internet Service Providers (ISP) and Telecoms companies
- a common strategy at international level.

Although one deems organised crime as a reality, other assessments prefer to talk about groups of individuals that deal with joint criminal actions over a certain period of time. A common point accepted by HTCUs in EU MS rests in the difficulty of providing a general picture about criminal groups.

Organisations have the same features as the others previously described, such as an international dimension in perpetrating crime through links with other groups. The horizontal use of technology by criminal groups is taken for granted, based on several cases carried out by LEA.

In general, all hi-tech crimes have an international dimension and because of the internet, all the criminal groups discovered are very well organised and flexible enough to change tactics as a result of any crackdown by police forces. There are several cases carried out by HTCUs in EU MS in which the international dimension is clearly evident.

These cases over the internet in which organised crime horizontally makes use of hi-tech particularly involve:

- The production and dissemination of child abusive images;
- The use of stolen credit cards;
- Phishing, ID theft;
- Distributed Denial Service of attacks (D-DOS), BOTNETS;
- Software piracy;
- Spread of crimewares;
- Cyber-laundering;
- Cyber-terrorism.

Criminal groups can always find new avenues to make money using the internet; they are flexible enough to immediately change their approach and discover new concealment technologies, directly used to avoid detection by LEA. They look for new vulnerabilities in network systems in order to find the latest way to exploit them.

Clear proof is seen, for instance, in cyber terrorism; a recent operation carried out in EU against an Islamic group, deemed to be the most active, witnesses that the group is composed of 50 people with international links. The group has been operational for 7 years, is heterogeneous but with the same ethnic background, and have links to other groups. The organisation has been very difficult to dismantle due to the different roles played by the members within the group. The Internet has been the significant factor in putting people into contact with each other, facilitating criminal behaviour at an international level.

Encryption, wireless connections, Voice Over IP (VOIP) and Peer–to-Peer (P2P) are just few examples of what organised crime can use to pursue its illicit interests. The dissemination of child abusive images over the internet is a clear issue in which OC makes huge revenues.

Moreover, child abusive images are one of the vehicles that lead to trafficking in human beings and sexual tourism. Currently the main source about the production of images comes mainly from East European countries and again the criminal groups are clever enough to re-structure their shape immediately after any crackdown made by the police.

Financial crimes are, however, the most widespread because they can generate the largest amount of money. Organised crime has moved towards the carding world; cases of phishing using BOTNETS are one of the most conducted by cyber crime investigators.

Specialised hackers can serve criminal organisations, illegally extracting financial data from compromised computer systems and passing them to the payers. The new generation of crimewares are so powerful in extracting data that organised crime can only benefit from these scripts. *In particular, carding is a chunking down activity from hacking until the cyber laundering, using web facilities, passing through phishing.*

One of the main problems in the trafficking of stolen credit cards over the internet is the difficulty in tracing the money trail. There are several cases in which criminal organisation are very clever in hiding the money transfers so that the investigators find it incredibly hard to trace the revenues.

Crime Types

Botnets, the Drones Army

The phenomenon of BOTNETS or BOTS[12] is currently considered to be one of the most dangerous cyber threats with a huge international dimension. There are a number of reasons for this:

- BOTS are difficult to detect
- there is still little data available comparing to the phenomenon in its whole
- police forces sometimes have inconsistent legal tools to investigate them
- the criminal activities in many cases are carried out from outside the victim's country
- on many occasions the victims have omitted to report the issue to the police.

These are just a few of the reasons for generally explain because BOTS are so difficult to contrast.

Moreover, BOTNETS are generally used as an avenue to commit other crimes like industrial espionage, phishing and extortion, to name a few. HTCUs in MS are fully involved in fighting BOTNETS because the danger can come from anywhere and it is continually increasing.

A study conducted in the second half of 2005 by Symantec Corporation indicates which countries were most affected by the phenomenon of BOTS, as seen in the table below:

12 BOTNETS or BOTS stands for robot networks which is a script which can remotely undertake the control of a computer (or a number of computers), eventually attacking other machines over the internet. In other words, a computer connected to the internet can be compromised by a hacker who undertakes the control of this machine remotely through, e.g., an installed Trojan. The compromised machine (called Zombie or Drone) becomes a robot in the control of the hacker and is used to attack other computers over the internet with the aim of extorting money, industrial espionage, theft of personal data, theft of bank account details, theft of credit card numbers etc.

Rank July–Dec 2005	Rank Jan–June 2005	Country	Percent of bot-infected computers July–Dec 2005	Percent of bot-infected computers Jan–June 2005
1	2	United States	26%	19%
2	1	United Kingdom	22%	32%
3	3	China	9%	7%
4	5	France	4%	4%
5	6	South Korea	4%	4%
6	4	Canada	4%	5%
7	10	Taiwan	3%	2%
8	9	Spain	3%	3%
9	7	Germany	3%	4%
10	8	Japan	2%	3%

Source: Symantec Threat Report July-Dec 2005

During that period, the USA was the most BOT-infected and the UK second. The UK was in first place in the first half of 2005 due to the fact that there was a considerable increase in bandwidth supply there at that time. Consequently, criminal activities also rose in the same proportion. *This is a clear example of how external factors can have an influence*.

Illicit revenues produced by the utilization of BOTNETS are huge. Recently, the American federal authorities[13] arrested a young hacker of 20 years of age who was able to manage 400,000 compromised computers, spreading a Trojan horse called '*rxbot*'[14]. It is believed he had already gained $60,000 and a BMW car through his illegal activities.

Amongst other targets, the computer systems of the Weapons Division of the US Naval Air Warfare Centre and the US Department of Defence's Information Systems Agency have been attacked. Critical infrastructure systems can also be targeted by BOTS, as well as the financial sector which is heavily affected by this issue.

The examples given above are real proof of how this phenomenon is evolving and the myriad of possibilities that it can offer, which can also include extortion perpetrated by the hackers threatening the target who can potentially be under attack.

BOTS are used to spread new crimewares by uploading them in other machines. The self replication of viruses is the quickest way to infect computers.

Spammers are now moving their operational axis to use zombie networks to spam other computers: in only 20 days, zombies can be commanded to send out 18 million spam email over 13,000 websites.

13 See http://www.eweek.com/article2/0,1895,1881621,00.asp

14 rxbot belongs to the family of crimewares (malicious codes)

It is well known that BOTNETS and their variations are created by installing a Trojan into the victim's unpatched/vulnerable computer, creating a backdoor in it and eventually using it to attack other targets especially generating, for instance, a D-DOS, which consumes a large part or even the whole bandwidth of the victim.

It is not only the damage caused by the malicious code in the machine that has to be borne in mind, but also its self replication in the computer system. Once operational, the BOTNET is also a means of guaranteed anonymity for the hacker in the perpetration of attacks, as the criminal remotely controls 'the zombies' army.

One of the main areas where BOTS can flourish are IRC channels where hackers can rely on a large number of victims through the delivery of plenty of 'DCC send[15]' infected files, usually attacking the port 6667[16] although other open ports are certainly not neglected. The reason that many attacks are perpetrated over IRC channels is that IRC servers have free access, they are easy to set up and many hackers already have lengthy experience in managing IRC.

It should be noted that D-DOS not only attacks target web-servers but every machine online can be targeted. BOTNETS do not require particular skills and in fact Script Kiddies can easily use them. The malware installed in the machine masters the processes that interact with the internet: this case is typical of a complaint reported by a victim to LEA.

The threat is not purely restricted to D-DOS attacks because BOTNETS can also be used to spam targets sending plenty of bulk email. They can also be used to sniff traffic passing through the compromised machine and even keylogging[17] is another avenue for hackers in getting useful information.

Such methods are used for committing crimes of identity theft and even phishing when the purpose is also to gain money through the use of BOTNETS. Many users receive fake email from BOTS where personal data is requested. The potential victims just fill in the fake template with personal data such as name, address, bank account and credit card number, not recognising that they are giving their details to a criminal who is pretending to be a credit institution, or Paypal[18] or Ebay[19]. A separate chapter will be dedicated to phishing and identity theft.

The phenomenon of BOTS increases every day, not only because of the ever new illicit possibilities this tool presents but also because there are external factors which influence the criminal market. As previously stated, larger bandwidths are becoming more and more affordable due to the low cost of flat connections: this means there are more computers online and thus more targets. Consequently, there are greater opportunities for criminals to perpetrate illegal conduct.

15 http://en.wikipedia.org/wiki/Direct_Client-to-Client

16 The port 6667 is usually utilised for IRC communications

17 http://en.wikipedia.org/wiki/Keylogging

18 http://www.paypal.com/

19 http://www.ebay.com/

The potential of BOTS is very high because they are able to not only scan the hard drive but also to disable the anti-virus program destroying it. Moreover, the risk is higher when the target is a machine connected to a network.

BOTNETS have been in existence for a long time but they are getting more public attention because they are spreading rapidly and because they are being used for the purpose of making money[20].

'Drones Armies' can be programmed remotely and stir up an attack at certain times against the target. The threat and the risk the attack may generate to networks can only be imagined. Nowadays, the main purpose of using BOTNETS is to gain money. BOTNETS can be rented as well as used as a tool to extort money from the victim. There are several examples of this glaring criminal phenomenon.

Crimewares scan plenty of networks pointing at open ports and looking for vulnerabilities. The most affected operating system is certainly Windows and the versions XP and 2000 are very much attacked for the obvious reason that they are the most used operating systems.

As previously mentioned, currently the trend is for BOTNETS to affect mainly IRC channels. But the spread of crimewares over the internet through attachments in emails is another successful vehicle. '*Phatbot*' is one of the most dangerous viruses with the potential to steal personal data and credit card details by launching D-DOS.

Google's Advertisement on companies' website can be another way to illegally make money. In fact, enterprises may use to host Google's advertisement earning money on the clicks. A criminal uses BOTS enhancing the clicks and raising the price to be paid. Finally, another chance offered by BOTS can be through manipulating online games/pools over the internet. The drones' armies are recognised by different IP addresses and they can therefore send requests for votes whilst being recognised as a credible source.

Moreover, BOTNETS can also ensure financial gains by exploiting 'Advertisement Add-ons'. In particular, a criminal can set up a fake website which can host a link to companies, making a deal with them about a price to be paid every time their advertisements are clicked. The criminal can use the BOTS that send continuous requests in order to automate these clicks.

20 http://swatit.org/bots

Criminal Groups on the Internet

According to a study made by the World Bank Treasury Security Team, entitled '*Cyber-Zombies*', one in three machines are enslaved to attack other machines. We are confronted with a new generation of e-epidemics over the internet.

By the same source, cyber criminals are becoming more and more sophisticated as they associate with each other worldwide. Now, the trend is to set up a crew to split the technical activities. In fact, a criminal project on how to perpetrate a computer attack can be prepared by different individuals:

- **The coder**, who is the writer of the malicious code;
- **The launcher**, who will run it;
- **The miner**, who will extract the data;
- **The washer**, who will launder the revenue, e.g. in an e-payment system.

This splitting technique is a successful method to avoid the map out of the criminal process in its entirety.

Another concern in fighting BOTNETS is the impossibility of working on prevention. In particular, D-DOS attacks come from everywhere and hundreds of thousands of BOTS are spread worldwide. Threats find their origins everywhere and listing some examples of how criminals can illicitly earn money through the use of the drones increases the fear felt by users of the internet.

An additional problem is the lack of data available in each country because the threat always comes from abroad. Police Forces in EU, for example, face serious problems in investigating BOTS, because of the lack of proper legislation, the slowness of legal procedures in order to get data from abroad, and because the phenomenon is growing as well as the number of criminal groups operating over the internet.

Initiatives at International Level

The best solution is always through cooperation amongst different partners: tackling BOTS involves several stakeholders.

Some initiatives have been taken by private industry, such as an interesting project carried out by Computer Associates International Inc, where a pool of one hundred companies tries to locate the source of the BOTNETS instructions, locating and disabling the 'Command & Control' (C&C) server where the main investigative activities are focused upon. Just shutting down a drone is useless because it is replaced by 20 other zombies afterwards.

The Botnet Task Force is another valuable project where a lot of efforts are invested, not only in the study phase but also in regularly training LEA in order to best fight the criminal phenomenon. It has been estimated that 70% of spamming comes from BOTS and currently there are tens of millions of zombies running over the internet.

The Internet Storm Centre (ISC)[21] is also working very hard in researching and supporting the study of BOTNETS. During a BOTS-dedicated workshop at the 4th International Symposium organised by GOVCERT[22] in the Netherlands in September 2005, the ISC said: '*BOTS are all about crime and not just a technological tool*'. Their flexibility is their main feature as BOTS can be used for different purposes. Not only it is the case that every day new types of BOTS are born, but the difficulty in detecting them is very high.

The 'Honeynet project'[23] is another valuable initiative to investigate and find new solutions to this issue. They have conducted several studies on cyber security at no cost to the public and are spread internationally. From their research on cyber threats, they have concluded that attacks are increasing and that they mainly come from economically depressed countries like Romania. After four months of research, the 'Honeynet project' estimated that over one million systems have been compromised and on average each of those compromised machines has been infected by 16 BOTS over the internet.

Cooperation between police forces and private industry is strengthening because this is the only effective way of tackling BOTS.

Technically, there might be several solutions to prevent or at least fight BOTNETS. That one in looking for Command & Control is surely a good approach, but there is a need for close cooperation amongst different partners at international level.

LEA in the EU has a lot of dealing with BOTS. All of them consider the phenomenon in continuous growth. The view about organized crime involvement is varied: in

21 http://isc.sans.org

22 www.govcert.nl

23 www.honeynet.org

some countries there are organized groups who deal with BOTNETS whereas other countries are just faced with individuals.

Generally, LEA cannot be the sole part dealing with this issue. Nowadays also network operators recognize a common benefit in fighting BOTNETS. The cooperation, for instance, with network operators is vital especially with the ones that carry Autonomous System Number (ASN)[24]. Large entities like universities and ISPs have ASN; managing directly large ranges of IP Address would really give the chance to properly tackle BOTS.

According to the Computer Crime Research Centre[25] important actions have been taken by ISP and enterprises which filter the traffic in order to avoid spamming but this solution cannot be applicable by all ISP. The countermeasure taken in fact is to crack down the open relay that is the mail server which manages that traffic.

Finally, BOTNETS can currently be considered the main cashier of the internet as they provide a large number of illegal services to earn illicitly money. They are used not only for financial or personal data but also for disrupting services of the target. The future trend will be an augment in the large use of BOTS for all the reasons described above. Criminals or better organised crime will increasingly fuel the use of this criminal tool to increase their profits.

Moreover, beside any doable technical solution, the cooperation between LEA and private industry has to be increased significantly. ASN and ISP, for example, should have the pulse on what is going on in their networks: the monitoring is compulsory and the bandwidth should be used in a more efficient way especially toward convergent systems.

The cooperation between LEA and Microsoft is also very valuable and needs to be kept on working[26]. Microsoft, amongst its programmes of cooperation with LEA makes available 2 hash databases: one on malicious codes and one on compromised machines victims of BOTS. This is a great help for the investigations.

24 http://en.wikipedia.org/wiki/Autonomous_system_%28Internet%29

25 See http://www.vnunet.com

26 Also known as 'BOTNET Task Force'

Phishing, Pharming, Vishing and SMiShing

Phishing is a type of social engineering over the internet that yields plenty of revenue for criminal organisations. This social engineering is combined with technical artifices with the aim of stealing personal and financial data. *The crimes that are conceived consist of fraud and identity theft*.

Phishing is very much used by criminal organisations for illicit purposes; misrepresenting companies, banks or other credible entities' names is the typical technique that is employed to obtain personal and financial data from the unaware users. This crime is very much connected to 'carding' but also other financial data is fraudulently used by criminals, such as bank account details. The addressee of the spoofed email usually discovers the fraud much later when the damage is irreparable.

Thousands and thousands of stolen credit card numbers are spread over the internet and the financial losses cannot be counted.

LEA in the EU is overwhelmed by several cases to which are effective in tackling criminals; the financial losses are estimated in millions of Euros. One of the main issues highlighted by some EU HTCUs is: *the threat comes from abroad, especially from Eastern Europe or the Far East, making investigations difficult*.

The internet has no boundary which unfortunately makes it impossible to paint a reliable picture of computer crimes, but considering just the European Union market, the size of the figures regarding the damages caused by the BOTNETS is imaginable.

In addition, phishers are becoming more and more skilled, adopting sophisticated techniques and emulating websites or emails in a manner that is difficult to recognise whether or not the sources are trustworthy. Recently, Barclays Bank in the UK has been recognised as one of the most attacked targets by phishers[27]; through the Panda antivirus software, they have discovered 61 new variants of spoofed emails sent to the bank's clients. Customers in fact are puzzled by the difficulty in distinguishing between the credible source of the message and the bogus one.

Material on '*how to phish*'[28] is freely available over the internet. Stolen global address lists are used by phishers to spam potential victims and faked URLs are used to collect personal data from the victim who is redirected to legitimate web sites afterwards.

---

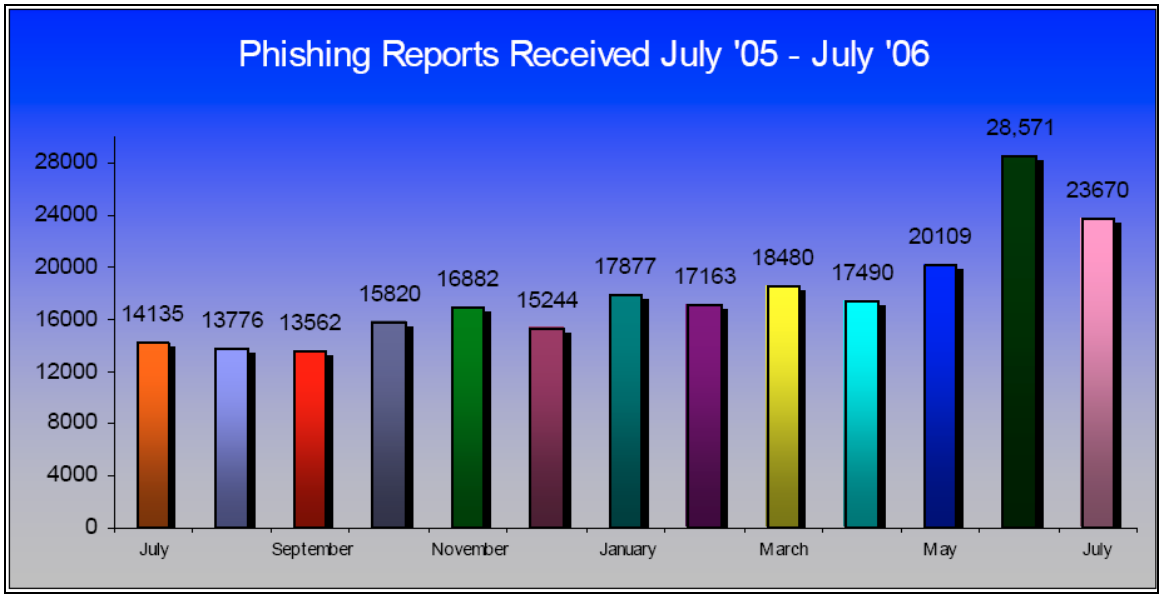
27 http://www.vnunet.com/vnunet/news/2164157/barclay-bank-targeted-large published 13th Sept. 2006

28 It could be useful also to consult http://en.wikipedia.org/wiki/Rock_Phish

Groups of criminals can be composed of a few persons and each of them is specialised in one chunk of the criminal process. It is believed, as with BOTNETS, that criminals are located in different parts of the world but they are very well connected to each other, exchanging scripts or stolen credit card numbers.

The losses suffered by credit institutes and interbanking systems, such as credit card companies, are enormous[29]. There are several initiatives launched by researchers and experts all around the world in order to deepen the knowledge about phishing. The Internet Storm Centre[30] has already published a manual, which gives some tips on contrasting phishing issues. Symantec[31] is another reliable source reporting on the phenomenon.

One of the most valuable initiatives is believed to be the Antiphishing Working Group (APWG)[32], which collects and publishes very useful information and best practice documents. The APWG has more than 2300 members amongst the private and public sectors, including LEA. The latest report shows below the current situation about phishing reports:



In the reports published by the APWG, new trends about phishing crime are described there, underlining the fact that most host phishing sites reside in the USA. Beside the statistic above that shows a flexion, there is a belief, however, that

29 http://www.theregister.co.uk/2004/09/29/phishing_survey/ published 29th Sept. 2004

30 http://isc.sans.org

31 http://www.phishreport.net/

32 http://www.antiphishing.org/

from some EU HTCUs, the phenomenon is growing with a high involvement of organised crime.

Phishing and BOTNETS are very much interconnected due to the peculiarity of BOTS in which the latest versions of virus become more and more dangerous, having the features to capture personal data and to transform the victim's computer into a zombie[33]. The proliferation of wireless connection just enhances this dangerous process; more and more people are always online with the consequence of having more threats in ambush.

In particular, *sophisticated techniques such as BOTNETS are used for sending e-mails and harvesting banking information, thus making impossible the identification of culprits. Also, the use of 'e-mules*[34] *to launder the proceeds through various jurisdictions creates significant delays in identifying those responsible.*

In fact, another serious problem is to map out the money laundered by criminals using e-facilities; the internationalisation of the phenomenon makes it very difficult to trace international payment.

Another kind of dangerous electronic social engineering, very similar to phishing, is called **Pharming**[35] which is more difficult to detect because it consists of the manipulation of the Domain Name Server (DNS) that at the moment of the resolving IP address, the user is re-directed to a fraudulent site.

The impact on the user's side is huge. For example, the favourites of the web browser are changed to contain faked information. When the unaware customer wants to connect to their online bank account using the favourites as a shortcut, he/she will be re-directed to the internet site managed by the fraudster. In this website, other traps might be embedded that can harm the victim's computer. The consequences are imaginable, e.g. the machine can easily be dragged into a BOTNETS.

Again, the problem in this area is the lack of reporting by banks, which actually hinders any investigation. Credit institutes still prefer to sort out any problems in-house for understandable reasons related to their reputation.

The latest 'phishing evolution' which yields illicit money for organised crime in this area is called **Vishing**[36] which is not web-based but consists of perpetrating fraud using VOIP[37]. In other words, a dialler calls customers and an automatic voice starts pretending to be the financial institute; it then requests credit card numbers

33 For more details see the part concerning BOTNETS

34 See http://www.banksafeonline.org.uk/moneymule_explained.html

35 http://en.wikipedia.org/wiki/Pharming

36 http://en.wikipedia.org/wiki/Vishing

37 http://en.wikipedia.org/wiki/VoIP

including the Card Validation Code (CVV)[38]. The frauds over IP are becoming more and more widespread[39].

At the moment, there is no real crime prevention as this phenomenon is very new but the advent of VOIP[40] facilities can be another avenue to best profit from this opportunity. The user's common sense would be the most suitable approach in contrasting vishing, seen the security measures are still not adequate.

Even less countermeasures can be adopted when facing one of the main criminal threats that will worry LEA in the immediate future, namely **SMiShing**[41]. In other words, this latest threat attacks mobile phones, connected to the internet. The user receives a link to a web site and when clicking a Trojan enters into action with imaginable consequences in the mobile phone's content.

Involving many stakeholders, there are several questions that should be answered in relation to how to best combat phishing, pharming, vishing, and smishing such as facilitating the protection of the business, overturning this criminal trend, building up effective crime prevention and, last but not least, discovering how governments can support the evolution of the market.

In principle, besides any security measure that should be taken by every user, such as installing specific toolbars that can recognise malicious pages, co-operation with ISPs is a fundamental step in this area; shutting down faked web sites is not sufficient. Moreover, there is a strong need, as within all other crime areas, to work on prevention: only suitable education at all levels is a solution which should be applied as soon as possible.

The private sector is moving very much towards a higher level of authentication: banks are providing customers with appropriate hardware to better validate access to their online account[42]. These countermeasures are compulsory to prevent criminal actions and to reduce financial losses because criminal organisations pursue financial gains through the use of phishing, pharming, vishing and, more recently, smishing.

Finally, it should be remembered that the four phenomena described are very much connected to other forms of crime, such as 'carding'[43], that may finance other illegal activities like money laundering and terrorism. These crimes definitely cannot be seen in isolation but are connected to other offences such money laundering or even to finance terrorist organisations.

Therefore the endless and rapid development of the technology also enhances the growth of computer crimes; frauds over the internet will never stop as new

38 http://www.internetnews.com/security/article.php/3619086 11 July 2006

39 See www.voipsa.org where there is a deep study on VOIP issues

40 Amongst others, Skype is one example, see www.skype.com

41 http://www.webopedia.com/TERM/S/SMiShing.html

42 http://lists.jammed.com/ISN/2005/10/0137.html published 31 Oct 2005

43 http://en.wikipedia.org/wiki/Credit_card_fraud

techniques appear which are exploited by criminal organisations. The proof is seen in how phishing has led to vishing, passing over VOIP coming now on mobile phones (smishing). The curve can be steady and increases as soon as new illicit methods in making money arrive on the market.

One of the key points in combating social engineering is '*education*': various studies have stated that in most cases, the incorrect behaviour of the user has made it easier for the perpetrator of the crime.

The phenomena described are just other forms of deception which are facilitated by inappropriate use of the technology by the users, such as accepting the installation of improper software on their computers or giving personal details on request to an untrustworthy website. Public and private sectors should invest more in official campaigns to make people aware on the dangerous consequence of inappropriate usage of technologies.

Criminal organisations are making money out of social engineering, either by having active members belonging to the group or just by hiring hackers/phishers to pursue illegal purposes. Moreover, it should be borne in mind that criminals are devious in complicating the investigation carried out by LEA: fraudsters are located in different parts of the world, splitting up the illegal activities, exploiting the bugs of Internet Explorer, URLs encoding, and targeting email global lists. They even use hacked servers to host and distribute the spoofed emails.

The hindrances are not only technical: many times ISPs are reluctant to give data, protecting themselves behind a privacy policy, or it appears victims seldom admit to having provided negligently personal data to an unreliable source. There is also still no international law that can help to solve the problem: the whole issue has to rely on existing domestic laws; the cyber crime convention has still not been ratified by many countries.

There could be several solutions; shutting a faked website is certainly not sufficient because they are like mushrooms and a closed one is just replaced by another in little time. LEA should improve co-operation; enhancing their partnership with the industry and banks would also be very desirable in order to achieve better results in tackling the criminal facts. Finally, better education for the users and a stronger authentication of the access to networks should be thought about, as already practised by some credit institutes.

The trend of phishing, pharming, vishing and smishing is becoming more and more incisive, especially with the new generation of crimewares. If before the creation of worms, viruses and Trojans were conceived more for the destruction of the content of computer systems, nowadays the crimewares are supposed to extract data such as key logging, causing additional problems on a system's security.

Critical Information Infrastructures (CII)

We live in a world of convergence of services and devices. Nowadays, computers are interconnected in network infrastructures in order to satisfy customers' needs. These services usually belong to public sector or private companies that provide facilities to citizens, like banks or telecommunications. However, the interconnectedness of systems often leaves them exposed to attacks. The convergence of voice and data particularly enhances the possibility of security breaches. Services, devices and the information managed are considered critical.

There are several ways to define critical information infrastructures; the most advisable could be:

Physical and IT facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on health, safety, security or economic well-being of citizens or effective functioning of governments[44].

Around Europe there are plenty of action plans at domestic level: The Netherlands[45], the United Kingdom[46], Sweden and Italy are just a few examples of how this issue very much affects many countries; overseas, the USA and Canada run similar programmes which pay a lot of attention to the problem. Governments and important institutions are exposing their information and services to the public, thus they need to take initiatives to protect these assets from attack, giving special attention to research and development. CII comprise a large number of stakeholders.

In cyber terrorism, as in other areas, organized crime heavily uses technology for illicit purposes and CII are the target of attacks: institutions must comply with security measures. Systems are becoming more and more interconnected and a common strategy is needed.

There are several examples about interconnected network systems; one of them can be hospitals' network. Databases of patients can collect a lot of information to be shared amongst medical institutions in order to electronically look for the profile of the person. The advantage to have a centralised recipient of information is clear: a person can be properly treated wherever because the patient's profile is immediately retrievable. But whether a security breach occurs on the database, the consequences can be imagined. Medical data can be destroyed or even maliciously modified.

Nowadays there is also the telemedicine. Patients can be surged in one hospital but a specialised doctor can act in teleconference from a remote site. Whether a

44 DGTREN – Security Directorate

45 http://www.tno.nl/

46 http://www.iwar.org.uk/cip/

computer incident occurs and/or the communication is cut off during the surgery the effects can be imaginable.

The same goes with the gas, electricity or water supply systems, which are becoming more and more interconnected. A disruption of one of all these frameworks can cause huge damages to the citizens. Again, a coordinating action is required.

The European Commission, within the 6th Framework Programme, is coordinating a very valuable project, led by Critical Information Infrastructure Research Coordination (CI2RCO)[47], in which the main mission is to enhance research and developments and to identify the gaps that have to be filled in order to satisfy the needs of all stakeholders.

Interconnected systems mean a series of combined vulnerabilities that have to be confronted with existing and forthcoming threats. The main issue is to address a proper policy and awareness to all the stakeholders that belong to different areas in both private and public sectors.

In a world where everything converges with IP addresses, there are several interests to protect. Private and public interests often clash with each other because business goals conflict with social interests.

The fields for discussion can mainly include:

- cooperation between different entities
- the interoperability of systems
- the response in case an incident occurs
- a common concept of an interconnected network in order to facilitate information sharing and to give the best service to the customer
- the protection of the critical information stored
- the settlement of a common scale of risks.

Basically, there is a lack of methodology in approaching these issues. LEA may face problems in investigations and with forensics due to what has been described above, especially concerning contact with the first responder, particularly when the interconnected systems are located in different countries. The Internet eases intercommunication but, conversely, complicates coordinated action.

Police forces cannot work in solitude: high involvement with other entities, such as Computer Emergency Response Teams (CERT) and the CII operators, is

47 http://www.ci2rco.org

fundamental. The European Network and Security Agency (ENISA)[48] would be a good coordination point as adviser in protecting the CII and preventing attacks.

48 http://enisa.europa.eu/

Cyber Terrorism

Terrorist organisations have learned how to use technology for criminal goals. Whether initially proclaims and flyers were the only ways to spread propaganda, nowadays internet is the perfect tool to achieve their scope. If sometime ago war and revenge could only be promoted through physical attacks, at present time the technology allows criminals to hit enemies at their critical information infrastructures: *The threat comes in different ways from different perspectives.*

The Framework Decision of the Council of the European Union 2002/475/JHA defines in the art. 2 the offences relating to a terrorist group:

'Terrorist group' shall mean: a structured group of more than two persons, established over a period of time and acting in concert to commit terrorist offences. 'Structured group' shall mean a group that is not randomly formed for the immediate commission of an offence and that does not need to have formally defined roles for its members, continuity of its membership or a developed structure.

There is not yet a commonly accepted definition of cyber terrorism; however the following one could be used as starting point in order to understand what the whole issue is about:

Cyber terrorism is the premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives[49].

Extremist Islamic organisations are currently the best users of the technology to pursue their criminal goals. In particular:

The Internet offers Islamist militants a low-tech, cost-effective, minimal-risk medium through which they can demonstrate their existence and operational status, conveniently reach out to their constituents and participate in the battle for public support in the Muslim world[50].

The usual scope of the terrorist is to fight against a belief deemed right by a society. The criminal has a deviant mentality and the intention is clear. Terrorist groups use technology in order to enhance their war against the enemies. Some of the criminals belong to the organisation but others are just external collaborators properly hired and paid for illicit scopes.

49 http://www.crime-research .org/library/Cyberterrorism.html

50 http://www.stratfor.com/products/premium/read_article.php?id=259110 30th November 2005

The utilisation of hi-tech is shown every day and terrorist groups turn their interest especially to the internet. The World Wide Web is a free access resource in order to spread their propaganda[51].

If before Islamist terrorists were using only physical weapons, nowadays their military strength is to build up an information system capable of reaching any point in the world, instructing proselytes wherever they are, recruiting new members, and keeping public opinion under pressure. This latter produces a great impact especially in some occasions like when a web site advertised the instructions on how to make a nuclear and biological bomb[52]. In a short time the web server recorded 57.000 accesses where a detailed manual was published about the realisation of the project.

In the 1990's the web sites sponsored by Islamic extremists were technologically primitive and often published in Arabic, limiting their audience. Today although the Arabic language is still dominant, other languages are used allowing militant groups to spread their message worldwide and recruit new followers.

Internet offers a variety of possibilities to reach different goals: not only for the propaganda and spread of fear, but training, support and tactical actions can be quickly taken. *Organised crime has discovered the tools of hi-tech that horizontally support any activity*.

The training online is one of the most used techniques to keep updating the members of terrorist organisations for what concerns tactic and operational modus operandi. The web pages written in Arabic languages can be understood by a certain number of people being the Arabic far from the comprehension of western world. Internet facilitates the flourish of new terrorist cells worldwide without the physical contact with the 'capo' of any organisation.

Instructions can be given by remote ensuring the operational outcomes by the soldiers as feedback for the leadership. Strategic directions can also be suggested e.g. in order to show ways of escape from the country where the aggressions have been accomplished.

Internet even eases the lavish of research of development done in remote countries and sent to the destination where, if done there, can be detected by LEA: this can be the case of how to build up biological weapons. Messages can be sent with strong encryption evading the control of police forces over the net: *virtual criminal communities come alive*.

The story about a 20-year-old student[53] at the University of Khartoum is evident: *terrorist organisations manipulate followers*. The boy incited by Al-Qaeda propaganda decided to use the scholarship support given by the parents to fly to Iraq for a suicide bombing: he was a kamikaze. He killed 22 people, 18 of whom

51 www.washingtonpost.com 7th August 2005

52 http://www.timesonline.co.uk/article/0,,2089-1859222,00.html 6th October 2006

53 http://www.spiegel.de/international/0,1518,382097,00.html 28th October 2005

were Americans. The same article says there are web sites containing the list of martyrs. It is self evident that propaganda via internet is highly incisive worldwide not only to keep the inners updated but also to recruit new followers with even more radical ideas.

In addition to propaganda, but the use of applications that guarantee the anonymity such as *FreeNet*[54] for Peer-to-Peer communication and proxy servers like *Tor*[55] for web browser are just two examples of the most common kits used by criminals.

On the internet there is even a 'New forum for posting calls for intensified electronic Jihad against Government Website'[56] in which there is a long vademecum describing how to destroy the digital resources of an enemy. Examples like keylogging, misrepresentation of IP address of the source, and anonymisers are the topics dealt with.

There are web forums which describe all these techniques giving also links to other sites where to find the proper application to be run against the political opponents. Moreover, on the same forums, members propose to create a cyber jihad community launching a unique D-DOS to be more effective.

The tragic terrorist events such as those which occurred in the USA in 2001, Spain in 2004 and England in 2005 prove that the Internet can be used for criminal purposes. The claim of responsibility for the attacks has the purposes to increase the fear level amongst the public opinion, to attract the attention both from the media and LEA, and last but not least to incite the followers to adopt a certain ideology.

The ideological justification is one of the most important subjects dealt with terrorist organisations to keep the followers together under the same driving principle. The propaganda plays a fundamental role in the whole issue: web sites and bulletin boards are the new e-flyers.

Most terrorist organisations are using high technology for criminal goals as follows:

- By recruiting *hacktivists* who belong to the organisation and defend their beliefs by attacking computer systems.
- By using of external computer experts who are only motivated by gaining money.

In the latter case, these experts are *black hats* who hack computer systems or in general serve criminal organisation to earn money easily.

54 http://freenetproject.org/

55 http://tor.eff.org/

56 http://www.jamestown.com 29th August 2005

This is the case of the virus writer[57] who, after the London's attack in 2005, just created an ad hoc virus to be used for spamming emails and spread the virus eventually building up BOTNETS[58].

Hi-tech experts such as engineers are involved in the propaganda of terrorist organisation by managing networks of web sites[59] in which they publish messages about Islamist extremism. Other Islamist web sites, which have already been shut down in the past, catered for an English audience the messages of jihads. This is significant: *the audience is not only the Arabic world but the western one as well.*

There are web sites where Islamist terrorists offer large variety of videos to download for all kinds of streams requested, from ASDL to dial-up connections. It is noteworthy that the organised crime can tailor the offer to a large number of customers.

Another criminal action taken by terrorist organisations is the attack of national critical infrastructures. Although there is a specific chapter on this subject in this document, one of the targets of terrorists is the networks which are vital to the society.

Computer systems are targeted by hackers who are either hacktivists or black hats hired by organised crime to destabilize the enemy's resources. The targets are usually information systems, gas or electric suppliers, just to name a few. Systems interconnected like hospitals that make use of telemedicine can be attacked by terrorists who can elude computer security, sniffing and alter personal data of the patients.

At the moment there is no proof of the possible content manipulation of the critical information infrastructures systems, but they are continuously targeted by hacking attacks. Hackers can use viruses and might corrupt the content of critical infrastructures' systems: *the public opinion is not giving the appropriate importance to this emerging threat*[60].

Companies have to realise that, as soon as they offer an e-service to the public, they can be targeted by hackers. There is not only the possibility of physical but also digital attack. Cyber terrorists also aim at this.

The hacktivists or simple sympathisers are driven by the ideology propagated by terrorist organisations and utilize the Internet for criminal purposes exactly like members of these associations. A very interesting case[61] is the story about the arrest of a 22 year-old hacker known with the nickname '*Irhabi007*' (Arabic for

57 http://www.theregister.co.uk/2005/07/08/london_bombing_spambot/ published 8th July 2005

58 The BOTNETS topic has a specific chapter.

59 http://www.washingtonpost.com published 8th July 2005

60 http://www.csmonitor.com/2005/0816/p01s02-stct.html 16th August 2005

61 http://www.adl.org/main_Terrorism_077_younis_tsouli.htm 1st March 2006

'Terrorist 007') who came to the attention of LEA already in autumn 2005 because of his jihadist-oriented behaviour over the Internet.[62]

He promoted himself on an Internet forum to be a very skilled hacker and able to elude LEA detection. He further demonstrated his skills in hacking FTP web servers and cracking password protected systems; he also made available videos and files concerning terrorists online. The hacker created a network of hijacked sites in order to create available resources regarding how to perform terrorist attacks, including the use of stolen credit cards for those needing paying customers. He even used the personal data of unaware people to register in some sites.

Irhabi007 also hacked some critical information infrastructures web sites in the USA, and raised the attention of American LEA after having sent out dozens of terrorist videos and files, transforming the hijacked sites in Al-Qaeda's bulletin board. Actually, Irhabi007 was arrested in another context. Only after his arrest, it became apparent that he was the renowned hacker.

As seen terrorists cluster large group of members all over the world, but because of the blurry internet a real assessment of the size of the groups is really difficult to make. As explained in the paragraph that describes the cyber criminal communities, there is only the perception about the dimension of the phenomenon that actually is more driven by the consequences of the effects that the attacks yield.

All LEA seem to be successful in fighting 'classical' terrorism, but when it comes to technology, the use of new tools by criminals impedes effectiveness at investigation level: there is a lack of reliable data on cyber terrorism issues. The national laws are going to be improved because combating terrorism is one of the first priorities worldwide; but the main problem remains and a proper law in order to regulate the use of the Internet is needed.

62 'Terrorist 007, Exposed', Washington Post, 26 March 2006.

Trafficking of Child Pornography Images on the Internet

Many operations against child pornography have been carried out worldwide by LEA during the past ten years. The outcomes are evident but the phenomenon is always increasing. Many HTCUs say the trend is continuously growing, which also increases the workload of the investigative unit; moreover the seizures of digital assets doubled in just one year as well.

The HTCUs in the MS raise a specific impediment in optimising their investigations: *the partial view of the phenomenon that hinders a reliable assessment of the production and distribution of child pornography worldwide*. The problem of geography is always present in all investigations on internet related crimes and it is difficult to collect sufficient data to make a reliable crime assessment.

The reason is mainly that the internet has no boundaries and the series of indecent images travelling over the internet is endless once they are put online at the disposal of everyone. In fact, one of the main issues in the distribution of child abusive material is the *redundancy* caused by internet that generates a re-victimisation of the depicted child.

A report from the National Children's Home **(NHC)**[63] says that cases have quadrupled in just two years; this after Operation Ore was conducted in the UK. Moreover, Europol has been co-ordinating several operations at EU level concerning child pornography: Icebreaker I and II, Baleno and others carried out within the framework of Europol Analytical Work Files (AWF), have produced several arrests, searches and identification of victims all over the world. Many criminal organisations have been dismantled since 2000 and police forces have discovered new modus operandi used by criminals, such as the Bulletin Board Systems (BBS) in which the users utilised particular techniques to hide their identities and special characters or fonts to recognise each other and to avoid detection by undercover LEA.

Encryption, anonymisers and anonymous payments (like virtual credit cards) seem to be the best tools used by criminals; this raises again the international dimension of the phenomenon of child pornography, especially through technological developments. The encrypted hard drive still represents one of the main hurdles in discovering information about the criminal conduct.

In fact, new technologies are always in place on the internet and criminals utilise them to enhance the effectiveness of their activities. Wireless Fidelity (WI-FI)[64] and wireless connection in general have witnessed an enormous growth recently and this expansion will not stop. Nowadays, wireless networks are based in every public area. VOIP is currently another technique used to lure children over the internet; the new version of Skype and the Microsoft Network (MSN)[65] are just two examples

63 http://www.nch.org.uk/

64 http://en.wikipedia.org/wiki/Wireless_fidelity

65 http://get.live.com/messenger/overview

of how voice with webcam installed can offer the proper support for criminal purposes. Even the new generation of mobile phones opens new avenues for enticing children.

By contrast, for security reasons and to ascertain the identity of the users, service providers are, in some countries, obliged to both encrypt the communications utilising encryption keys and also are shown a valid ID card by whoever wants to utilise their equipment. This is the case for the new Italian anti-terrorism law that can be used in parallel to fight child pornography.

Besides any technological development, co-operation with private industry is always needed. The need to strengthen dialogue and collaboration with ISPs and Telecommunication companies has to have high priority because they retain the data for the identification of the machines, which make the connections to the internet.

Overseas, in some countries like Australia in order to properly fight the traffic of indecent images, ISPs are obliged to report illicit activities to the competent authorities. In Europe, such a partnership with LEA would be highly desirable: Italy could be as considered a valuable example they are introducing this type of regulation.

Furthermore, it has to be borne in mind the enormous problems in managing the large amount of data when seizing equipment at the crime scene. The issue of finding child pornography, decrypting hard drives and other support, such as uncovering images that are most likely concealed through steganographic techniques, are just a few examples to describe the sometimes unmanageable situation.

Forensic operations in child pornography make up a large part of the whole investigative process and specialised investigation units are not always able to fulfil their tasks due to the lack of technical resources in managing data or even in finding a proper expert to consult when a new technical solution has been utilised to encrypt the hard drive or hide pictures.

Processing evidence takes longer than expected due to the reason mentioned above: forensic investigations take time and require a huge allocation of resources. Collaboration amongst police forces is considerable but *the redundancy of images is one of the major hindrances* because the supports have to be entirely analysed.

Applications, such as Peer to Peer, consistently ease the collection of child pornography and many police forces are therefore very much involved in Peer to Peer investigations. P2P networks are one of the main vehicles used to stream the traffic of child pornography.

There are reasons to believe the threat of the production and dissemination of child abuse images also leads to the development in trafficking in human beings, illegal immigration and sex tourism. Furthermore, the further goal of criminal

organisations is likely to be money laundering, or even, for criminals to get into the parallel markets of extortion, prostitution and child abuse in general.

As common statement it can be said, criminal activities in child pornography are going more in the direction of making more and more profit, especially bearing in mind what was described above about pay-per-view business.

The aim of child pornography cases is twofold: to arrest the offenders but at the same time to identify the victims of the abuse. The creation of central databases of indecent images based such as at Interpol and others spread throughout the EU countries can certainly ease the tracing of the criminals and the identification and possible rescue of the victims.

Concerning the forensic examination of the digital support, Encase[66], Ilook[67], Sleuthkit[68] are still the most used software, but troubles may be encountered when it is presented at court. Certainly, the main issue is connected to the license and the use of commercial products for forensic purposes.

However, the common problem in forensic examinations in HTC investigations at European level is the lack of official tools that can be used by all LEA and valid as universal instruments to carry out expertise, and which are recognised by all the stakeholders.

An additional problem that seems to have worsened child pornography investigations is the amount of revenue organised crime makes through the sale of images over the internet. The more recent use of pay-per-view has led to an increase in illicit profits. Virtual payments systems are one of the main avenues exploited by organised crime. A successful investigation led by the National HTCU in the UK[69] in 2004, showed how e-payments are the best means of making quick profits while guaranteeing anonymity.

Nevertheless, traditional credit cards are still used to trade child pornography and the inter-banking systems should join efforts to combat it. Huge profits are made by criminal organisations, especially using stolen credit cards to pay for images purchased online.

The use of webcam and other internet tools facilitate cyber sex online that currently yields millions of Euro per year and most of the sites mainly reside in the former Soviet Union area. The reason is that there is a lack of proper legislation in place in those countries, especially concerning data retention, and it is therefore difficult to track the source of information.

66 http://www.guidancesoftware.com/

67 http://www.ilook-forensics.org/

68 http://www.sleuthkit.org/

69 The NHTCU in the UK has recently become part of the new Serious Organised Crime Agency (SOCA).

Initiatives at International Level

Nowadays, there is not only the child molester but also the child pornographer, who does not have a real interest in abusing children; this new kind of criminal concentrates their attention on producing child pornography to earn money out of it.

Child pornographers or child offenders are known as 'white collars'; they are often clever and skilled enough to avoid detection by LEA. Due to the large number of offenders across the internet worldwide, it could be a good initiative to have a central database just tailored to these people to improve the way of profiling.

Europol is doing a lot as an operational co-ordination point at EU level, especially within the analysis processes. During the past 5 years operations such as TWINS, XING, ICEBREAKER, BALENO and their following phases have resulted in a dramatic crackdown on the criminal networks involved in the production and distribution of child pornography content on the internet.

These investigations run under the umbrella of AWF TWINS and the ongoing successes can show how co-operation among LEA, international organisations such as Europol and Interpol, and non governmental entities, is effective.

The achievements of many international operations rest mainly in the mostly harmonised legislation on child pornography. Currently in the EU, there is principally a common legal approach on child pornography investigations rendering co-ordination and co-operation easier, although the usual obstacles on data retention and privacy regulations apply. There is a unanimous response that HTCUs in the MS are satisfied with their individual achievements in this area.

Co-operation is also strengthened through training programmes: Europol delivers on an annual basis a training course on combating the sexual exploitation of children on the internet. The course is aimed at investigators who are new to this subject; the course is for both EU Member States and non EU countries and open both to both law enforcement and the judiciary. The training course provides a horizontal platform for general internet investigations for the first part of the course, which is interspersed with sessions on offender profiling and a victim identification workshop, a specific session particularly dedicated to picture analysis.

Still at international level there is a lack of common approach and perception of the problem of child pornography: the phenomenon of the traffic of indecent images over the internet is still underestimated. It should be paid more attention to the identification and protection of children and not just to the criminals, especially because this phenomenon is largely international.

But the internet is fast-changing and web sites that publish child pornography images pop up and disappear quickly, thus access to vital information is not easy.

ISPs still do not follow a common approach on data retention and privacy regulations.

ISPs and NGOs are the focal points for a lot of gathered intelligence. One of the most effective examples is the Child Exploitation and Online Protection Centre (CEOP)[70] in the United Kingdom that plays a fundamental role, as a partnership between police forces, child protection services, offender profilers, etc. all aiming at the protection of children.

LEA takes a lot of initiatives to improve collaboration with private sector and non-governmental organisations; *this multi-disciplinary approach is fundamental in the crackdown of child pornography on the internet.*

70 www.ceop.gov.uk

Drugs Trafficking on the Internet

The illicit traffic of drugs over the internet is an increasing phenomenon. There are several studies about the development of selling drugs electronically, which offer more proof of how the internet has a horizontal approach. The use of technology to ease criminal activities, especially in these cases, shows how technology is very much ahead of regulations.

One of the issues concerning drugs over the internet is the incredible growth in internet pharmacies. Many people prefer seeking treatment over the internet instead of getting a medical prescription from their doctor in the traditional way. Yet, concerns should not be about the personal use of the drugs but it has to be considered how local market can be fuelled by the use of false medical prescriptions containing large quantities of drugs.

Moreover, there has been a huge increase in clandestine laboratories all over the world, the main reason for which could be the closure of many factories working in the chemical and/or pharmaceutical fields. Such closures have resulted in many people being laid off and therefore, faced with unemployment, they have sought other ways of making a living.

The trafficking of pharmaceuticals can also be another clandestine operation carried out by existing industries in their 'back offices', especially when situated in countries where controls by the government are poor. They are able to use the internet to sell the products and make additional profits.

According to the report of the International Narcotics Control Board[71] (INCB), in 2004, the Lithuanian authorities confirmed that there was a huge traffic of counterfeited tablets into Scandinavian countries seized by LEA. The originating countries of the raw material were China and India whilst the goods were ordered over the internet.

The INCB is working very hard to apply its convention among its members in order to prevent and control drug trafficking, especially regarding the misuse of the internet. The USA and Caribbean areas are the source regions whereas China, India and Thailand are where the internet pharmacies operate.

In Europe, a MS appears to be the place where internet pharmacies are the most active. In general terms, the highest number of 'shoppers' of internet pharmacies are located in the USA and Europe. Even though most of the transactions are related to controlled drugs, it has been calculated that there are 450 sales per day using internet pharmacies.

71 www.incb.org

The main problem that is very much experienced at an international level is that there is a lack of common regulation and coordination against illegal activities connected to internet pharmacies.

In particular, one of the key factors is that consumers can rely on a very discreet delivery, allowing them to remain anonymous. The price may also appear to be more favourable but this is not true at all. In the INCB study, the prices charged by internet pharmacies were compared with those found in ordinary shops: prices were found to be much higher on the net (even without taking into account any medical prescription for which the patient can be reimbursed).

The main explanation for persons purchasing drugs over the internet would seem to be the possibility to ensure anonymity, as the individual does not have to make public the need for certain medicines; drugs allegedly improving sexual performances is a typical example of one of the most bought products over internet.

It should not be neglected the varieties of anti-depressants which also are one of the main goods traded by internet pharmacies: *Diazepam is one of several significant examples of a class IV drug mentioned in the United Nations "Convention on Psychotropic Substances*".

One of the main concerns, aside from any issue of lost customs revenue, is the high probability that clandestine laboratories receive counterfeited raw materials, especially from countries like China or Thailand where the counterfeiting market is huge. Therefore, the possibility that the buyer receives a genuine drug could be really low, with the imaginable consequences on the health of the customer.

Another issue that preoccupies LEA committed to fighting those criminal organizations involved in this area of criminality is the traffic of precursors. There are several cases concerning precursors sold over the internet from one country to another, fuelling plenty of clandestine laboratories. *Precursors, legally traded, are instead used for illegal purposes, especially by drug traffickers for the production of psychotropic substances.*

Moreover, it has to be borne in mind that the trade of some drugs deemed legal in some countries is conversely considered illegal in others. Internet again constitutes a facilitating factor in the deal of this good. There is a need for an international coordination and harmonisation aimed at a common legal approach in the commerce of these substances.

The hindrance in combating such phenomena is not only the lack of common legislation at an international level, but mainly the fact that the internet has no boundaries, making it very difficult to locate and prosecute people abroad.

There are forums where users talk about classified pharmaceuticals and where there is a search engine to find the closest internet pharmacy. There are also websites where the precursors for the production of drugs are mentioned. In connection with this, it is important to note the fact that the trading of precursors is

not illegal when trading is conducted under certain rules but the use of them for producing drugs poses a real concern.

There are even websites where it is possible to find all kinds of seeds for germinating cannabis, flowering time, and price lists. The sites offers advice on many different ways of cultivation, specifying in which countries it is not possible to deliver the goods because of legal restrictions. The owner of the website does not accept any payments by credit card because the billing companies have not given their agreement; therefore only cash in an insured envelope or bank transfers are accepted.

A very impressive operation called 'cyber chase' against the illegal traffic of narcotics, amphetamines and steroids was carried out worldwide in 2005, as a result of which 200 websites advertising such drugs were shut down. Countries like India, the USA and Canada cooperated in this international case against a criminal organisation that used the internet to deliver the goods worldwide.

In Europe, LEA carried out a joint action operating on chat-rooms and bulletin boards on the internet against a criminal organization operating in the traffic of marijuana and its seeds during 2004 and 2005. The sites advertised the availability of the substances online. 17,000 connections to the sites were recorded and 53 cultivators were identified. During searches, large quantities of cannabis plants were seized along with computers and bank accounts which provided details of the revenue made.

This is not the only successful example. In 2005, a joint operation against the traffic of synthetic drugs on the internet was carried out between the United Kingdom and Russian LEA dismantling a criminal organization operating in the two countries. In this operation, a person in Siberia ordered a batch of ecstasy via the internet from the UK. The drugs were shipped through the airport of Moscow and were tracked until their destination, allowing the criminal to be caught. Cooperation between the two countries also led to the discovery of the sender from the UK; he was a Baltic States citizen.

Russia is becoming one of the most attractive drugs markets, especially according to the UK[72], with the recent discovery of several synthetic drugs laboratories there. The internet again eases operations for such criminal purposes.

There is a need for strong cooperation, not only at LEA level but also with private industry, like ISPs, credit card companies and financial institutions. All should give their strong support on this matter.

It would also be useful to promote an awareness campaign by the competent bodies in order to properly inform users about the risks of using internet pharmacies. At the moment, only a few countries are taking action in this area, although many already recognize that there is an issue. However, the traffic of

72 Dow Jones and Reuters published 22 March 2004

drugs, especially those that are illegal, is a fundamental resource for criminal organizations that can count on e-avenues to earn money.

Conclusions and

Recommendations

A Quick Look to the Future

This report has tried to explain how hi-tech may facilitate criminal behaviour in each of the different subjects described. The report had to deal with some consistent constraints: one of them is clearly the lack of sufficient data about the internet; it is always difficult to gain a reliable global overview.

The Internet in particular continues to offer more and more opportunities to users; new generations of services and devices are continuously available online, new web technologies come out every day and new solutions on how to manage information and services are appearing on technological markets.

Web 2.0[73] is a significant example of how to create and manage new services, and sharing resources. This will surely have a great impact on high tech crime investigations and will generate new threats.

Several companies on the internet offer large storage space on their servers where users can save a lot of information. The Internet is really internationalising communications: Google is procuring a lot of services and managing them centrally at one point. It currently offers several translation services and even searches in more than 110 different languages[74]. 'Google Talk'[75] is another vast resource to network people and communications.

Gmail[76] is a clear example of the mass of information that can be stored in a webmail server. Subscription is free, the interface allows the usage of 40 different languages and 260GB are available for storage. This makes the facility ever more flexible and versatile, just considering that emails can be viewed directly on a mobile device.

Moreover, the Eastern part of the world should not be forgotten. Currently, Google in China[77] actually counts 150,000 guests, with all parallel services offered.

Geocoding[78] is again an additional and valuable opportunity as an application that assigns geographic identifiers. Amongst other features, it can locate images, associating them to the related IP address that identifies the area where the picture was taken. Geocoding gives the future regionalisation of searches over the internet.

Plenty of services can be managed remotely and users can access resources directly from their computers at home; even operating systems could be placed remotely

73 http://en.wikipedia.org/wiki/Web_2.0

74 http://www.google.com/language_tools?hl=en

75 http://www.google.com/talk/

76 http://mail.google.com/mail/help/about.html

77 http://www.qq.com/

78 http://en.wikipedia.org/wiki/Geocoding

and the machine when booting could access those services through the open internet connection directly.

One great opportunity afforded by the user is to engage a smaller part of the machine's memory which can be dedicated to store other information. Moreover, the ADSL connection is becoming more and more affordable and therefore users are becoming keener to connect to the internet. A recent study revealed that in the UK alone, the number of online users is expected to be 64% by the end of 2008[79].

Other online services are dating sites and blogs[80], where people place their messages, personal data, photos and movies[81], all of which eases social networking. Everyone can create their own blog. Dating sites collect millions of customers from all over the world; the host servers are enormous recipients of information and therefore new profiling techniques are appearing on the market.

New models in accessing network systems and the concerned utilities are now in place. The Single Sign On (SSO)[82], for example, is a software authentication system that uses a web interface, allowing the user to access a series of services. There will be only one authentication server where this task will be deferred and through a cascade mechanism, the system will grant the user access to several web based applications and services. Microsoft improves the security of its authenticating system called Kerberos placed in Windows Vista: the future is the biometrical access to the networks.

The flat rate of ADSL connections makes the convergence of numerous applications into one more and more desirable. The use of VOIP[83] is growing dramatically and in the future there will be less usage of Public Switch Telecommunication Network (PSTN) and more reliance on internet telephony. Fierce competition amongst service providers, through the lower rates offered as well as additional features such as chat and file sharing, will raise the possibility for users to choose this or that provider.

Groove[84], recently bought by Microsoft, is a new concept of virtual office and will be included in the professional version of the Microsoft package in 2007. The data stored into the users' hard drive will be encrypted causing the imaginable troubles to forensic investigations.

The problem of authentication, especially for internet services, is still one of the most significant issues under debate. E-banking is very much utilised by most internet users and the chapter regarding phishing explains extensively this issue in its entirety.

79 http://www.vnunet.com/vnunet/news/2165994/uk-broadband-penetration-double published 9 Oct. 2006

80 http://www.blogger.com

81 http://www.youtube.com/ and http://www.myspace.com are just two examples of the two most known websites

82 http://en.wikipedia.org/wiki/Single_sign-on

83 www.voipsa.org/Activities/VOIPSA_Threat_Taxonomy_0.1.pdf this reports describes the new threats on VOIP

84 http://www.groove.net/home/index.cfm

Last but not least, the Microsoft Vista operating system will be introduced in 2007; it is predictable this will bring along new threats, although Microsoft has invested a lot in security countermeasures such as re-writing the source code, setting new anti-phishing filter, and incorporating malicious software removal tool just to name few. In particular, the encryption application called Bitlocker embedded into Microsoft Vista will impact seriously the forensic investigations carried out by LEA in analysing hard drives.

The Conclusions

The increasing 'technicalisation' of the modern world offers great opportunity for all mankind, including criminals. The availability of modern technology creates both the opportunity for new types of crime, and for new ways of committing more traditional crimes. Together these aspects have become known as HTC.

Occurrences of HTC are becoming apparent in all other areas of crime which Europol is mandated to deal with, giving it what is increasingly termed a 'vertical' and 'horizontal' natures.

Furthermore, being virtual, HTC is completely cross-border; in fact Internet makes HTC borderless. The fact that HTC often requires careful planning and expensive investment, against the potential for high criminal profits, inevitably makes it an area where serious organised crime becomes involved, a point explicitly recognised by the 2006 Europol Organised Crime Threat Assessment (OCTA) which stated:-

Technology is increasingly becoming a facilitator for Organised Crime. New types of fraud such as data streaming of payment cards have emerged in recent years, and traditional forms of crime such as money laundering, drug sales, the dissemination of child abuse material and prostitution have evolved as a result of technological developments. The internet has had an especially profound effect on crime.

It is hoped that this report is viewed as a tool to support the strategy and the cooperation amongst different stakeholder that manage technology every day.

Having described just some examples of new trends in the near future and how hi-tech can be lawfully used by the internet community, Europol has tried to draw a picture of what it could be expected and on which fields and topics more attention should be paid.

Following the methodology and from the information collected, the next points can be highlighted especially in relation to intelligence gaps:

- There is still a lack of consistent data about organised crime due to the volatility of the internet, no common reporting system about hi-tech crimes and a lack of reporting by the victims.

- There is little information about internet communities because they are closed groups and it is difficult to penetrate them.

- There is still a preponderance of US sources instead of European ones, hindering the collection of information about the European market.

- The horizontal use of hi-tech is more and more beneficial for organised crime; investigators are always followers. Several cases have been exposed by LEA in which criminal organisations massively use Hi-Tech to pursue their goals.

- The main driving factor for criminals is usually money. 'Hacking for Dollars' is proof of how the internet facilitates criminals in gaining illicit revenues.

- There is a rapid growth of underground economy through attacking computer systems. Hackers sell their skills online to the best bidder; the example of renting 'Exploits' or BOTNETS is very significant.

- The new generation of crimewares is more vicious, aiming at not only destroying the computer system but also to extract data.

- In general, there is a consistent growth of social engineering on the internet; the identity theft is strongly involved. Phishing, Pharming and lately Vishing and Smishing are the avenues to illicitly gain money.

- E-commerce, and in particular the traffic of stolen credit cards on the internet, is one of the chief ways to launder money and to finance criminal as well as terrorist organizations.

- It is possible to notice an increase of child abusive content distributed and exchanged over the internet. The spread of the internet all over the world has generated the increase in the availability of child abusive content and the possibility for child sex offenders to better communicate among each other in order to find new material. As a consequence of this greater demand, cooperation with NGOs and private industry is needed.

- A consistent threat to Europe is still emanating from Eastern European countries: investigations and reports already mentioned in this report bear witness to this.

- The Internet enables organised crime to have a very flexible structure; criminal organisations easily change tactics after a police crackdown, have several links at international level with other members, and exploit the internet as a networking tool.

- HTC is beginning to be of concern to the public, who is beginning to assess criminal potential. The threat to critical information infrastructure networks is a real example.

- Because new services are placed in remote servers, we are likely to go back to the mainframe concept instead of the current personal computer one. This will generate an impact on forensic investigations and on the relations with the first responders.

- One of the main critical issues is still authentication: a large proportion of business is currently conducted on the internet and users face problems at the authentication stage with computer systems.

The Recommendations

Based on the above, the following recommendations can be made:

- There is a need to share more intelligence and for enhanced cooperation amongst all stakeholders; the more information is shared, the easier it will be to build an efficient common strategy to properly fight HTC. The Internet facilitates the split of different tasks amongst criminals that come together towards the same goal. The example regarding BOTNETS is very exhaustive, as well as the proliferation of new potent crimewares. The Internet has reduced considerably the distance between members of criminal organisations. Terrorists use the internet for many criminal purposes such e-learning.

- There is a need to improve common understanding with private industry; the private sector is one of the main sources and ways for LEA to tackle HTC.

- There is a need to improve the cooperation with the free software developers on the internet which constitutes nowadays a large foundation of information and products used as open sources by all internet community.

- There is a need to educate users of internet on how to utilize technologies. Handling HTC is not only a LEA's issue, therefore proper awareness programmes for the users should be organised. Information is an asset and it has to be protected. Education is the keyword.

- The ratification of the Cyber Crime Convention should never stop until it has become the largest common legal platform amongst countries. Although the treaty has been ratified by the USA recently, giving a great boost to the tackling of HTC[85], the process should never end. Moreover, all countries should make an effort to update their legislation, keeping pace with technology.

- There is a need to harmonise forensic investigations in order to have a common approach about how to present evidence at court.

- There is a need to pay a great attention to the encryption that is still one of the main solutions for criminal to conceal evidences.

- ISP and Telecoms cannot be deemed the only ones responsible for data retention and preservation; some businesses should be considered accountable as well. Therefore, there is a need to improve the cooperation with these new data storage enterprises.

- There is a need to solve the problem of the use of VOIP in terms of encryption, data retention/preservation and last but not least the interception.

85 http://www.usatoday.com/tech/news/techpolicy/2006-08-04-cybercrimetreaty_x.htm published on 4 Aug. 2004

- Critical Information Infrastructures are targeted by hackers and the right amount of attention should be paid to this issue, especially to devise a common European strategy.

All the above points are complex but given what has happened in the last few years, the rapid technological development impels LEA to keep the same pace. Unfortunately, criminals are always one step ahead in using hi-tech for their purposes and investigative bodies have difficulties in keeping abreast.

Nevertheless, it should be acknowledged that International organisations are already carrying, for instance, many initiatives in order to facilitate coordination and action against cyber crime:

- The Council of Europe is one of the main actors and points of force in fighting HTC. The Octopus programme is a firm milestone within many stakeholders work for the discussion and implementation of the cyber crime convention. In fact, the Council of Europe is working for the implementation of the Cyber Crime Convention that is going to be ratified by additional countries in the next months. Many States will finally have a common legal platform, whose lack has been one of the main hurdles in fighting HTC.

- The European Commission is continuously working on the topic of data retention and amongst other things is paying great attention on the development of new technologies in order to rightly influence the policy at EU level. The European Commission has already issued a new strategic policy paper on cyber crime[86]. The document, that stresses the need for the creation of a common EU and international policy on cyber crime, proposes amongst others the following main objectives to be pursued[87]:

    - Improvement of operational cross-border law enforcement actions against cyber crime in general and against serious forms of cyber crime in particular, and to improve exchange of information, intelligence and best practices between law enforcement agencies in Member States and beyond

    - Identification and creation of operational instruments for cooperation and common goal-setting between the public and the private sector and to improve the exchange of information, intelligence and best practices for the fight against cyber crime between the public and the private sector at EU level

    - Establishment of a political platform and structures for the development of a consistent EU policy on the fight against cyber crime, in cooperation with the MS and competent EU and international organisations, and to make existing legal and institutional framework more effective, also by clarifying responsibilities and liabilities for all relevant actors

86 Document n. 10089/07 CRIMORG 102 published on 30.05.2007

87 Excerpt from the cited document

- To meet the growing threat from serious forms of cyber crime by promoting skills, knowledge and technical tools; including actions to strengthen relevant training and research

- To raise the overall awareness of the threat of cyber crime, especially among consumers and other vulnerable groups of potential victims, while avoiding to undermine the trust and confidence of consumers and users by focusing only on negative aspects of security

- Eurojust[88] enhances the effectiveness of the competent authorities within Member States when they are dealing with the investigation and prosecution of serious cross-border and organised crime. Eurojust, competent for the types of crime and the offences in respect of which Europol is at all times competent to act pursuant to Article 2 of the Europol Convention, has in computer crimes an area specifically mentioned in its mandate[89].

- OLAF[90] actively works in high tech areas especially supporting the forensic investigation at EU level.

- Interpol[91] is actively working in HTC areas through the very valuable contribution and efforts of European Working Party on Information and Technology Crime.

- G8[92] through its 24/7 experts' network mostly focuses on the first and prompt contact amongst the members in order to freeze the evidences, e.g. at ISP or Telecoms; the official international channels are subsequently involved to formalise the requests to obtain the logs. G8 group meets on regular basis and the forum gives a great opportunity to network and discuss HTC issues.

- CEPOL[93] is making a great deal of efforts to improve its cooperation with Europol in the field of training. As a result, Europol is supporting regularly CEPOL courses with its own trainers.

- European Network of Forensic Science Institutes (ENFSI)[94], established to share knowledge and experiences in the field of forensic sciences, holds in its within the Forensic Information Technology Working Group that studies all the information technology forensics and the technical disciplines combined to allow the examination of material which contain digital information in order to assist an investigation and, eventually, present evidence for a trial.

88 http://eurojust.europa.eu/

89 In particular the above issue regarding VOIP was raised during a meeting at Eurojust held last 29 September 2006 in which operators from Skype were invited to explain the functionality of this application and what kind of support Skype could give to investigative bodies.

90 http::://ec.europa.eu/anti_fraud/index_en.html

91 For more information see http://www.interpol.int/public/technologycrime.default.asp Moreover, the forum that takes place quarterly is composed by a group of experts who constantly feed the manual on computer crime investigations available to all LEA. The working party has regional approach dividing its competencies in different areas worldwide.

92 http://www.usdoj.gov/criminal/cybercrime/intl.html

93 http://www.cepol.net

94 http://www.enfsi.org/ewg/fitwg/

It is clear that LEA are trying their best to keep pace with the technological development of criminals to ensure that the crimes they perpetrate can be effectively prevented or detected. However, there still is a lot to be done; given the borderless nature of HTC, LEA and all the other stakeholders must ensure similarly high standard throughout the EU so as not to allow 'weak spots' to develop where HTC can flourish with impunity.

Despite all the considerations above, it must be borne in mind cooperation in the HTC arena is easier than one could think: irrespective of different legal systems and languages, in hi-tech crime investigations the same technical tools are mostly used. This will not only improve the chance to properly fight HTC, but will also give more confidence and trust to the whole internet community.