THREAT ASSESSMENT
(ABRIDGED)

INTERNET FACILITATED ORGANISED CRIME

iOCTA

O2 – Analysis & Knowledge
The Hague, 07/01/11
FILE NO.: 2530-264

TABLE OF CONTENTS

1. KEY JUDGMENTS & RECOMMENDATIONS

- The European Union is a key target for cybercrime because of its advanced Internet infrastructure, rates of adoption and increasingly Internet-mediated economies and payment systems. As Internet connectivity continues to spread, EU citizens and organisations will be subjected both to a larger volume of cyber attacks, and to attacks from previously underconnected areas of the world. Combatting cybercrime will therefore require **new international strategic and operational partnerships**.
- The dynamism of online illicit markets requires an equally dynamic response which is constantly updated. **Active partnership with the private sector** – especially Internet Service Providers, Internet security organisations and financial services – is essential to the success of this, not only for the sharing of intelligence and evidence, but also in the development of technical tools for law enforcement and design-based measures to prevent online criminality. The academic community also has an important part to play in the research and development of such measures.
- The global reach and scale of Internet Facilitated Organised Crime, its disparate nature, and the unprecedented volumes of data pertaining to it, present significant challenges to current law enforcement resources and skills. **Centralised coordination of intelligence** gathering, analysis, training, and partnership management is now required at an EU level, to ensure that Member States and EU agencies make the most effective use of their current investigative resources. The establishment of a **European Cybercrime Centre**, as outlined in the recent Council Conclusions on cybercrime, will be an important and timely step forward[1].
- Because of the pace of technological development cybercrime evolves on a daily basis. Law enforcement agencies need to factor this into their **strategic planning in order to ensure that there are sufficient resources** and skills to meet future threats.
- Internet technology increasingly facilitates a **wide range of serious and organised crime activity** as a communication, research, logistics, marketing, recruitment, distribution and monetarisation tool. Where not already the case, in the near future the vast majority of investigations into transnational Organised Crime will necessitate some form of Internet investigation. The online investigation of criminal networks should be a matter of course, as should the **extension of "Know Your Customer" legislation** to all online financial services.
- There is a **dynamic relationship between online and offline Organised Crime**: control measures applied in one environment may displace crime into another, while new opportunities may cause criminals to turn away from higher risk activities. Such flexibility demands that investigators be equally aware of the online and offline environments in which criminals operate.
- Botnets are the tools most crucial to cybercrime's industrialisation and profitability. Their dismantling has a clear impact on the capability of cybercriminals to act on a large scale. The public and private sectors, the academic community and volunteer organisations work together with law enforcement to achieve this. The **dismantling of botnets must be an international policing priority**.
- Given the role of social engineering in current criminal business models, awareness raising and the engendering of individual and corporate user responsibility are key to combatting cybercrime. **EU-wide awareness raising programmes** are now required for:
    - Illegal downloaders unaware of the links with Organised Crime
    - Individuals on the subject of social engineering
    - Organisations on responsibility for data breaches
    - Payment card holders on transaction security

[1] Council of the European Union, *Council conclusions concerning an Action Plan to implement the concerted strategy to combat cybercrime*, 3010th GENERAL AFFAIRS Council meeting, Luxembourg, 26 April 2010

- Children on the risk of online solicitation for sexual purposes
- Wireless Internet subscribers on the misuse of unsecured connections

with **dedicated points of contact** for the public to report and receive advice on the above.

2. BACKGROUND

This document is an abridged, public version of Europol's threat assessment on Internet Facilitated Organised Crime. It has been produced in line with the objectives of the Stockholm Programme and the Draft Council Conclusions on an Action Plan to implement the concerted strategy to combat cybercrime[2], and to assist in strategic planning for a European Cyber Crime Centre. Findings are based on intelligence submitted to Europol by law enforcement agencies of the EU Member States and a range of open source material.

3. INTERNET FACILITATED ORGANISED CRIME

As a communication tool, information source, marketplace, recruiting ground and financial service the Internet facilitates all types of offline organised criminality, including illicit drug extraction, synthesis and trafficking, trafficking in human beings (THB) for sexual exploitation, illegal migration, Mass Marketing Fraud (MMF), MTIC (VAT) fraud, Euro counterfeiting and the trade in prohibited firearms. In particular, the perceived anonymity afforded by communications technologies such as email, instant messaging and Internet telephony (VoIP) has led to them being used increasingly by Organised Crime groups as a countermeasure to law enforcement detection and surveillance.

Online banking provides Organised Crime groups with the opportunity to move criminal assets faster than ever before, and irrespective of offline geographical barriers. Online gambling is used for the laundering of criminal proceeds, as are the in-game currencies of virtual worlds. Virtual payment systems have also been used by Organised Crime for laundering and monetarisation.

The widespread adoption of Internet technology in the EU has also prompted an unprecedented expansion in the markets for child abuse images and intellectual property theft, especially for copyrighted audio-visual material and software. Child victims of sexual abuse are exposed to prolonged victimisation as a result of the global and continued circulation on the Internet of visual records of their abuse.

3.1 The Digital Underground Economy

There is now a sophisticated and self-sufficient digital underground economy, in which data is the illicit commodity. Stolen personal and financial information – used, for example, to gain access to existing bank accounts and credit cards, or to fraudulently establish new lines of credit – has a monetary value. Not only credit card details and compromised accounts, but also information such as addresses, phone numbers, social security numbers, full names and dates of birth are retailed in this market. This drives a range of new criminal activities, such as phishing, pharming, crimeware distribution and the hacking of corporate databases, with a fully fledged infrastructure of malicious code writers, specialist web hosts and individuals able to lease networks of many thousands of compromised computers to carry out automated attacks. As this economy has grown in sophistication, mature technical service providers such as payment card verification number generators and illicit data brokers have emerged. Whilst the value of the cybercriminal economy as a whole is not yet known, one recent estimate of global corporate losses stands at approximately $1 trillion per year[3].

Payment card fraud is of particular note because of the way in which this type of organised criminality blurs the distinction between online and offline activity, and highlights the profitability of data in both environments. Payment card data – especially from credit cards – is the ideal illicit Internet commodity because of the ease with which it is internationally transferred. Organised Crime groups benefit from globalisation, moving to different countries and even different continents to withdraw cash from skimmed cards, and using foreign

[2] CRIMORG 22
[3] McAfee at the World Economic Forum, Davos, January 2009 – http://www.mcafee.com/us/about/press/corporate/2009/20090129_063500_j.html

payment data to purchase services such as transport and accommodation online, thereby obscuring the money trail attached to this type of criminality.

3.2 Cybercriminal Business Models

The structure of cybercrime groups marks the cleanest break to date from the traditional concept of Organised Crime groups as hierarchical. Very often there is no obvious leadership, labour is divided according to individuals' technical specialisms, and most members know each other only online. Online forums are therefore essential introduction and recruitment services for the digital underground economy. These both facilitate collaboration and exhibit a degree of organisation at the administrative level, enabling criminal elements to swarm together to work on specific projects[4]. They are also where crimeware components are advertised, and budding cybercriminals learn their trade by means of tutorials.

Moreover, it has been argued that cybercrime's organisation lies in its automation, which by using the force of technology dispenses with the operational requirement for physical groupings and force of numbers[5]. In this context, botnets – networks of infected "zombie" computers – are crucial to cybercrime's profitability. With a botnet, cybercriminals can make use of many thousands of compromised computers at a time to automate attacks on private individuals and corporate systems, send spam, host phishing websites, distribute crimeware, mount denial of service attacks and scan for vulnerabilities: without one, they must target victims and machines manually and individually.

The monetarisation of data is likewise essential to cybercriminal enterprise. "Mules" are recruited via employment search websites and social networking sites to "cash in" stolen personal and financial information, very often in different jurisdictions to those from which the funds have been removed. As the individuals tasked with turning data in hard cash, mules are the visible face of cybercrime.

The high-tech nature of cybercriminal activity results in a demographic profile not traditionally associated with transnational Organised Crime – namely, young, highly skilled individuals who are often recruited from universities. These features find analogies in hacker culture more generally, where absence of hierarchy, celebration of technical proficiency and comparative youth are prevailing characteristics. This younger offending demographic is to some extent maintained by the ready availability of exploits and attack tools on the Internet: one recent study found that over 60 per cent of hackers surveyed were under the age of 25, and that a similar proportion had started hacking between the ages of 10 and 15[6]. Phishing and spamming require fewer technical skills than some other types of cybercrime, while complete crimeware kits like Zeus arguably make attacks more accessible.

3.3 Cybercrime 2.0

"Web 2.0" is the term often used to describe the ongoing transition of the World Wide Web from a collection of websites to a fully fledged computing platform which has spawned a second generation of Internet based services – such as social networking sites, wikis, and real-time communication tools – that emphasize online collaboration and sharing among users. This has both been of great benefit to the general public and provided new and creative opportunities for the digital underground economy.

Significant in this regard is the ability of web developers and users themselves to draw web page content from a number of different sources: just as Facebook users are able to embed videos from YouTube or photos from Flickr on their profile pages, and application developers are able to market tools and games to the users of social networking sites, so also do

[4] Arquilla, J. & Ronfeldt, D. (2000) *Swarming and the Future of Conflict*, http://www.rand.org/publications/DB/DB311.pdf
[5] Brenner, S. (2002) "Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships", *North Carolina Journal of Law and Technology* 4: 1-50
[6] Chiesa, Ducci & Ciappi (2009) *Profiling Hackers: The Science of Criminal Profiling as Applied to the World of Hacking*, Boca Raton

cybercriminals inject malicious code into posted items and share links to phishing and pharming websites, exploiting the trust of users who consider themselves to be in a "closed" network of acquaintances. An increase in crimeware delivery through social networking sites has been one of the key trends in recent years.

In as much as social networking sites are environments in which users feel a sense of security, they enable cybercriminals to bypass the more labour intensive aspects of social engineering so characteristic of offline and email-based attempts to elicit personal and financial information. Moreover, the unprecedented size of social networking's user base - there are, for example, as many Facebook and Twitter accounts as there are EU citizens[7] – provides the digital underground economy with a ready-made means of distribution for malicious software.

"Augmented Reality" is the term commonly used for Internet mediated services which enhance a user's interaction with the physical world, the most widely used current examples of which are perhaps satellite navigation, Google Earth and location based applications which give information on local services. Online location-based services such as Foursquare and Google Buzz have developed in tandem with social networking to allow users to locate their friends more easily offline, and to add geographical information ("geotagging") to visual or written content. Concerns are already being expressed over the willingness of Internet users to divulge their offline locations, as there is an obvious security risk run by users of social networking sites who clearly state that they have left their personal property unattended. As an increasing number of services encourage transparency concerning real-time offline location, Organised Crime groups will increasingly seek to use social networking as a research and target selection tool.

Web 2.0 has also resulted in the development of services which aggregate personal financial information from savings and checking accounts, credit cards, investments and loans. Since these platforms enable access to a range of assets with a single set of log in credentials, it is reasonable to expect that they will be of interest to criminals engaged in the retail and exploitation of personal financial data.

3.4 Social Engineering

Social engineering – the act of manipulating people into performing actions or divulging confidential information – is a key feature both of hacker culture and of many cybercriminal *modi operandi*: when engaged in phishing and its variants, criminals commonly seek to persuade recipients that they represent organisations requiring verification of customers' personal data; spoof websites are designed which replicate legitimate online services such as banking, to dupe customers into inputting their account details; social engineering even plays on the fears of Internet users that they will fall prey to this very tactic, manipulating them into paying for rogue anti-virus software which can otherwise be obtained for free, is useless, or in fact contains crimeware.

Social engineering has been the dominant feature also of Advanced Fee Fraud, from the letters which first came to prominence in the socio-economic context of Nigeria's oil boom, through its migration to fax technology in the late 1980s, to its wholesale transformation in the Internet age. Advanced Fee Fraudsters entice victims with the promise of gain, often fleshing out approaches with elaborate narratives which respond to current or recent events. This type of fraud continues to be profitable not only because Internet-mediated mass mailing technology provides fraudsters with a cost effective means of scaling up their activity, but also because of the vulnerability of Internet users to psychological manipulation, particularly when this incorporates the prospect of reward. Accordingly, Internet users from a variety of social backgrounds continue to pay release fees for non-existent legacies and lottery winnings.

External social factors also have a bearing on levels of vulnerability: while the effects of the ongoing economic crisis do not appear to have hindered the underground economy's attacks on financial services, Internet users may be more susceptible to scams which promise to save them money, or indeed may discover more incidents of fraud in the course of subjecting their

[7] 400 million Facebook and over 100 million Twitter accounts, April 2010

finances to greater scrutiny. In this context, the prevention of cybercrime is as much a matter of raising awareness amongst Internet users as it is of employing technical solutions to combat infection and data loss.

4. CHALLENGES AND OPPORTUNITIES

Internet Facilitated Organised Crime exhibits unprecedented mobility and dynamism, and operates on a scale which places substantial and increasing demands on law enforcement. The global and often disparate nature of this type of criminality, and the ability of criminal groups to launch mass, automated attacks, requires highly responsive and internationally coordinated control measures: this is particularly the case for cybercrime, where individual offences may only attain significance when viewed from an international perspective[8].

Underreporting is an obstacle to appreciating the true scale and nature of cybercrime. Individuals may fail to report because they simply do not notice the offence taking place (e.g. in the case of infection by crimeware), because amounts lost to fraud may be considered too small to be of interest to police, or because (especially in the case of Mass Marketing Fraud) they may be subject to blackmail or threats of violence: organisations, particularly those in the financial and retail sectors, may fear a loss of reputation. In addition, it is likely that since government law enforcement agencies are not the only ones engaged in policing online environments, a number of incidents reported e.g. to service providers may not be finding their way to the competent authorities[9]. The essentially international nature of cybercrime and the multiplicity of actors even within law enforcement often results in a lack of clarity concerning the ownership of investigations. To meet this challenge, Europol's Internet Crime Reporting Online System (ICROS) will provide centralised coordination of reports from authorities in EU Member States.

4.1. The Need for Cross-Sectoral Working

The highly resource intensive nature of cybercrime investigation in terms of the scale of identified offending and volume of data generated is compounded by the requirement for sufficient numbers of investigators with specialist technical and linguistic skills[10]. In this context, external partnerships are fundamental to the successful investigation and prosecution of cybercrime.

Active engagement with the private sector is now a priority, to ensure that criminal offences facilitated by the Internet are properly identified and referred to law enforcement. Both Internet service providers (ISPs) and Internet security organisations monitor the Internet for suspicious traffic: law enforcement can therefore draw on their resources and technical skill to investigate and prosecute cybercrime more efficiently and improve its knowledge of Internet-facilitated offending. This is not simply a matter of data access, however, although this is an essential requirement. From an investigative perspective, law enforcement must continue to work with the private and other sectors to develop technical tools and strategies for the investigation of Internet facilitated criminality: in recent months, Internet Service Providers (ISPs), Internet security companies, defence intelligence organisations, volunteer monitoring organisations and the academic community have all been instrumental in the dismantling of botnets[11].

Crucially, there is also scope for the authorities and providers of Internet infrastructure and online services to collaborate in the provision of design-based crime prevention solutions, just as architects and urban planners seek to design crime out of the offline world[12].

[8] Wall, D. (2007) *Cybercrime: The Transformation of Crime in the Information Age*, Cambridge
[9] Wall, D. (2007) *Cybercrime: The Transformation of Crime in the Information Age*, Cambridge
[10] Hunton, P. (2009) "The growing phenomenon of crime and the Internet: a cybercrime execution and analysis model", *Computer Law and Security Review* 25: 528-535
[11] E.g. the Storm and Mariposa botnets – http://www.darkreading.com/insiderthreat/security/client/showArticle.jhtml?articleID=223101396
[12] Katyal, N. (2002) "Digital Architecture as Crime Control", *The Yale Law Journal* 112:2261-2289

Users and user groups also have important roles to play in the prevention of Internet-facilitated criminality, both at the individual and organisational level. Just as lack of public awareness and user neglect of security measures facilitate cybercrime, so too does an increased sense of online civic responsibility have the potential to reduce cybercriminal activity[13]. At the level of the private individual, this can be achieved through coordinated awareness raising and the provision of a central point of contact, to which EU citizens can report offences and turn for advice. In organisations, the regulation of standard data and communications security measures and a requirement for reporting data breaches to the authorities would go some way to harmonizing the responses of law enforcement and the private sector[14].

Closer engagement with one particular section of the Internet user base – the hacker community – would arguably bring significant benefits to those with a responsibility to prevent cybercrime. In addition to gaining insights into hacker motivation and methods, such as those of UNICRI's Hacker Profiling Project, consideration should be given to making best use of the sense of civic responsibility and Internet stewardship shown by certain ethical hacker groups[15].

4.2 The Mobility of Data

Wireless technology (Wi-Fi) has enabled Internet users to have more flexible access to the Internet. As an increasing number of companies and services provide wireless access nodes and hotspots, users expose their personal data in these environments, while others make use of open access zones and unsecured private connections to mask criminal activities, with the potential that unwitting account subscribers are held liable for criminal offences committed using their connections. Raising public awareness of such is one way of encouraging Internet users to take responsibility for the security of their own connections. In the longer term, the introduction of WiMAX wireless access across entire cities, and technology to turn devices such as vehicles into wireless hotspots will require the authorities to continue to develop other means to protect user data and identify criminal targets.

Hardware developments have likewise enabled more flexible access to the Internet and greater portability of data. Preventing cybercrime is no longer simply a case of protecting home computers: many users now have access to a PC, a laptop, a smartphone and a games console, all of which have processing power and Internet connections, and are therefore vulnerable to attacks. Crimeware for smartphones is already in circulation, while Denial of Service (DDoS) botnets are active on the XBox Live gaming platform.

Mobile devices are increasingly the primary tools for connecting to the Internet, and are being marketed in large numbers to areas of the world which have previously enjoyed limited Internet connectivity. The "always on" culture fostered by mobile devices ensures that potential victims are online, and their data exposed, for a longer amount of time, while the mass distribution of corporate smartphones and the increasingly porous boundary between individuals' professional and private lives has resulted in cybercriminal exploits against iPhones and Blackberries in an attempt to access data which mirrors information on corporate servers. Handheld devices are arguably also less physically secure than notebooks and desktop computers, in as much as they are more likely to be subject to loss or theft, and less likely to be encrypted (many organisations disable encryption in order to preserve battery life and optimise performance).

Widespread availability of mobile processing power and Internet connectivity means that crime also is more mobile: this has brought greater efficiency to certain types of serious and organised criminality, such as the distribution of child abuse images produced by travelling sex offenders. Coupled with substantial increases in the amount of data and hardware to be

[13] Brenner, S. & Clarke, L. (2009) "Combatting cybercrime through distributed security", *International Journal of Intercultural Information Management* 1.3:259-274
[14] Brenner, S. & Clarke, L. (2009) "Combatting cybercrime through distributed security", *International Journal of Intercultural Information Management* 1.3:259-274
[15] Chiesa, Ducci & Ciappi (2009) *Profiling Hackers: The Science of Criminal Profiling as Applied to the World of Hacking*, Boca Raton

analysed, this improvement in criminal productivity and operational speed presents a clear challenge to current law enforcement response capability.

5. EMERGING & FUTURE TRENDS

The world is increasingly dependent on high-tech communications and banking systems. As the globalisation of markets further accelerates – with an increasing number of international virtual economies – there will be more data to compromise, with a higher impact, particularly for those developing economies which will depend on globalisation and connectivity to thrive. Internet facilitated organised crime will likewise continue to increase in line with broadband Internet uptake, finding new offenders and victims in areas of the world where Internet access has previously been limited to large organisations and Internet cafés. Even within the EU, differing national adoption rates for very high speed broadband and other emerging technologies are likely to affect the internal movements of fraud and crimeware activity.

Increasing bandwidth, automation, and criminal technical skill will also make cybercrime easier to commit. Criminals engaged in cyberfraud will continue to exploit the favourable market conditions of the last ten years, which saw both a substantial increase in e-commerce and a considerable reduction in the cost of being online. More specifically, the proposed introduction of carrier grade ethernet for Internet access in metropolitan areas has the potential to greatly increase the spread and speed of crimeware infections, while the promise of IPv6 to provide infinite web address space will likewise furnish a much larger number of websites vulnerable to criminal exploits, and vast new spaces for cybercriminality.

Globalisation, cost-cutting exercises and – in some cases – concern for the environment mean that larger organisations are increasingly moving towards deploying remote workforces. Technological developments have accelerated this trend, which threatens data security as much as it improves lifestyles, productivity and air quality.

5.1 Cloud Computing

Individuals and organisations are increasingly opting to outsource their data storage to third parties, as a cost-saving option and to enable remote access to data from any location. This poses both a threat to users and a challenge to law enforcement.

Data stored in “The Cloud” is not only accessible to all authorised users, but also vulnerable to external attacks. And whilst corporate owned servers are evidently themselves subject to hacking, the lack of direct control entailed by cloud computing raises concerns about whether security measures will be properly enforced by the storage provider, or understood by the data owner or customer. In the cloud computing scenario, for example, the personal and financial data of retail customers could be stored on the Internet by a third party without that customer’s knowledge, and without the direct control of the organisation who has processed that data. The key to cloud computing’s success and long-term uptake will be whether the convenience of remote access will be matched by confidence in its security provisions.

5.2 Corporate Virtual Worlds

Further evidence of the blurring of the boundary between corporate and private life is emerging through the introduction of corporate virtual worlds. Corporate social networks have existed in an albeit limited form for some time, in which organisations including law enforcement agencies have enabled access to corporate email and instant messaging on smartphones.

When public social networking sites (SNS) first became popular, organisations were concerned largely about the effect that access to these immersive services would have on productivity. A few years later, the majority of corporate and even government entities have accepted use of SNS at work, and the chief threat lies in the use of social sites and other Web 2.0 functionalities to distribute crimeware. Under the right circumstances, SNS access at work has

the potential to infect corporate networks with spyware and other means to harvest large amounts of personal, corporate and financial data for profit.

The expansion of remote working now demands a fully functioning replica of the office environment in which employees can interact directly in order to complete tasks as if they were physically present in the same location, rather than bound by the inherent delay of message exchange. Under-adopted functionalities such as video/avatar conferencing and collaborative document editing will finally come into their own, and arguably will be key to the success of remote working. As with the majority of Internet mediated technology, the level of encryption protecting these spaces from data theft and crimeware distribution is likely to be determined in the short-term by the speed with which users will need to access them and, ultimately, the time organisations are prepared to lose waiting for files to decrypt.

6. CONCLUDING REMARKS

The European Union comprises 7 per cent of the world's population, but just under a fifth of its Internet users. The global reach of the Internet, its networked processing power, and its provision of instant communication and data transfer technologies combine to create an environment in which every one of these 320 million citizens may fall victim to criminal activity from anywhere on the planet[16]. In short, the Internet eliminates distance, bringing the general public and Organised Crime activity into close proximity, and eroding the distinction between internal and external threats[17].

Mobile Internet access introduces new levels of vulnerability, with potential victims online for longer periods of time; the introduction of broadband Internet technology to developing countries poses a potential threat to the EU; and the increasing trend for outsourcing data management to third parties presents imminent risks to information security and data protection. While cybercrime requires a modest financial outlay, it is increasingly lucrative.

There is now an urgent requirement for authorities in the EU to optimise measures to counter cybercriminality in active partnership with other sectors of society, not only drawing on their knowledge of Internet culture, Internet facilitated criminality, and emerging technological developments with a view to anticipating criminal behaviour, but also pooling resources and expertise to deliver coordinated, high impact control measures and enforcement responses. In the ever escalating "arms race" between cybercriminals and the authorities, vulnerabilities in people, processes and technology will continue to be exploited: accordingly, the introduction of, for example, a European eID card for online authentication would not on its own prevent identity fraud and cyberfraud. Responses and proactive countermeasures must therefore address all three of these key areas, and the development of a centralised EU capability will be fundamental to their success.

[16] Internet World Stats – http://www.Internetworldstats.com (data to 31/12/09, accessed 10/05/10)
[17] Brenner, S. & Clarke, L. (2009) "Combatting cybercrime through distributed security", *International Journal of Intercultural Information Management* 1.3:259-274