FIRST YEAR REPORT

EUROPEAN CYBERCRIME CENTRE

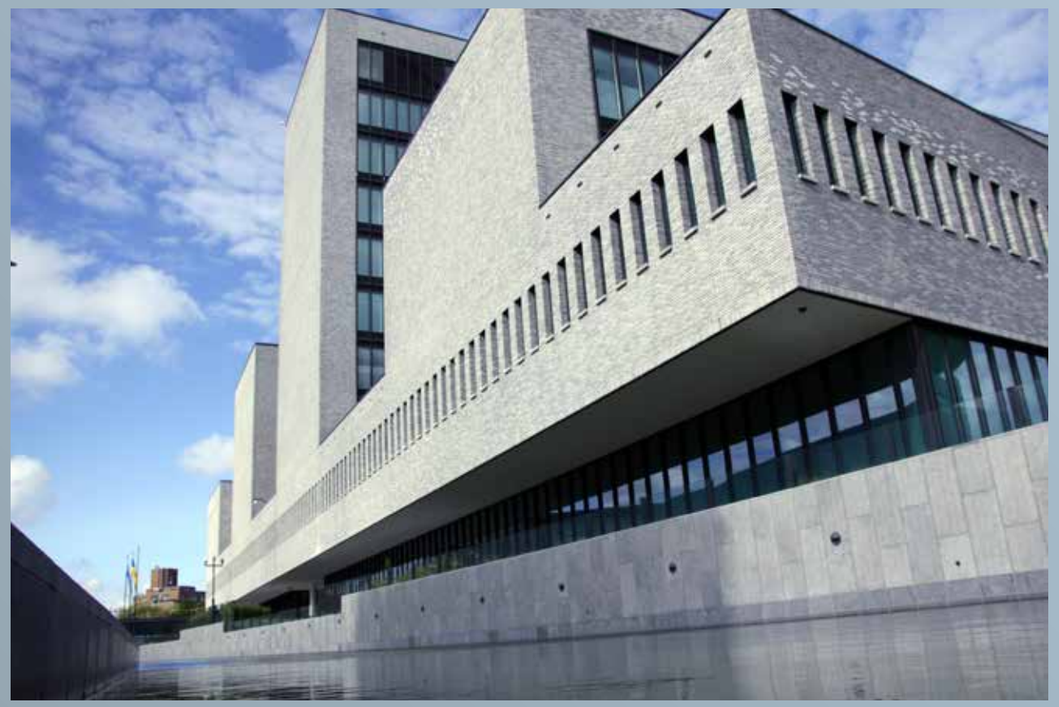
EC3

EUROPOL

Introduction

The European Cybercrime Centre (EC3) was launched in January 2013 to strengthen the law enforcement response to cybercrime in the EU and thereby help protect European citizens and businesses. The establishment of a European Cybercrime Centre was a priority in the EU Internal Security Strategy[1]. This report presents the highlights of the first year of EC3 and its future orientation.
This report's aim is to give EU Member States and institutions an insight into the establishment, performance and future perspective of EC3.

This should enable those stakeholders to assess if the actual developments live up to their expectations and – where needed – to contribute to policy decisions that optimise the course of the new Centre.



1 The EU Internal Security Strategy: five steps towards a more secure Europe. COM(2010)673 final, 22 November 2010.

Functions of EC3

The positioning of EC3 within Europol meant a continuation of some functions and a significant expansion of others that had already been in place for several years, in particular the operational and analytical support to Member States' investigations. In addition new functions were created specifically for the establishment of the new Cybercrime Centre. EC3 was tasked with focusing on the following three areas[2]:

- Cybercrimes committed by organised crime groups, particularly those generating large criminal profits such as online fraud
- Cybercrimes which cause serious harm to their victims, such as online child sexual exploitation
- Cybercrimes (including cyber-attacks) affecting critical infrastructure and information systems in the Union

With regard to these three areas EC3 was expected to:

- Serve as the central hub for criminal information and intelligence
- Support Member States' operations and investigations by means of operational analysis, coordination and expertise
- Provide a variety of strategic analysis products enabling informed decision making at tactical and strategic level concerning the combating and prevention of cybercrime
- Establish a comprehensive outreach function connecting cybercrime related law enforcement services as well as private sector, academia and other non-law enforcement partners to the work of EC3
- Support training and capacity building, in particular of competent authorities in the Member States
- Provide highly specialised technical and digital forensic support capabilities to investigations and operations
- Represent the EU law enforcement community in areas of common interest (R&D requirements, internet governance, policy development)

2 Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre, COM (2012) 140 final, 28 March 2012.

Creation of EC3

Europol launched EC3 in January 2013, only six months after the official decision to establish EC3 was taken. Fortunately the existing Europol framework, including its legal basis, corporate structure and information processing tools, offered a solid basis. Moreover, there was a knowledgeable team with practical experience and insight into the key issues and priorities of the subject matter.

A simple and lean organisational structure was designed to allow for an efficient delivery on the combination of tasks allocated to EC3 and to ensure strong cohesion and communication within the Centre.

EC3 Management

Operations

- Cyber Intelligence
- Cyborg: High-Tech Crimes
- Twins: Online Child Sexual Exploitation
- Terminal: Payment Fraud

Strategy

- Outreach & Support
- Strategy & Development
- Forensic Expertise (including Forensic Lab)

Due to the short timeframe between the decision to establish EC3 and its launch date, the implementation of certain parts and functions continued in the course of 2013. In this first year of existence the major achievements in the establishment of EC3 included:

- The official opening event with around 400 participants, representing the cybercrime community in law enforcement from the EU and cooperation partners, EU institutions and agencies, private industry and academia. It was important to create awareness among key partners about EC3's existence and the event contributed to a swift increase in EC3's involvement in cybercrime cases.

- The development of the forensic lab that provides a professional and fully equipped environment for technical support in digital forensics

- The development of the Multi-Disciplinary Centre for Cyber Innovation that provides a dedicated, technically suited environment for collaboration between law enforcement, private sector and academia on specific projects

- The delivery of several ICT tools and applications for the specialised processing of cybercrime related data, including two versions of the malware analysis solution, a large-file exchange tool, an encryption/decryption platform and an instant messaging facility within the communication platform

Performance of EC3 in 2013

Central hub for criminal intelligence and information – Cyber Intelligence

The key focus in this area is to bring together relevant data from various sources and to assess its relevance for Member States' cybercrime divisions and for the three operational teams in EC3 that each cover a specific crime area.

The Cyber-Intelligence Team at EC3 has worked tirelessly to enhance the work of the focal points. In 2013, the Cyber-Intelligence Team published 30 cyber-intelligence products, informing both law enforcement and private industry stakeholders of the latest threats and criminal modus operandi. Internet fraudsters, drug dealers and gun runners have all received the attention of the team in the first year of EC3. It has assisted with coordinating several cyber operations; one operation currently being coordinated involves several hundred suspects on whom intelligence has to be enriched and information packages prepared for arrests. The Cyber-Intelligence Team has also been involved in post-case analysis of cyber operations at the focal points[3].
These analysis reports act as references, creating corporate memory and training for EC3 and EU law enforcement when confronted with similar operations in the future.

3 Focal points are teams within Europol's Operations Department that are focussed on a specific category of crimes or criminal networks.

Support to operations and investigations

Even though Europol had been active for many years supporting Member States in their investigations into the various types of cybercrime, the continuation of this work under the European Cybercrime Centre has gone through a remarkable development. Whereas such investigations in the past had a predominantly national focus with some international links, the emphasis has now shifted towards the coordination of international cybercrime operations, which have required the development of much stronger cooperation with and through EC3. In all mandated areas of EC3 the size, complexity and number of operations has increased significantly. This has led to many more investigative actions and criminal arrests.

This tendency is likely to continue in the future given the active role of EC3 in the EU Policy Cycle . In 2013, preparations were made for the new cycle, which will run from 2014 to 2017. The consequence of the EU Policy Cycle[4] is that Member States will increasingly coordinate their law enforcement actions together at EU level, where they receive strategic and operational support from EC3.
The interest to work with and via EC3 was not limited to the competent authorities of Member States. Law enforcement agencies of the non-EU cooperation partners have also brought in cybercrime cases, participated in joint actions and strengthened their representation at Europol headquarters to better cover the domain of cyber related cross-border cooperation. Some of these partners have run a pilot with the posting of a cyber liaison officer or are considering this option (AU; CH; NO; US Immigration and Customs Enforcement), while others prepared or implemented more permanent plans in this regard already (Interpol; US FBI; US Secret Service).

In the following sub-paragraphs only those operations that have been concluded are presented specifically. Those that are still on-going are referred to at a higher level of abstraction to avoid compromising their outcome.

4 The EMPACT Policy Cycle was created in 2010 by the Council of the European Union to tackle the most important criminal threats in a coherent and methodological manner through optimum cooperation between the relevant services of the Member States, EU Institutions and EU Agencies as well as relevant third countries and organisations. Three of these top criminal threats have been identified in the realm of cybercrime, namely online and payment card fraud, cybercrimes which cause serious harm to their victims such as online child sexual exploitation, and cyber-attacks which affect critical infrastructure and information systems in the EU. This corresponds with the three specific crime types addressed by EC3.

Focal Point Cyborg: high-tech crimes (cyber-attacks; malware)

Focal Point[5] Cyborg assisted in the coordination of 19 major cybercrime operations in this first year of EC3. Two major international investigations that were concluded related to ransomware. 'Police' ransomware is a type of malware that blocks a victim's computer, accusing the victim of having visited illegal websites containing child abuse material or other illegal activity. Criminals request the payment of a 'fine' to unblock the victim's computer by displaying a splash-screen on their computer making the ransomware look as if it comes from a legitimate law enforcement agency investigating the illegal activities of the victim. Cybercriminals convince the victim to pay the 'fine' of €100 through two types of payment gateways - virtual and anonymous - as a penalty for the alleged offence.

It is estimated that the criminals infected tens of thousands of computers worldwide, bringing in profits in excess of €1 million per year. The first investigation led to 11 arrests and the second one to two arrests and the seizure of €50 000. More recent versions of the ransomware malware have been more aggressive, encrypting victims' data and making victims more likely to pay the ransom in the hope of retrieving their data.

Furthermore, Cyborg has supported several international initiatives in the areas of botnet takedowns, disruption and investigation of criminal forums, and malware attacks against financial institutions. The recent takedown of the ZeroAccess botnet with Microsoft and the high-tech crime units from the German BKA, Netherlands, Latvia, Luxembourg and Switzerland was an excellent example of a coordinated action taken by European police in partnership with private industry to dismantle criminal infrastructure on the internet.

5 Focal points are teams within Europol's Operations Department that are focussed on a specific category of crimes or criminal networks.

> *“ As stated at the outset of this disruption effort, Microsoft and its partners did not expect to fully eliminate the ZeroAccess botnet because of the complexity of the threat. [...] However, because we were monitoring their actions and able to identify new Internet Protocol (IP) addresses the criminals were using to commit their crimes, Europol’s European Cybercrime Centre (EC3) took immediate action to coordinate with member country law enforcement agencies, led by Germany’s Bundeskriminalamt’s (BKA) Cyber Intelligence Unit, to quickly track down those new fraud IP addresses. [...] Microsoft’s partnership with EC3 was crucial to the success of this disruption. In turn, EC3’s coordination with Member States’ law enforcement agencies like BKA in Germany and the National Hi Tech Crime Units from the Netherlands, Latvia, Switzerland and Luxembourg demonstrates the need for international cross-jurisdictional cooperation at a speed equal to the criminal cyber threats affecting people globally. ”*

Mr Richard Boscovich
Assistant General Counsel at the Microsoft Digital Crimes Unit

Other cases in which Focal Point Cyborg has been involved have targeted malware writers, fraudsters and hackers. The Focal Point has also supported the training of EU law enforcement officers, the coordination of operational and expert cybercrime meetings and the coordination of the European Union Cybercrime Task Force (EUCTF).

Challenges to the effective initiation and coordination of cybercrime operations have been EC3’s inability to receive essential evidence and intelligence directly from private industry[6]. Under-reporting of cybercrime to law enforcement, for fear of brand damage, has resulted in police not having the fullest picture of the extent and trends in cybercrime. This also prevents the sharing of threats with private industry to help protect them without undue delay.

6 Operational crime-related information, in particular personal data that comes from private companies and citizens, has to be reported domestically and routed to Europol via the National Unit of the Member State where they reside. In cases of multinationals this may cause difficulties because the information they hold may not be related to the country in which they are based. Some European countries have a high presence due to, for instance, their tax climate. In such countries there is then a large number of reports that are of no interest for the national competent authorities. For them it means that if they were to pass data on to Europol, they would first have the workload and secondly, the legal responsibility and ownership of that data as long as it is of relevance for EC3 to process it. In practice this hampers the flow of relevant information from important actors in the private sector to Europol and the law enforcement authorities of the affected Member States.

Focal Point Twins: online child sexual exploitation

At present, Focal Point Twins is supporting 9 large child sexual exploitation operations within the European Union. In the first year of EC3, significant efforts – jointly with many Member States and non-EU cooperation partners – were put into combating the illegal activities of paedophiles engaged in the online sexual exploitation of children using hidden services.

The Focal Point is involved in many operations and joint investigations targeting the production and distribution of child abuse material on various internet platforms. It is providing ongoing operational and analytical support to investigations on the dark net, where paedophiles trade in illicit child abuse material in hidden forums, as well as to investigations into 'sextortion'. Sextortion is the term given to the phenomenon where child abusers gain access to inappropriate pictures of minors and use these images to coerce victims into further acts or the abuser will forward the images to family and friends of the victim.

Furthermore, the Focal Point has initiated projects to improve information exchange on travelling sex offenders, in particular concerning EU residents travelling abroad for that purpose. And 2014 will see the beginning of a project to improve the EU-wide coordination of child sexual abuse victim identification.

In November 2013, Focal Point Twins organised its annual Child Sexual Exploitation Experts seminar at Europol headquarters. The seminar was attended by more than 190 representatives from law enforcement, the European Commission, Eurojust, Interpol, private sector partners, NGOs and academia. Spread over three days, the conference addressed important issues such as transnational travelling child sex offenders, police cooperation, victim identification, as well as cooperation among law enforcement authorities, hotlines, NGOs and the private sector.
In several Member States, child sexual abuse is reported online or through hotlines to NGOs. Therefore, in this crime area there is also a strong dependency on private industry partners and NGOs for obtaining important crime-related information as soon as possible.

Focal Point Terminal: payment fraud

Focal Point Terminal provided operational and analytical support to 29 major operations in 2013. The Focal Point supports operations with both card-present fraud (requiring the physical presence of the card for committing the crime) and internet based card-not-present fraud, as well as sophisticated ATM and retail point-of-sale terminal skimming attacks.

The year 2013 saw Focal Point Terminal support investigations that resulted in the dismantling of three different international networks of credit card fraudsters. One operation led to the arrest of 29 suspects who had made €9 million profit by compromising the payment credentials of 30 000 credit card holders.
The second network that was tackled resulted in 44 arrests during the operation (which followed 15 previous arrests; 59 arrests in total). During this operation two illegal workshops for producing devices and software to manipulate point-of-sale terminals were dismantled. Illegal electronic equipment, financial data, cloned cards and cash were seized during 82 house searches in Romania and the United Kingdom. More than 400 police officers were involved in this international operation. The organised crime group had affected approximately 36 000 bank/credit card holders in 16 European countries.

The third operation targeted an Asian criminal network responsible for illegal internet transactions and the purchasing of airline tickets on compromised credit card credentials. Two members of the criminal gang, travelling on false documents, were arrested at Helsinki airport. Around 15 000 compromised credit card numbers were found on the criminals' seized computers. The criminal network had been misusing credit card details stolen from cardholders worldwide. In Europe alone, over 70 000 euros in losses were suffered by payment cardholders and banks.

As stolen credit card details were reported as being frequently used to purchase airline tickets, a European Action Day against airline fraudsters was organised and coordinated at EC3. The operation was coordinated in 38 airports in 16 European countries. During the operation more than 200 suspicious transactions were reported by the industry and 43 individuals were arrested (followed by another 74 arrests after the action day; 117 arrests in total). These were all found to be linked to other criminal activities, such as the distribution of credit card data via the internet, intrusions into financial institutions' databases, other suspicious transactions, drug trafficking, human smuggling, counterfeit documents including IDs, and other types of fraud. Some of those detained were already wanted by judicial authorities under European Arrest Warrants.
Focal Point Terminal also has several operations running in the areas of retail payments, skimming and online card fraud.

Strategic analysis

EC3 has produced several analytical products. These include an analysis on the *darknet and deep web*; on *bitcoins* and on the *digital underground economy* (Crime-as-a-Service; virtual payment systems). Furthermore, each of the focal points referred to under paragraph 4.2 have produced several knowledge products for the Member States' competent authorities to better understand crime in the respective areas and to fight it more effectively. Among these are the *ransomware report and action plan*; the *strategic assessment on commercial exploitation of children online* and the *situation report on payment card fraud in the EU*.

Also worth mentioning is the publication of the white paper on future threats as part of the launch of Project 2020, a joint initiative of EC3, the International Cyber Security Protection Alliance (ICSPA) and Trend Micro. The highlight of this joint endeavour was the presentation of the Project 2020 movie in September 2013.

Last but not least, input on cybercrime was provided to the 2013 EU Serious and Organised Crime Threat Assessment (SOCTA) and to the meetings held in the framework of the EU Policy Cycle.

Outreach and Communication

In order to connect with the multitude of actors and stakeholders involved in the fight against cybercrime, EC3 has delivered a large number of presentations and hosted many visits. In addition, a large number of external conferences and meetings were attended to present the existence and work of EC3. The establishment of EC3 has in general been very much welcomed and partners are willing to cooperate with and through the Centre.

EC3 actively participates in several fora that represent specific stakeholder groups. Examples are the EU Cybercrime Task Force (EUCTF); the Virtual Global Taskforce (VGT); the European Financial Coalition (EFC) and the European Cybercrime Training & Education Group (ECTEG).

In addition, Europol works closely with other EU agencies. With the European Police College (CEPOL), an alignment was made for structured cooperation; with the European Union's Judicial Cooperation Unit (Eurojust) working arrangements were agreed, including for the involvement of their liaison officer, and with the European Network and Information Security Agency (ENISA) the annual joint conference was organised, focussing on improving cooperation between computer emergency response teams (CERTs) and law enforcement.

The first joint Europol-Interpol Cybercrime Conference was held in The Hague. It was attended by more than 260 representatives from law enforcement and the private sector from 42 countries, and had over 50 speakers. This will become a joint annual conference, next hosted in October 2014 by Interpol at its new Interpol Global Complex for Innovation (IGCI) in Singapore.
To foster communication between the many partners, EC3 has successfully launched its Secure Platform for Accredited Cybercrime Experts (SPACE), with already almost 700 end-users and over a dozen sub-communities. It is one of the largest and most active communication platforms of the Europol Platform for Experts (EPE).

Training and capacity building

In each of the previously mentioned crime areas EC3 has delivered dedicated training to share their expertise with the law enforcement community:

- May 2013 – Wiesbaden (DE). Forensic Expert Training on Examination of Skimming Devices (in close cooperation with the German BKA)
- October 2013 – Selm (DE). Training Course on investigating online child sexual exploitation
- November 2013 – Avila (ES). Introductory Open Source IT Forensics and Network Investigations course (leveraging inter alia ECTEG training material)

In addition, EC3 has contributed to several training events of CEPOL and the European Law Academy (ERA).

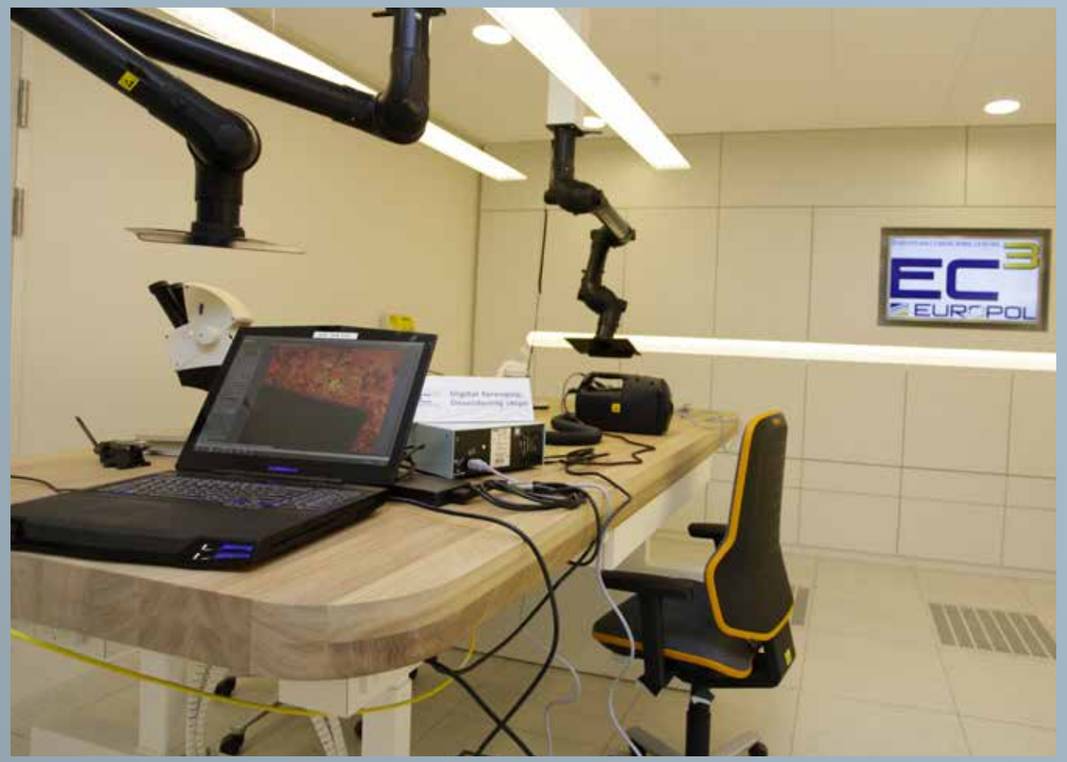
Together with ECTEG, EC3 supports capacity building in Member States and beyond by facilitating the distribution of ECTEG's training packages. For the further development of training material EC3 has come to a structural arrangement with CEPOL and ECTEG on the specification of needs and the prioritising and coordination of additional packages.

Operational support capabilities (IT forensics and tools)

Operational support to law enforcement operations and investigations has been built up gradually during the year. A milestone, extending the support capabilities in this area, was the creation of the digital forensic lab.

Furthermore, an in-depth assessment has been made of opportunities for Research & Development. This has led to a list of prioritised concepts for capacity building in the area of digital forensics.
In practical terms, the digital forensics team has supported the technical preparation and facilitation of several large scale international investigations, by providing state-of-the-art technical facilities for 24/7 covert operations with secure connections and advanced processing systems.

In addition, dozens of operational requests for technical assistance in forensic data analysis were supported in full compliance with the high standards applicable to such data processing.



Staff and financial resources

In the months preceding the launch of EC3, there was an enduring uncertainty about resource allocation to EC3. As a consequence, the preparations in terms of recruitment, housing and allocation of tasks and responsibilities had to be adjusted regularly. In the end, it was decided that in view of the financial crisis, neither staff nor finance were to be added to the overall Europol budget in 2013 for the creation of EC3. Evidently, the challenge of delivering on all accounts in the first year of existence became all the more demanding.

Since Europol's engagement in establishing EC3 was very strong, it was internally decided to shift resources from other parts of the organisation. This of course had a significant impact on the operational capacity of the affected business areas. This applies in particular to other parts of the Operations Department. But also in terms of ICT the specific needs of the Cybercrime Centre drew away resources that were initially planned for the delivery of other tools. Equally, general corporate services such as legal, finance, HR, procurement and communication faced a steep increase of their workload to support the establishment of EC3. Thanks to the very hard work of the staff involved, the needs of EC3 could be accommodated successfully.

Thanks to the sacrifices made in other parts of the organisation the staffing level of EC3 could be raised to 44. Corrected for temporal vacancies, on average around 40 staff were working in EC3 during 2013. This number was increased by about 10 full-time equivalents (FTEs) who were part of the implementation team that supported the establishment of the Centre with activities throughout the year.

The outlook for the future in this regard is modestly more promising. The Conciliation Committee of the Council and the European Parliament has voted for an increase of the Europol budget by €1.7 million for 2014, from which EC3 should also benefit. With this budget increase two temporary agents and five contract agents can be recruited. Furthermore, as from 2015 a budget increase is envisaged to strengthen the IT capabilities of Europol, including those in support of fighting cybercrime[7]. Although in financial terms this is very welcome, the question remains whether - in terms of staffing - EC3 will be able to cope with the steep increase of its workload.

---

7 A horizontal assessment of the necessary resources for decentralised agencies over the period has been performed recently and resulted in Communication COM(2013)519. This Communication states that, over the period 2014-2018, Europol may receive 15 additional posts, as well as the corresponding appropriations. Combined with the 5 % staff reduction and the annual levy for the redeployment pool, this results in a total number of posts which decreases from 457 in 2013 to 427 in 2020. Finally, the EU contribution to the agency is intended to be increased in 2015 to further develop the IT tools necessary to carry out its extended mandate, both for data collection and treatment, and for cybercrime related ICT tools. The net effect of this increase is yet to be determined.

Programme Board

In terms of organisational structure EC3 is, in all respects, fully embedded within Europol. Since the Centre is expected to operate in a complex, multi-actor environment to perform its tasks, a Programme Board has been established.

In this board the key actors in the area of cybercrime and cyber security are represented. This includes the European Commission (DG HOME and DG CNECT), European External Action Service (EEAS), Eurojust, ENISA, CERT-EU, CEPOL, Interpol, EUCTF, ECTEG and the EMPACT[8] drivers from the three cybercrime sub-priorities for 2014-2017.

The objective of the EC3 Programme Board is to provide strategic guidance and to ensure optimal complementarity and alignment of the activities of EC3 and the other represented partner organisations. In total, four meetings of the EC3 Programme Board were held in 2013.

As EC3 also strongly depends on close cooperation with the private sector, two specific advisory groups have been created to provide advice to the Programme Board: one on Internet Security and the other on Financial Services. Each group had an initial meeting in 2013, and the establishment of more advisory groups is being considered.

8 European Multidisciplinary Platform against Criminal Threats.

Future Orientation

Cybercrime characteristics

To position the future development of EC3 properly it is important to understand the criminal phenomenon of cybercrime. In essence, there are four fundamental characteristics of cybercrime to be considered: the *borderless nature*, the *scalability*, the *ease to hide* and the *nature of criminal cooperation*.

- The *borderless nature* makes it possible for anyone to commit crimes against governments, businesses and citizens in the EU from almost anywhere around the globe. Compared to other, more traditional, crime types, criminals using the internet for hacking computers, stealing data and emptying bank accounts are not hindered by logistical constraints, such as travelling and transporting the looted goods. There is hardly any identifiable link between the criminal and the crime scene.
  It is important to note that access to the internet is expected to increase significantly in the coming years. Currently, around 2.5 billion people worldwide have access to the internet. Estimates suggest that around another 1.5 billion people will gain access in the next four years[9]. Especially in Southeast Asia, South America and Africa the number of users are expected to grow fast. Since these are regions with which limited judicial cooperation exists, the EU law enforcement response against perpetrators from those territories will face an increased level of complexity and constraints.

- The *scalability* results from the ease to replicate crimes on a massive scale due to the standardisation of software and the possibility to reach millions of computers without any logistical constraints.
  This enables criminals to create and operate botnets controlling tens of thousands of computers and launch massive attacks against governments, financial institutions and other critical infrastructure. They can launch these attacks for their own criminal intentions or commercially exploit them by servicing other criminal groups. In particular organised crime groups in Eastern Europe (Belarus, Ukraine, Moldova and Russia) have a strong position in running botnets.
  Also, the global economy has led to massive vulnerabilities in terms of data security. Major retail corporations hold masses of payment credentials of their customers. Successful data breaches allow proficient hackers to steal such credentials by the millions. In December 2013, the hack at Target, the third-largest US retailer, amounted to the theft of personal data of over 100 million customers, including payment card details and PIN numbers. Those details were subsequently offered on the internet for around USD 100 per card.
  Internet connectivity and dependency are increasing rapidly. In 2012, around 8.7 billion devices were connected to the internet according to Cisco. It expects that this number will increase to 50 billion by 2020. Analysts from Morgan Stanley expect this figure to go to 75 billion by that year[10]. Developments over time have shown that every two years computing power doubles[11], bandwidth triples and storage space quadruples. These are top-down drivers accelerating the use of the internet and the delivery of low-cost cloud computing services.
  Also governments process personal data of citizens on a massive scale and consequently can be considered as interesting targets for malevolent hackers and criminal groups.

---

9 http://www.internetworldstats.com

10 http://www.businessinsider.com/75-billion-devices-will-be-connected-to-the-internet-by-2020-2013-10
http://share.cisco.com/internet-of-things.html

11 The exponential growth of computing power doubling every two years is also known as Moore's law, after the Intel co-founder G.E. Moore who identified this development already back in 1965.

- The *ease to hide* comes from techniques to re-route traffic through numerous nodes while obfuscating the origin, as well as the use of hacked computers and stolen identities. In addition, operating from or via countries in which the regime has limited competence or ambition to prevent and fight cybercrime, is an effective means to hide.
  The anonymity of internet communication is frequently misused for child sexual exploitation. Child abuse material is offered and exchanged via anonymous networks like Tor (The Onion Router) and I2P (Invisible Internet Project), but also through peer-to-peer networks like Freenet and peer groups on social media. The intensive use of encrypted files and messages further complicates law enforcement intervention. An increasing trend of offering on-demand child abuse through live streaming leaves police services without any trace or evidence at all, unless intercepted at the time of transmission.
  The possibilities for online anonymous communication are used for many other types of crime as well. The trade in illegal goods and services benefits from the existence of hidden trading places on the deep web (password shielded environments) and the darknet (Tor, I2P). Well-known examples are Silk Road, Silk Road 2.0 and Black Market Reloaded. Also, inadequate registration of domain owners is exploited by criminals, for instance for fake websites used for phishing or the selling of counterfeit products.
  Furthermore, hidden internet communication services are used by terrorists and groups of violent extremists to promote radicalisation, for recruitment and operational coordination.
  Criminal transactions can remain as good as untraceable thanks to a range of anonymous payment systems like e-currencies (Bitcoin, Perfect Money), pre-paid debit cards and anonymous money transfers.
  Furthermore, cloud services allow cybercriminals to avoid storing any illicit material on their own computer. And also the fluidity with which data can be transferred across jurisdictions in a matter of seconds, multiple times within the hour, is a major challenge for law enforcement.

- The *nature of criminal cooperation* via the internet has resulted in networks of criminals that complement each other's criminal services. This applies in the area of cybercrime as well as other types of crime. In fact, a complete underground economy has developed, where all sorts of criminal products and services are traded including, drugs, weapons, hired killings, stolen payment credentials and child abuse. As mentioned above, it is facilitated by anonymous payment systems, such as virtual currencies and hidden market places where the criminal services are offered. Especially for cybercrime this underground economy has a multiplying effect, because any kind of cybercrime can be procured by anyone even without any technical skills or instruments: password cracking, hacking, tailor-made malware, zero day exploits, distributed denial-of-service (DDoS) infrastructure and attacks, malware testing and many more. As a consequence, the threshold for stepping into the business of cybercrime is extremely low.

Vulnerabilities and Threats

How these elements will influence the evolution of cybercrime in the near future also depends on the vulnerabilities. These exist predominantly in areas where the defence against cybercrime is sub-optimal, partially because there is a false perception of trust.
Most vulnerable are minors, especially when little or no attention has been given to making them aware of the threats. Online solicitation and 'sextortion' are persistent threats to children.
Citizens in general tend to be less security-oriented when using A) social media, and B) their mobile devices. Through social media the user can be easily deceived by the nature of the communication. It is relatively easy for criminals to introduce themselves with a fake identity. Besides, the posting of private information poses a risk in the sense that it can easily be harvested for social engineering or facilitating password cracking. In the use of mobile devices, the user values the ease of use over the limitations of a consistent and robust security regime. And of course, when using social media by means of mobile, the vulnerabilities add up.
In more general terms, the customer is confronted with the challenge that most ICT products offer only two out of the following three aspects: freedom – security – convenience. Many are tempted by the combination of freedom and convenience, leaving them as a relatively easy target for cybercrime.
For businesses and governments the referred vulnerabilities of the citizen are introduced indirectly by any BYOD[12] policy that does not anticipate the cyber threats of mobile devices. Insiders - the normal staff and consultants - are considered the biggest risk for private and public employers. In most cases such insiders are unaware of the damage they are causing. Social engineering is still high on the list of intruding successfully into corporate networks.
Other corporate vulnerabilities are associated with budget considerations concerning internet security. The use of cloud services to reduce costs is a good example of that. The security measures taken by cloud service providers are likely to differ from one to the other. The augmenting centralisation of data clearly makes them an increasingly interesting target for hackers. Also the willingness and priority of investing in internet security is an important factor. Due to higher security investments by large-scale companies, a shift of cybercrime targets is visible towards small and mid-sized enterprises, where less budget and expertise is available for proper protection. This applies in particular to the banking sector, but is also perceived in other areas.
For governments and private industry, protecting their information against compromise and theft is essential. Spying malware and activity aimed at retrieving confidential information is difficult to detect. Advanced persistent threats (APTs) can continue unnoticed for long periods of time. Unauthorised retrieval of sensitive information from governmental services and intellectual property from companies can cause huge damage.
Based on these vulnerabilities and on-going cybercrime trends it is expected that the major cybercrime threats from organised crime and criminal networks will be the following:

- An increased demand for and use of cybercrime services, resulting in an even stronger growth of the development, testing and distribution of malware; building and deployment of botnets; theft and trade in payment credentials as well as money laundering services. The increased demand will be fuelled by the extended possibilities for internet access in Southeast Asia, Africa and South America. Those areas will also be more victimised due to less developed protection measures and a lower awareness of newly acceding internet users.

---

12 BYOD stands for bring your own device. Employees are allowed to use their own mobile device at work for corporate purposes.

- A further sophistication of methods of phishing, social engineering and other ways of obtaining relevant information for intrusion, committing fraud and malware distribution. But also innovative, new ways of malware distribution are expected. For instance, the embedding of malware in the official firmware of software and hardware manufacturers is likely to increase as a successful approach to circumvent detection mechanisms.

- The development of more aggressive and resistant types of malware. This applies to forms of ransomware malware with already advancing levels of encryption complexity, but also to more resilient structures of botnets, such as peer-to-peer based connections. Banking malware and trojans will equally continue to advance in terms of sophistication and effectiveness, especially to circumvent protection measures by bigger financial institutions.

- A shift of malware development towards the operation on, and distribution through, mobile devices, including the use of such devices as bots in DDoS infrastructures. This development is expected to affect both citizens and the institutions they work for, especially if BYOD policies are inadequately addressing security aspects. In particular through Android applications malware deployment through mobile communication tools could in the mid-term also have a knock-on effect on a multitude of interconnected devices (the Internet of Things).

- Criminals will continue to seek easy ways of cashing and laundering their profits. Targeting large numbers of citizens and small to mid-sized companies for relatively small amounts is a scenario likely to continue. But also misusing payment credentials for online purchases will grow, especially for products with a short delivery time. The demand for e-currencies and the use of other anonymous payment systems will rise further.

- The further technical evolution of Tor and other anonymous networks, as well as the application of enhanced encryption techniques and the use of cloud services, will help criminals to better protect themselves against detection, investigation and prosecution. This will facilitate nearly untraceable online trade in illegal services, exchange of child abuse material and laundering of criminal profits.

- The hacking of cloud services becomes more and more interesting for criminals. Reduced costs for storage as well as the configuration of many software applications push private and corporate customers towards the use of these services that are, in terms of security, out of their control. It is expected that criminals will increasingly aim at hacking cloud services for the purpose of spying, retrieval of credentials and extortion.

Future Focus of EC3

Considering the four characteristics of cybercrime and the derived threats, EC3 foresees the need to focus its efforts on:

- Assisting Member States and cooperation partners, predominantly in the framework of EMPACT, in fighting especially the facilitating factors of the digital underground economy (to address the nature of criminal cooperation):
  - the infrastructure, including market places
  - criminal services that enhance cybercrime
  - the anonymous payment systems
  - the main criminal networks that operate (in) the underground economy

- Pooling all relevant information and intelligence to enable the identification and prioritisation of top targets and threats for (joint) investigations (to address the nature of criminal cooperation)

- Intervening as soon as possible against new crime developments and sharing information on the emerging threat expeditiously with relevant partners to enable timely protection and combating (to reduce the scalability)

- Investing in R&D to develop high-tech tools to enhance the traceability of criminals and the lawful provision of digital forensic evidence (to make it more difficult to hide)

- Structuring, standardising and promoting comprehensive training and capacity building of competent authorities of the Member States as well as those outside the EU (to address the borderless nature);
- Extending the inclusive partnership to all relevant actors in a concerted manner to enable all to contribute their share to the prevention of and fight against cybercrime (all aspects).

Conclusions

The call upon EC3 support for large scale cross-border investigative action has increased significantly in the course of 2013. This shows that Member States and cooperation partners clearly see the benefit of joining forces internationally and seizing the opportunity of the capabilities that EC3 offers in this respect. Investigations that without EC3 might predominantly stay at a domestic level, with limited cooperation with other countries, are made truly international by bringing the expertise, technical facilities, intelligence and partners physically together. As such, the effect of operations – the impact on cybercrime – is being leveraged to a maximum with current resources.

The investigation and prosecution of cyber criminals is the key element of the EU law enforcement response. The mere takedown of botnets and online criminal trading places only results in a shift to other infrastructure and domains. The criminals behind it must be caught and convicted.
In its other tasks, such as training and capacity building, strategic analysis and digital forensic support, EC3 has in its first year delivered important products and services that matter to EU law enforcement.

In 2013, EC3 saw the initiation of important partnerships - not only with law enforcement authorities involved in combating cybercrime, but also with CERTs (Computer Emergency Response Teams), important internet and financial services companies, anti-malware industry, software manufacturers and universities. In addition, cooperation with the European Commission and agencies like CEPOL, ENISA and CERT-EU have taken off very well. Eurojust posted a cyber-liaison officer to EC3 and Interpol is preparing for that too. From all sides the cooperation with and through EC3 has been actively supported.

However, due to successes thus far, the current human and financial resources are already starting to constrain the progress of investigations. At the rate major investigations are coming in since the summer of 2013, EC3 will simply not be in a position to keep up. Increased resources, efficiencies, innovative approaches to cooperation, as well as capacity building among the broad range of partners, all need to be considered to maximise the impact on cybercrime and the criminals that benefit from it.