*Special Committee on Organised Crime, Corruption and Money Laundering (CRIM) 2012-2013*

**Thematic Paper on Organised Crime**

# Cybercrime - New Investigation Strategies and New Technologies

Author: Mrs Emma McClarkin (ECR)

September 2012

## Introduction

Every day 500 million people in the European Union and its economy rely upon international cyber networks. The World Wide Web is an invaluable resource with many opportunities, but it has also brought with it a formidable enemy. The prosperity and safety of the European Union is reliant upon these networks being secure as well as open.

Cybercrime is vast in both its definition and its effects, and is one of the fastest growing areas of crime. Cybercrime encompasses a diverse range of crimes, which require a diverse and skilled approach to combat them. Cybercrime can include attacks against computer data and systems, identity theft, the distribution of child sexual abuse images, Internet auction fraud, the penetration of online financial services, as well as the deployment of viruses, Botnets[1], and various email scams such as phishing[2]. The use of the Internet by terrorists, particularly for funding, recruitment and the incitement of radicalisation; and the threat of security vulnerabilities related to information technology infrastructure such as power plants, electrical grids, information systems and the computer systems of government and major companies, are all equally a challenge for law enforcement agencies and governments. [3]

The security and economic interests of the EU are now irreversibly tied with the rest of the world. No Government, company or institution is too big or sufficiently protected to not be a potential victim. Global high tech companies such as Google, as well as the Estonian Government and the European Commission have all been recent victims. However, the breach of the Estonian Government system in 2007 highlighted just how difficult it was to implement agreements, and organise a response, on an international level. The attack caused numerous problems; with certain Government and banking functions were unable to be carried out. Yet gaining agreement between the NATO Members as to whether Article 5 should be applied in this circumstance was a problem in its own right. Within the scope of a cyber attack, the definition of a hostile act of war was, and still remains, ambiguous.[4] Both NATO and the European Commission have recently formulated common policy areas, and new proposals, in order to update and renew international cooperation. The new proposals provide legal instruments and establish commonalities; but it is still a slow moving progress against a fast paced threat.

The anonymous nature of the Internet and the wide range of business and infrastructural functions that are carried out on the web have meant that the opportunities to wreak havoc and make money online are vast. More importantly the Internet is the greatest facilitator of anonymity. The origins of potential threats and attacks have the possibility of being spread throughout the world, involving whole networks of individuals and groups of people with the ability to plan and act together from across the world without ever having to meet. It is the ease of movement, the

[1] Botnets - a network of remotely controlled systems by third parties, used to coordinate attacks and distribute malware, spam, and phishing scams.
[2] Phishing - is the act of attempting to fraudulently acquire through deception sensitive personal information such as passwords and credit card details by assuming another's identity in an official-looking email, IM, etc.
[3] http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime.
[4] Article 5 of the TFEU - the Treaty on the Functioning of the European Union.

anonymity, and the profitability of the Internet, which has meant that the traditional structures of crime rings such as Hezbollah and the Mafia have moved out of shop fronts, and into cyberspace. It is estimated that criminal organizations are making 800 % more profits with piracy than with drugs.

**Impact on society, the changing face of crime**

In many ways cybercrime has become a socially accepted norm, something that a vast number of people do not take the effort to report. Many do not see it as "real crime", or believe that committing a crime on the internet is somehow less important than committing an offence in the "real world". It is crime without a face. It is essential that governments articulate the very real damages and costs of IP theft to both the economy and the consumer. Citizens need to be aware that often, unbeknown to them, they are committing or are complicit in a very serious and real crime, and often a crime that can result in a great deal of harm. The sale of fraudulent pharmaceuticals products online is booming. Consumers need to be made aware that it is estimated that 90% of the software, DVD's, and CD's sold in some countries are counterfeit, and that the total global trade in counterfeit goods is more than 600 billion USD a year. In the US alone, IP theft costs businesses an estimated 20 billion annually, and 750, 000 jobs.[5] Yet IP theft is a socially accepted practice, and seen as something that 'everyone does'. Consumers and internet users need to be made aware of the impact that IP theft and the online trade of counterfeit products has on people's health, the economy, jobs and growth, and the very serious reality that this is an industry that feeds into and proliferates serious and organised crime, terrorism, and the illegal drugs and arms trade.

**Awareness and Education**

Yet with regard to this booming criminal industry, there appears to have been comparatively little public awareness. Put quite simply, Governments and global organisations can do more to educate. 431 million adults worldwide were victims of cyber crime last year.[6] A large-scale global study suggests 5-10% of all domestic computers are regularly linked to criminal networks called botnets. The figures suggest that about 6% of the UK's 19 million net-using households are enrolled in botnets. At the top of the list of infection rates were Greece where nearly 20% of all broadband subscribers are thought to be regularly recruited into a botnet. More than 90% of spam is sent through botnets. The UK occupies the number 19 position in the top 20 nations with the biggest botnet problem. 89% of internet users avoid disclosing personal information online, and 74% agree that the risk of becoming a victim of cybercrime has increased in the past year. 12% of internet users across the EU have experienced online fraud already, and 8% have fallen victim to identity theft.[7]

And yet . . . . . just 47% of people changed any of their online passwords during the past year.[8]

---

[5] Sean B. Hoar, International Trends in Cyber Law Enforcement: The Dark Side of the Internet, International Security National Resilience Conference 2010, Abu Dhabi, United Arab Emirates, 2010.
[6] Norton Cyber Crime Report for 2011.
[7] Sean B. Hoar, International Trends in Cyber Law Enforcement: The Dark Side of the Internet, International Security National Resilience Conference 2010, Abu Dhabi, United Arab Emirates, 2010.
[8] July 2012, Eurobarometer report on Cyber security.

A great deal of progress can be made, by:

- Increasing awareness of illegal downloading and its links with organised crime;
- By educating people on the dangers of social networking, on personal responsibility for data breaches and payments for card holders and transaction security;
- By educating parents, legal guardians and children on the risks of online solicitation for sexual purposes;
- By making wireless internet users aware of the potential misuse of unsecured connections, and;
- By creating dedicated points of contact for the public to report and receive advice on all of these areas.[9]

Education is essential so that people are aware of how to protect themselves online, and of what constitutes online crime. Promotion of legal platforms for reporting criminal activity or websites, and giving online users the tools and the information necessary to do so, are essential ways of reporting and 'shutting down' of websites related to IP theft and websites that contain child abuse images.

**Impact on the economy**

The value of the online economy is currently placed at $8 trillion USD's each year.[10] $ 388 billion USD's is the estimated cost of Cybercrime to the global economy. To put this into context, the UNODC estimated that the global profits of the illicit drugs trade are $320 billion USD. The cost of cybercrime to the global economy is nearly 1% of the world's Gross Domestic Product or put another way, higher than the GDP of 88% of the countries in the world.[11] As for corporate cyber espionage, cyber criminals have stolen intellectual property from businesses worldwide worth up to USD 1 trillion.[12] Over the past year, the median cost of cyber crime increased by 56 percent and now costs companies an average of $6 million per year.[13] Moreover, cybercrime is slowly but surely eroding confidence in the internet and eroding confidence in the legitimate services which are provided online. The internet is worth £100bn to the UK economy alone, more than 7% of its national income, so it is essential in these economically challenging times that confidence is kept high.[14]

Therefore, the EU's emphasis ought to be on nurturing emerging technologies, and encouraging businesses to conduct effective and constant risk assessments on current systems, and further developing the sharing of best practice.[15] There must be repeated testing of our own systems with continued assessment of performance and failure. Such examples have been the United Kingdom Police Services who have been working on the development of a 'Best Practice' within the Intellectual Property Office, and bringing together all IP Crime Group members' resources to support businesses and enforcement agencies on Intellectual Property.[16] There have also been

[9] EUROPOL - Threat assessment - internet facilitated organised crime IOCTA 7/01/2011.
[10] Communication from the Commission to the European Parliament - tackling crime in our digital age. Establishing a European Cybercrime Centre.
[11] UNODC World Drug report 2005.
[12] http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime
[13] Second Annual Cost of Cybercrime Study - Poneman Institute.
[14] The internets economic impact - connect world series. Jan 2012.
[15] EU-US working group on cyber security and cybercrime.
[16] http://www.ipo.gov.uk/ipcreport11.pdf

steps taken by the UK Department of Business, innovation and skills to establish a global common response to Cyber security.[17] Such initiatives are being replicated throughout the EU, and throughout countries around the world. It is important that we keep building on this, to establish a real, effective and credible global network of businesses, law enforcement agencies and governments.

The promotion and protection of intellectual property and best practices must be made a priority by businesses and governments, and a key feature of the single market. Consistent dialogue between Governments, business, investors, consumers and the industry, as well as a better Early Warning System amongst international partners must be established. We must increase and coordinate penalties for those who build, use and sell tools and software designed to carry out cyber attacks, and seek to build a targeted and prioritized approach to the profitability of certain online tools such as botnets. The European Union needs to make combating cybercrime a viable option to our shared marketplace. Further work is needed to encourage the production of "safe" software, systems, and services which are appealing to the consumer as well as economically desirable. Governments must work domestically and internationally to achieve this in order to make investment attractive to the manufacturers, and purchasing desirable to the consumers. The support for innovation and the free market also has to feature prominently.

**Tackling the problem**

What can Europe do next? Firstly, it can examine how we can better implement legislation across the EU and enhance the existing tools that we have at our disposal. Europe will only ever be as strong as its weakest link. The EU should take action on the information that is provided and exchanged, and make sure that this system is quick and effective. In order for this rapid and effective exchange to take place we need to make sure that our legislators provide European governments, law enforcements agencies, businesses and homes with both the legal and practical tools necessary to combat cyber-criminals and the infringements they carry out. At present there is too greater disparity between Member States and third countries in the penalties that are applied, thus allowing for forum shopping where criminals carry out their activities.

Secondly, the solution cannot exist with law enforcement agencies alone. Combating Cybercrime must be done in partnership with individuals and businesses, so that they can look at how they can develop public-private partnerships between government and businesses to combat Internet crime and address security holes. Skills need to exist in banking, in industry, in homes, in schools, and in offices. It is only through skills and awareness being an everyday part of using the Internet that the effects of cybercrime, that the economic impact can be diminished. Fraud officers have been present in companies and banks for decades, looking for internal corruption and threats, yet this same rationale is not being applied to the external threats that exist in Cyberspace.[18]

[17] BIS Common Responses to a Global Challenge - Cyber security Forum 2010.
[18] EUROPOL - Threat assessment - internet facilitated organised crime IOCTA 7/01/2011

And finally, accuracy is required in where we harness resources and funding. Public and private sectors must make simultaneous investment in research, statistics, and technology, which at present is lacking. The effectiveness of law enforcement operations is reliant upon both technical and human resources. Investigations, whilst successful, are lengthy and labour intensive, and without suitable investment, solutions and results will be slow coming. Technological advances need to be developed and used to our advantage, so that we can gain the upper hand, and so that businesses and law enforcement agencies have answers that match the sophistication of the threat. At present, as quickly as new tools are developed, technology speeds ahead, overtaking those tools, it is a constantly evolving problem.

**International & inter agency cooperation**

The EU is currently responding to a crime that has no geographical or jurisdictional boundaries, and combating an area which is technologically developing and changing at a daily rate. Tools which have been created by the European Union include the 2011 Directive on combating sexual exploitation and child pornography; the Directive on attacks against information systems, which was due to be adopted in 2012; numerous operations and monitoring carried out by EUROPOL and ENISA , and attempts by the EU to seek consensus through the Council of Europe cybercrime Convention.[19] Now we await the newly established European Cybercrime Centre, also known as EC3. And yet, despite these efforts, you are more at risk of being a victim of cybercrime this year, than you were in the last.

It is clear that the only way we will find a lasting solution is through working together. Both the president of the United States and the Director of Europol have stated that cyber-security poses the greatest modern threat to civilisation. Increasingly, the realization is being made that cybercrime cannot be fought with an isolationist or uncompromising approach, and that diplomatic links must be made further a field than obvious historic allies. A good example of this cooperation is the FBI programme which has partnered with at least 60 nations to set up a network of legal attaches. The FBI has also embedded law enforcement agents with other equivalent agencies around the world who operate in Eastern Europe on organised crime. Other initiatives for inter-agency cooperation include recommendations from INTERPOL to establish a global list of contact officers available around the clock for cybercrime investigations by law enforcement agencies, (the list contained 131 contacts at the end of 2011), and to provide a secure web portal for accessing operational information and documents. [20] EUROPOL and INTERPOL must continue to strengthen their operational links, just as police forces and agencies throughout Europe and the globe must find ways of facilitating communication and information sharing.

Good communication and cooperation between the EU and its international partners, particularly the United States, is integral to our success in combating Cybercrime. Cyberspace transcends the geographical, economic, and social boundaries that exist in other industries and other criminal activity. The ability for the EU to operate with

[19] Council of Europe Cybercrime Convention - 23/11/2001. CETS No.: 185.
[20] National Security Council - Strategy to combat transnational organised crime. A Growing Threat to National and International Security.

third countries is as integral as the ability to operate well within its own borders. In order to strengthen this approach, Cybercrime should be tackled in a horizontal and crosscutting manner. Emphasis on cyber-security and the responsibility of third countries to tackle the problem should feature in trade agreements with third countries in order to respect the international priorities in the fight against IP fraud and Cybercrime.

It is important that the legislation and the tools which the European Union and the international community eventually create are both adaptable and flexible enough, as well as legally strong enough, to be effective in combating and prosecuting a teenager operating out of his bedroom, or a terrorist cell operating out of a country that we do not have an international agreement with. At an international level this is only complicated further by trying to find definitions and commonalities of cyber threats and sharing resources and information: a task the European Union finds difficult enough within its own Member States, without the reluctance to compromise on legal parameters and definitions, and rely on the capabilities of allies.

There have of course been previous international efforts, such as the Council of Europe's Convention on Cybercrime in 2001 (a Convention still not ratified by all countries), as well as recent proposals from NATO, the European Commission and the U.S. Administration. Yet despite the level of threat increasing, there is not a single international agreement on cyber security, even between great allies like the U.S. and the EU. A study by the ENISA concluded that European countries differed greatly in how they were prepared to deal with cybercrime and cyber attacks. The reality is that not all EU countries can agree how best to cooperate and take on the problem. It is therefore easy to understand that this is an issue not easily negotiated and concluded between the EU and the wider world, but we must persist.

**Conclusion**

The Internet has made the world a smaller place. Our security and economies are more inter-linked than at any other time in history. The global nature of this problem requires a global effort to find a solution. There is no silver bullet to tackle Cybercrime, but clearly an international and multi layered approach is the path forward. We must protect EU citizens from becoming victims of Cybercrime, especially minors and the most vulnerable. We should consolidate and renew confidence for consumers online. We have a duty to protect our knowledge economy and our ideas here in the EU; and to ensure that we invest in the creativity and innovation that will eventually provide a defence. It is our responsibility as legislators to make the Internet as safe a place as possible, and ensure that people can enjoy it as a place of freedom of expression and gained knowledge, free from harm or danger.