Europol’s European Cybercrime Centre
The EC3 Bulletin

01 A word from Wil van Gemert
02 A word from Steven Wilson
03 EC3 Operations
04 EC3 Meetings
05 What’s new?
06 Within EC3

Issue 7
October 2015 - February 2016

Europol Unclassified - Basic Protection Level
I would like to conclude by drawing your attention to the latest VGT Child Sexual Exploitation Environmental Scan. This very important report identifies the methods used by offenders to solicit their victims and avoid detection when sharing abuse material online, as well as the challenges faced by law enforcement when combating these crimes.

All this and much more - enjoy the reading!

Wil van Gemert
Deputy Director of Operations

A word from the Head of EC3
STEVEN WILSON

Several weeks have passed in a flash since I have joined Europol. My very first impressions of a positive workplace with highly committed staff undertaking some fantastic work have only been reinforced through personal contact with them. It has been a steep learning curve for me, trying to understand the complexities of the organisation, extensive partnerships, European regulations and the individual requirements of the EU Member States. I am however aware that these challenges are small compared to theirs - understanding my Scottish accent!

I hope to take another few months to fully assess where we are and where we need to go, but I am already seeing some key areas for EC3 as we move forward, and I trust we can report on progress in future editions of this bulletin:

• The delivery of educational material for children to make them aware of online threats, including sexual extortion, is a significant project that can save children’s lives if delivered effectively. Having seen first-hand the effect of such criminal activity on children in Scotland, I will be a strong supporter of anything that helps make children across Europe safer.

• The strong level of partnership that EC3 has with relevant stakeholders in relation to significant cyber threats is impressive. I have learned more in a few hours of discussing this topic with staff than I had previously done in months, proving that the level of expertise within EC3 is extremely high.

• I have met with a representative of CERT EU and I see the possibility to work together to counter the threat to Critical National Infrastructure and networks.

• The global scale of operations such as theline Action Day underlines the true effect EC3 can have on other criminal areas, not just cybercrime. These will continue in 2016.

As we move forward I would start by looking both within Europol and outside of it. I will ensure the continuation of EC3’s role in assisting all other Europol departments to maximise the significant benefits that cyber can bring to all enquiries. Externally, I will seek to enhance the positive relationship already in place between law enforcement, the private sector and academia in the fight against cybercrime.

I look forward to meeting all of our stakeholders in person and, in the meantime, I hope to keep all partners informed about our operations and activities in the coming months through materials such as this bulletin.
In October 2015, a joint operation led by the Romanian Police (Brigada de Combatere a Criminalitatii Organizate Craiova) and supported by Europol’s European Cybercrime Centre (EC3) and the Italian State Police (Servizio di Polizia Postale e delle Comunicazioni) targeted criminal services misusing illegally obtained credit card credentials and advertising the sale of fake plane tickets on the Internet.

As a result of Operation Travel, fifty individuals, including four leaders of the organised crime group, were arrested in the southern part of Romania. Sixteen house searches were executed, and a significant amount of digital evidence, computers, mobile phones, SIM cards, memory cards and documents were seized for further analysis.

Modus Operandi

Active since 2013, the apprehended criminal organisation illegally obtained payment card information and other personal data from victims worldwide, and subsequently used this data to acquire high-value goods and services including, most frequently, plane tickets, but also sports bets, electronic devices, jewellery, agricultural machinery and real estate. The proceeds from the online fraud were also used to facilitate other crimes on national and international levels.

Internet-facilitated credit card fraud has resulted in substantial financial losses for the airline and payment sectors, and has been proven to facilitate other forms of serious crime by providing means of transport and funds for organised crime groups.

Outcome:

- 50 individuals arrested, including 4 leaders
- 16 house searches
- Computers, phones, memory cards and other digital evidence seized

Following the implementation of EMV chip card technology (often referred to as ‘Chip and PIN’) in the EU, card-present fraud has reduced significantly in Europe. The reason behind this is that cardholders’ confidential data is more secure on a chip-embedded payment card than on a magnetic strip card. However, this type of fraud has migrated to those countries where EMV technology is not yet fully implemented. Therefore, the level of illegal transactions overseas has sharply increased, as cards cloned in Europe are being used to withdraw money in non-EU countries.

In order to tackle this issue and to improve cooperation among the actors involved, several meetings were organised to discuss payment card fraud overseas and money withdrawals.

The aim of both events, supported by the ATM Security Team (EAST), was to increase awareness among experts about card skimming and overseas money withdrawals, modus operandi and best practices, and to identify new logical attacks and ATM and point-of-sales terminal malware.

**EC3 Operations**

**Travel**

Europol’s EC3 assisted this operation by:

- providing analytical support;
- facilitating exchange of information and evidence between the involved countries;
- assisting with the final on-the-spot operation in Romania.

**Outcome:**

- 50 individuals arrested, including 4 leaders
- 16 house searches
- Computers, phones, memory cards and other digital evidence seized

**EC3 Operations**

**Fighting payment fraud overseas**

Following the implementation of EMV chip card technology (often referred to as ‘Chip and PIN’) in the EU, card-present fraud has reduced significantly in Europe. The reason behind this is that cardholders’ confidential data is more secure on a chip-embedded payment card than on a magnetic strip card. However, this type of fraud has migrated to those countries where EMV technology is not yet fully implemented. Therefore, the level of illegal transactions overseas has sharply increased, as cards cloned in Europe are being used to withdraw money in non-EU countries.

In order to tackle this issue and to improve cooperation among the actors involved, several meetings were organised to discuss payment card fraud overseas and money withdrawals. The most recent took place in the following regions:

- **Latin America:** 28 and 29 October / 26 experts from EU Member States (Spain, Portugal and Romania), the United States and Latin America (Colombia, Brazil, Dominican Republic, Mexico and Chile).

The fraud resulted in substantial losses for the airline and payment sector.

A criminal organisation illegally obtained payment card information and other personal data from victims worldwide.

The stolen data was used to acquire high-value goods and services, including plane tickets, sports bets, electronic devices, jewellery, agricultural machinery and real estate.

A joint operation led by the Romanian Police targeted the organised crime group in the southern part of Romania.

The aim of both events, supported by the ATM Security Team (EAST), was to increase awareness among experts about card skimming and overseas money withdrawals, modus operandi and best practices, and to identify new logical attacks and ATM and point-of-sales terminal malware.
Project Skynet was launched in January 2015 for a period of two years. Set up by the United Kingdom’s Dedicated Cheque and Plastic Crime Unit (DCPCU), it is a European Commission funded initiative to improve the response to e-crime in the payments sector. Europol’s European Cybercrime Centre has supported the project since its launch, with commitments also from law enforcement agencies in Belgium, Finland, France, Hungary, Romania, and the Netherlands. The focus is on the ever-increasing cyber threat to the UK payments industry in the context of remote payments, which in 2013 accounted for 66% of fraud losses on cards in the UK.

As part of this operational phase, Skynet is currently working on a number of investigations with the aim to arrest and prosecute organised criminal networks who continue to be involved in these activities. This involves close collaboration with other EU law enforcement agencies, the private sector, payment providers and Focal Point Terminal. Additional operational activities are planned throughout 2016.

Project Skynet was launched in January 2015 for a period of two years. Set up by the United Kingdom’s Dedicated Cheque and Plastic Crime Unit (DCPCU), it is a European Commission funded initiative to improve the response to e-crime in the payments sector. Europol’s European Cybercrime Centre has supported the project since its launch, with commitments also from law enforcement agencies in Belgium, Finland, France, Hungary, Romania, and the Netherlands. The focus is on the ever-increasing cyber threat to the UK payments industry in the context of remote payments, which in 2013 accounted for 66% of fraud losses on cards in the UK.

As part of this operational phase, Skynet is currently working on a number of investigations with the aim to arrest and prosecute organised criminal networks who continue to be involved in these activities. This involves close collaboration with other EU law enforcement agencies, the private sector, payment providers and Focal Point Terminal. Additional operational activities are planned throughout 2016.

The Project Skynet Academic Study, or any further information on this project can be requested by contacting Skynet at skynet@dcpcu.pnn.police.uk

The Project Skynet Academic Study, or any further information on this project can be requested by contacting Skynet at skynet@dcpcu.pnn.police.uk

The criminal group, composed of Romanian and Moldovan nationals, was involved in large scale ATM ‘Jackpotting’, causing substantial losses across Europe to the ATM industry. ATM ‘Jackpotting’ refers to the use of a Trojan horse, physically launched via an executable file in order to target an ATM, thus allowing the attackers to manipulate the ATM cash cassettes via direct manipulation, using the ATM PIN pad to submit commands to the Trojan.

Guidance and recommendations regarding logical attacks on ATMs

EC3 recognises the severity of the threat presented by ATM logical and malware attacks and has prepared security guidelines regarding this new cyber threat to ATMs. The production of this document has been coordinated by EAST (European ATM Security Team) and is the first of its kind.

The guidance and recommendations regarding logical attacks on ATMs, which also covers malware attacks, is an excellent example of a coordinated central response from both law enforcement and the industry to fighting ATM malware threats in an effort to respond much more quickly and effectively.

The document is available in English, German and Italian.
On 3 and 4 November 2015 law enforcement agencies from across the world, supported by Europol’s European Cybercrime Centre (EC3), joined forces with the airline, travel and payment card industries in a major concerted operation to combat online fraud in the airline sector.

Participation

Some 35 airlines and 32 countries were involved in this initiative, which took place at 109 airports across the world. The coordinated Global Airline Action Day targeted criminals suspected of fraudulently purchasing plane tickets online using stolen or fake credit card data. Rapid increases in this Internet-facilitated crime have left millions of innocent people affected every year whilst the banking, airline and travel industries have suffered huge financial losses as a direct result.

Crime facilitator

In many cases it was revealed how credit card fraud is linked to other forms of serious crime such as drugs trafficking and human trafficking. The increasing role of fake online ‘travel agencies’ as a facilitating factor (crime-as-a-service) was also reported.

Behind the scenes

Representatives from airlines, online travel agencies and major payment card companies worked at Europol’s operational centre with experts from EC3 and law enforcement officers from across the EU, Latin America, US and Canada to identify suspicious airline ticket transactions resulting from the use of fake or stolen credit cards via the Internet.

On receipt of alerts from airlines, credit card company representatives confirmed suspicions using their own financial data systems, and the International Air Transport Association (IATA) provided fraud intelligence from its databases. Notifications were sent to transport hubs across the world as waiting law enforcement officers intercepted and detained criminals attempting to travel using fraudulently obtained flight tickets. Further support was received on the day from Frontex and Europol. Playing a pivotal role in the operation, Europol deployed specialists and equipment to locations across Europe and to the Command Post in Bogota.

In addition, a dedicated team of analysts working from the Europol operational centre provided live access to centralised criminal intelligence databases, whilst INTERPOL assisted with information from its databases.

The operation was organised globally through coordination centres at Europol in The Hague, AMERIPOL in Bogota (National Police of Colombia – Cybercrime Centre Police and Federal Police of Mexico) and Canada. During the operation more than 162 suspicious transactions were reported and 133 individuals were arrested.

In many cases it was revealed how credit card fraud is linked to other forms of serious crime such as drug trafficking and human trafficking.'
DROIDJACK allows cybercriminals to:

Modus Operandi - DROIDJACK

DroidJack is a mobile phone malware that allows cybercriminals to take control of Android smartphones without their owners’ knowledge. Once infected, cybercriminals may perform activities such as monitoring a smartphone’s data traffic, eavesdropping on phone conversations or hijacking a phone’s camera.

Modus Operandi - DRIDEX

Dridex is a multifunctional malware package that most frequently infects users running Windows operating systems. It is generally distributed through phishing email messages that contain malicious Microsoft Word attachments. Once users receive and open documents in seemingly legitimate emails, computers become infected.

R2D2

Bluebonnet

Europol’s EC3, in collaboration with the UK’s National Crime Agency (NCA) and the US Federal Bureau of Investigation (FBI), joined efforts to bring down Dridex - a peer-to-peer (P2P) bank credential-stealing malware - which has inflicted an estimated GBP 20 million in losses in the UK alone.

To stop the network of infected computers from communicating with the criminals, the NCA and the FBI had been sinking the malware, which rendered a large portion of the botnet harmless. This part was of a sustained campaign supported by EC3 and the Joint Cybercrime Action Taskforce (J-CAT), alongside a number of international law enforcement agencies and key private partners, targeting multiple versions of Dridex and the cybercriminals behind it who operate in hard-to-reach parts of the world.

Dridex, considered the successor of Cridex banking malware, first appeared in November 2014. It has been developed by technically skilled cyber criminals in Eastern Europe to harvest online banking credentials, which are then exploited to steal money from individuals and businesses worldwide. Global financial institutions and a variety of different payment systems have been particularly targeted by this malware.

DD4BC

On 27 October 2015, in an investigation initiated by Germany and supported by Europol’s EC3 and Europol, law enforcement officials from Germany, France, United Kingdom, Belgium, Switzerland and the United States carried out a number of house searches and arrests of suspected users of the mobile phone malware DroidJack. Europol contributed to the investigation by providing analytical support and by facilitating information exchange in the framework of the J-CAT.

The operation was conducted as part of a global law enforcement response against the criminal organisation. Key members of the organised network were identified in Bosnia and Herzegovina by the UK Metropolitan Police Cyber Crime Unit (MPCCU). The action resulted in two arrests: a main target and a suspect. Multiple property searches were carried out and an extensive amount of evidence was seized.

The operational activity, initiated by Austria, was supported by EC3 and the J-CAT. Police authorities from Australia, France, Japan, Romania, the USA, Switzerland and INTERPOL supported the coordinated activities. Operational meetings were organised in The Hague to discuss and plan coordinated law enforcement actions against DD4BC. On the action days, Europol deployed a mobile office, allowing direct access to Europol’s forensic tools and its databases for cross-checking, analysing and exchanging intelligence in real time.
In December 2015, Europol’s EC3 and a number of law enforcement and judicial authorities across Europe carried out a two-week long coordinated action against the use of Remote Access Trojans (RATs). Operation Falling sTAR resulted in multiple house searches and the arrest of 12 individuals in France, Norway and Romania.

EC3 supported the countries in their efforts to identify EU citizens, mainly young adults suspected of misusing RATs to commit various types of cybercrime. Europol hosted a number of operational coordination meetings, collated intelligence and provided analytical and other operational support to nine European countries. The participating countries worked together in the framework of the EMPACT project targeting cyber-attacks that affect critical infrastructure and information systems in the EU.

During the operation a large number of computers and internet accounts were seized. This joint international effort follows previous successful actions against the threat posed by this type of malware (Operation Mousetrap).

1 EMPACT (European Multidisciplinary Platform against Criminal Threats) is the EU’s multi-annual policy cycle.

In Colombia, approximately 650 people attended the workshops and organised online rather than physical pop-up shops. These pop-up events were part of Operation Blackfin, a global cyber-awareness mining campaign led by the UK National Crime Agency, targeting the four pillars of their national cyber security strategy: Pursue, Prevent, Protect and Prepare.

EC3 Operations
Falling sTAR

EC3 Operations
Project VIC

Europol’s EC3 hosted the first international Project VIC meeting on 14 and 15 September 2015. Participants included representatives from law enforcement, the private sector and non-governmental organisations (NGOs). Their discussions on various topics strengthened the Project VIC initiative by contributing new ideas, supporting current initiatives and fostering international cooperation among practitioners involved in fighting child sexual exploitation.

Project VIC is a framework promoting a victim-centric approach to investigations in the area of child sexual exploitation. The project is coordinated by the International Centre for Missing and Exploited Children (ICMEC) in collaboration with global law enforcement, child protection NGOs and the computer forensic industry.

The purpose of Project VIC is to create an ecosystem of information and data sharing between domestic and international law enforcement agencies that are working on crimes against children and the sexual exploitation of children. Its aim is to reduce the workload for forensic investigators, supporting them in identifying the victims of child sexual exploitation.

EC3 recognises the importance of these efforts and has contributed on this occasion by providing a venue for this first international meeting.

Although Project VIC is well known for its robust image hash values, they also offer domestic and international training through partnerships with the National Criminal Justice Training Center (NCJTC) and ICMEC.

RATs are different from legitimate remote administration tools that are often used in corporate environments to assist computer users or install software remotely, with the consent and knowledge of the users.

A number of cyber safety pop-up events, supported by Europol’s European Cybercrime Centre (EC3), were held in Europe and beyond. The coordination of the various activities programmed was facilitated via the J-CAT members of the participating countries: Australia, Colombia, France, Germany, Italy, the Netherlands, Spain, UK and USA.

The initiative aimed to educate the public about understanding and dealing with some of the current online threats. Law enforcement and private sector partners were on hand to offer advice to the general public at locations ranging from cities in the UK, to Madrid’s Atocha train station, central Bogota and two of Italy’s busiest airports. They offered on-the-spot support to members of the public on how to best protect their phones and computers from criminals seeking financial and personal details.

In most cases, the pop-up sessions commenced on 9 November and lasted for one week. One of the exceptions was Australia, which conducted the event in October and organised online rather than physical pop-up shops.

A total of 2500 people attended the campaign events in the UK. In Colombia, approximately 650 people attended the workshops and 85 infected PCs were discovered.

These pop-up events were part of Operation Blackfin, a global cyber-awareness mining campaign led by the UK National Crime Agency, targeting the four pillars of their national cyber security strategy: Pursue, Prevent, Protect and Prepare.
The second cybercrime prevention and awareness forum was held at Europol headquarters in The Hague on 28 and 29 September 2015, with the participation of 17 Member States, INTERPOL, the European Commission and Europol’s EC3 representatives.

The network convened with the main objectives of defining common interests and identifying concrete initiatives for joint prevent and protect actions to be suggested for the Cybercrime Operational Action Plans 2016 within the framework of the EMPACT Policy Cycle.

Participants had the opportunity to assess recent and ongoing cooperation, with updates on some of the latest developments delivered by the UK (Operation Blackfin) and Greece. The group also included non-law enforcement participants from Kaspersky, presenting the No Ransom project, the Anti-Phishing Working Group (APWG), introducing the global campaign Stop.Think.Connect, and the European Commission, who shared the internal awareness raising campaign on cybersecurity and cybercrime risks. From EC3’s side, the prevention findings of the Internet Organised Crime Threat Assessment (IOCTA) 2015 were presented and discussed.

The attention of the Cybercrime Prevention Network stretches across high-tech crimes, child sexual exploitation online and payment fraud, all sub-areas defined under the current EMPACT Cybercrime priority.

The group was established in 2014, and met for the first time on 9 and 10 December 2014, with the aim of bringing together the network of cyber prevention contacts to discuss matters of common interest in this area, to introduce the EU Communication Strategy on Cybercrime Prevention and Awareness 2014 – 2017, and to agree on the line of work and cooperation for the coming years.

In 2016, the Forum is scheduled for 15 and 16 September, also at Europol’s headquarters.

Cybercrime Prevention projects 2015

One of the European Crime Prevention Network’s (EUCPN) main tasks is to organise an annual conference for sharing and disseminating experience, knowledge and best practices in preventing crime and increasing safety and security in the EU Member States.

The European Crime Prevention Award (ECPA) is a contest which rewards the best European crime prevention project. The nominated projects are presented each year during the Best Practice Conference.

In 2015, the conference took place on 15-16 December in Luxembourg under the theme of ‘Cybercrime’. Europol’s EC3 had the opportunity to present the Centre’s activities in the area of cybercrime prevention.

The 2015 ECPA was awarded to the Dutch entry: ‘SME Cybersecure, Cybersecurity Business edition’. Second place went to the German entry: ‘Media Heroes’. Luxembourg took third place with their entry: ‘Bibi and friends’.

For further information, contact eucpn@ibz.eu
Conference conclusions:

For countries that are already willing to undertake such cooperation, the taskforce is to look into the development of a compatibility chart, which would help harmonise various legal and handling codes for information.

To set up a Joint Cyber Taskforce between INTERPOL and Europol, welcoming interested law enforcement partners from around the world to join. The taskforce aims to make the best use of existing frameworks to establish and promote conditions for operational cooperation.

To jointly develop a partnership against the abuse of virtual currencies, to be concluded with law enforcement from countries around the world. It will have concrete joint actions to fight the abuse of virtual currencies by criminals, focussed around policy matters, operational cooperation and training.

Next edition: 28 to 30 September 2016, at the INTERPOL Global Complex for Innovation, in Singapore.
Theme: Solutions for attribution.
**EC3 Meetings**

**Fourth ENISA-EC3 Workshop between CSIRTs and law enforcement agencies**

O n 8 and 9 October 2015, Europol hosted the fourth edition of the Annual Workshop to enhance cooperation between CERTs/CSIRTs (Computer Emergency/Security Incident Response Teams) and law enforcement agencies (LEAs), co-organised by ENISA (the European Union Agency for Network and Information Security) and the European Cybercrime Centre (ECS).

**Goal**

More than 40 representatives from national and governmental EU CERTs/CSIRTs and their law enforcement counterparts convened at this annual event. Its goal is to bring together the two professional communities, facilitating information sharing and coordination of efforts to tackle cybercrime.

**Common taxonomy**

The two-day event placed a particular emphasis on identifying a common taxonomy for the exchange of information regarding incidents, as well as a sharing mechanism between LEAs and CERTs/CSIRTs. Several examples of common taxonomies already in place in specific EU countries and cross-sector cooperation were presented.

The study resulted in the publication of a report on Information Sharing and Common Taxonomies between CSIRTs and Law Enforcement Agencies.

**Cooperation**

ENISA and EC3 work hand in hand to share best practices and enhance cooperation among both the EU Member States and related Network and Information Security (NIS) communities in the joint fight against cybercrime. ENISA is a member of the ECS Programme Board and EC3 representatives are part of ENISA’s Permanent Stakeholders Group.

The two Agencies have a record of successful cooperation including:

- the production of a joint paper on Botnet mitigation,
- participation in the European CyberSecurity Month and cyber exercises such as Cyber Europe,
- the production of a good practice guide for CERTs,
- the enhancement of CERT/law enforcement cooperation through different workshops and conferences.

**What’s new?**

**Steven Wilson - New Head of EC3**

Less than six hours into his new job and Steven Wilson, EC3’s new Head of Business Area, was fully settled in. He had already got to know most EC3 staff and had his agenda filled for the days to come with meeting the people he will be working with. He enjoys socialising and, while often asking his audience to tell him to slow down when his Scottish accent becomes overwhelming, is an excellent communicator.

Born and raised in Ayrshire on the West coast of Scotland, Steven has worked in and around Glasgow most of his life. With the recent amalgamation of the eight Scottish police forces into a national force, he has spent the past three years overseeing eight separate business areas for all of Scotland. ‘I joined the police force when I was 19 years old,’ he says. ‘I have since then changed many positions and taken various specialist training courses in various areas.’ He has always been passionate about his work, driven by the same belief as Steve Jobs, that great work is only achieved when you love what you do. While trying different areas of policing, it was cybercrime that captured his interest most. ‘Cybercrime is probably the biggest threat and opportunity to modern policing,’ he said, adding that he has always been interested in understanding the technical side of it, at least enough to provide him with a clear view on how it all comes together and ways to apply this knowledge to his operational work.

Steven retired from his position within Police Scotland to take the job with EC3. ‘I have worked closely with Europol over the years and always found it to be an organisation with a positive attitude, where work is not constrained by national borders,’ Steven explained. He continued, stating that the biggest challenge he sees ahead is ensuring cooperation between law enforcement, the private sector, academia and governments. ‘I am an optimist at heart,’ he said. ‘I think the cyber world offers a huge opportunity if we get it right. If the foundation of cybersecurity is not properly built, then the EU digital strategy will struggle to achieve its potential. We all have to play our role.’

Steven is a keen golfer, with a handicap 2, and is already planning to ride his bike among the dunes of The Hague. He has already started learning Dutch and is in search of a good spot where one can watch a rugby game. Most of all, he looks forward to getting up to full speed as Head of EC3, a position from which he hopes to further consolidate the state of the European cyber security arena. He explained that the mission of those fighting cybercrime within the EU is to ensure that all generations, and particularly children from EU countries, can recognise a cyber-threat. As it has been the case throughout his career, his determination and passion for making a difference will help him lead EC3 into fulfilling its mission of fighting crime in a digital age.

Steven completed 30 years of service with Police Scotland, previously having also served with Strathclyde Police, Scottish Crime and Drug Enforcement Agency and Her Majesty’s Inspectorate of Constabulary. He has worked in a wide range of Senior Detective roles on major investigations, counter terrorism, covert policing, management of sex offenders, fugitives and witness protection. He had responsibility for all aspects of cyber and cyber enabled crime in Scotland and sat on government, private sector and academic groups. He also represented Scotland on UK national and European cyber groups.
What’s new?
Fernando Ruiz - New Head of Operations

After having worked here for seven years, Fernando Ruiz is no stranger to Europol, Europol’s European Cybercrime Centre or even this bulletin (where he was featured in 2013, following his appointment as new Team Leader of Focal Point Twins). Now, as the new Business Manager of EC3 Operations, Fernando hopes to continue fostering partnerships in the fight against cybercrime and providing the quality service that EC3 is known for.

At Europol, you went from Liaison Officer to Team Leader of FP TWINS to Head of Operations. How do you see this new challenge of having to coordinate different fields of cybercrime and a team of 40 people?

Fernando: The experience gathered in previous posts, leading operational high-tech crime teams in the Spanish National Police and coordinating information exchange in the area of cybercrime in the liaison bureau, has given me a sound understanding of how international police cooperation mechanisms work and the kind of services the EU Member States expect from Europol. Working within EC3 since its establishment has allowed me to become fully aware of the challenges we face. I have the privilege of leading the best possible teams of experts in the area of cybercrime. Given the wide spectrum of criminal activities involved, one of the key challenges is ensuring proper coordination and interaction between the four operational teams under EC3 (FP Terminal, FP Twins, FP Cyborg and Cyber Intel) and other business areas in the organisation. Technology plays a key role in all criminal fields, and we have good examples like operation Onymous, where all kinds of illegal commodities were traded through black market sites. We work to implement internal and external mechanisms to guarantee the sharing of the expertise gathered within EC3 for the benefit of the law enforcement community.

What are your aspirations in this new position and the biggest challenges in making them happen?

Fernando: Europol’s mission is defined in our recently renewed strategy: to support the Member States in preventing and combating serious organised crime and terrorism. My main challenge as Business Manager in EC3 Operations is ensuring a constant dialogue with our stakeholders to align our activities and resources properly to their needs, delivering an effective and efficient service. This dialogue has been essential since EC3’s establishment, and I’m committed to boosting it through continuous coordination of the different initiatives and agencies involved in the fight against cybercrime. We have a shared responsibility and only through proper partnerships will we be in a position to give the response EU citizens deserve. We are on the right track and we will continue working with organisations such as INTERPOL, Europol and Europol, through common projects and initiatives like EMPACT, the I-CAT or the EUCTF. Likewise, we will seek new ways of cooperation with the private sector, NGOs and academia, who also play a key role in this fight.

How is it fighting crimes that are borderless while having to consider legislation that varies from country to country?

Fernando: It’s an issue that we have always faced. Cybercrime is borderless by nature and that is where we play a key role in supporting the Member States. From an operational perspective, different legislations could be an obstacle in some cases; nevertheless, it could also offer some advantages if you have a clear idea on what can be done and where. We have coordinated operations where one participating country was limited by its legal framework; however, we were able to continue the investigation in another partner country where the legal framework was more flexible. But indeed, it is a challenge, and we need proper communication and discussions to set the right strategies at both law enforcement and prosecution levels. It is within this regard that cooperation with partners like Europol is really important. Moreover, at a strategic level, one of our roles is to raise awareness among policy-makers on these legal issues in order to facilitate their decision-making process. Legal issues and gaps are some of the topics we discuss in our regular meetings with the European Commission.

Any predictions for 2016?

Fernando: Continuous new technical developments in a society where IT communication systems are playing a bigger role every day become the perfect field for cybercriminals to exploit new attack vectors. We can only expect more demand for support and expertise from our law enforcement partners. Unfortunately, for different reasons, this increasing demand is not aligned with an increase of our resources. The dialogue with our partners as referred to above will be extremely important to properly prioritise our capacity with their needs.

How can EC3 and law enforcement keep pace with increasing technical developments, more people accessing the Internet and cybercriminals getting more creative?

Fernando: We have to be ready to provide expertise to our partners if they turn to us for advice regarding a new system or a new technical development. That is why our cooperation with the private sector and academia is so important. There are many researchers looking into how new technology works and we have to make sure we are in contact with the best, in order to address the problems we have in our investigations. Facing legal and technical issues is nothing new for law enforcement agencies; we always have and always will. The difference now is that we have the mechanisms to tackle these issues together, making the best possible use of our capabilities and expertise.

With your workload steadily increasing here are Europol, do you have any time left for personal professional development and/or hobbies?

Fernando: I try to find time for my hobbies and to practice sports. It helps me clear my mind and review my activities from a fresh point of view. Thinking 24/7 about work for long periods can make us lose perspective.
What’s new?

Cathal Delaney - New FP Twins Team Leader

One of the largest police operations in the Republic of Ireland, Operation Amethyst involved simultaneous searches of over 100 targets across the country in 2002. The operation involved house searches and the seizure of child abuse material, and was a great success. It was also Cathal Delaney’s very first incursion into fighting child abuse, as he was nominated to provide forensic support to nation-wide investigators on this case. Over a decade later, he has been appointed the new team leader of Focal Point Twins, in charge of overseeing the team responsible for supporting the EU-wide fight against child sexual exploitation.

‘Fighting child sexual exploitation is a very pure form of policing with a simple motivation, to make children safer both online and offline,’ Cathal said. Trained in computer forensics, he had not always thought that he would work in this field. With a triple degree in English, Economics and Greek and Roman Civilizations, Cathal started his working life as a bartender, journalist and teacher, but soon changed his path and took a job with An Garda Síochána, where he became a Detective within the National Bureau of Criminal Investigation. Being called to support Operation Amethyst was a turning point that led him giving technical and forensic support to the Paedophile Investigation Unit before working at the Computer Crime Investigation Unit in 2011. In the meantime, he has taken various courses in computer forensics and child sexual exploitation, including Europol’s own course on combatting Online Child Sexual Exploitation.

In 2013, Cathal took the position of Cybercrime Specialist within Focal Point Twins, working, among other tasks, on computer forensics, the Victim Identification Function and training. After less than three years, he has become the team’s leader: ‘Our work encounters similar challenges as all other areas of fighting cybercrime. It is often hindered by encryption, attribution and anonymisation,’ he said. ‘However, specific issues within online child sexual exploitation that we now face are the live streaming of child sexual abuse, as well as content-driven and economic sexual extortion of children.’

He is leading a team he knows well and has ambitious goals set for the coming year. ‘We will have two Victim Identification Taskforces this year, which has never been done before,’ he explained. ‘This is consistent with the introduction of the Victim Identification Function at Europol, strengthening the focus that Twins has on identifying the victims of abuse.’

When he is not helping EU law enforcement in combating crime, he reads about it. He enjoys crime fiction, with his favourite author being Kathy Reichs, a forensic anthropologist.

Fighting child sexual exploitation is a very pure form of policing with a simple motivation, to make children safer both online and offline.’

What’s new?

Gregory Mounier - New Outreach & Support Team Leader

A political scientist and international relations specialist by training, with a specialisation in security issues, Gregory saw Europol as the perfect match when he was asked to join the Office of the Director in 2008 to deal with policy developments and Europol’s external relations. But after eight incredibly exciting years, during which he has promoted Europol’s interests in the Brussels political arena and strengthened partnerships inside and outside EU, it was time for him to leave his position of Team Leader of the Strategic and External Affairs unit (G21). His career would continue within the European Cybercrime Centre (EC3) where he is now leading the Outreach and Support Team.

Prior to joining Europol, Gregory held various temporary and policy-related positions in the private sector, academia, EU institutions and international organisations. He therefore lived in many different countries, such as Belgium, the UK, Bosnia and Herzegovina, Moldova, the US and Germany; before settling in the Netherlands.

As Team Leader for Outreach and Support, Gregory wants to contribute to the consolidation of EC3’s foundations and to ensure that the outreach efforts directly serve the needs, and reinforce the successes, of EC3’s operational teams. ‘I want to help ensure the establishment of a network of partners that can bring concrete added value to EC3’s overall output,’ he said. ‘It’s always important to raise the profile of an organisation but I believe that our achievements and successes should speak for themselves. But for that, you need good intelligence and good allies.’

Further to his role as Outreach Team Leader, Gregory will also lead Europol-EC3’s policy engagement in what he describes as his greatest challenge yet: Global Internet Governance. The Internet is the largest political and economic arena the world has ever known and there is a race to control it. I am fascinated by the political dynamics at play,’ he explained. From the current global debate on encryption, to the more technical but yet essential ‘ICANN-led discussions on the reform of the domain name system WHOIS, the Internet is profoundly disrupting power relations between governments and corporations. In that context, Gregory’s ambition is to strengthen the law enforcement voice so as to ensure that police can continue to keep citizens safe offline as well as online. He represents Europol-EC3 at the ICANN Public and Safety Working Group (PSWG).

On the personal development side, Gregory doesn’t want to stop learning. He is presently following an intensive course on Internet governance with an emphasis on cybercrime.

“The Internet is the first thing that humanity has built that humanity doesn’t understand, so we’d better keep learning.’

(Main quote by Eric Schmidt, Alphabet’s Executive Chairman)
The ‘orchestra approach’ as a successful way forward

Under the orchestra approach, there must be cooperation of international platforms and integration of a variety of experts in order to better fight cybercrime and to improve the network of existing partnerships.

Cooperation initiatives will not be unified under one unique platform, but the different stakeholders will play together, ultimately working in perfect unison.

The mission

Our mission is to fight cybercrime. Its fast progress is affected by two main drivers. The first one is the illegal business model known as ‘Cybercrime as a Service’ (CCaaS), the latest product of the cloud computing concept which is becoming increasingly significant. A whole criminal industry has been established around it, with the digital underground providing an enormous range of cybercrime products and services.

The second driver is the illegal trade on online marketplaces, comprising of drugs, weapons, stolen goods, forged IDs and materials related to child sexual exploitation. Our strategies have to address both of these drivers in order to achieve maximum effect.

The vision

The vision behind J-CAT is based on sustainable cooperation management that I call the ‘orchestra approach’. A strongly unified police network is crucial in ensuring comprehensive cooperation in fighting cybercrime. This entails the existence of a proper architecture of communication and cooperation platforms at an international level, with a linking operational purpose leading to common success. Under the orchestra approach, there must be cooperation of international platforms and integration of a variety of experts in order to better fight cybercrime and to improve the network of existing partnerships.

Operations and cyber-related projects

The steady growth in the number of our operations (as short-term activities) and cyber-related projects (with a longer term approach) against cross-cutting crime enablers like ‘Botnet activities are just a few of the latest areas that organised cybercriminal groups are currently exploring and that the J-CAT will support the fight against.

At the same time, with the arrival of the new Eurojust Seconded National Expert to EC3, we have also witnessed improved judicial coordination. In September, the J-CAT Board had the opportunity to meet with the US Attorney General to discuss our cooperation in combating cross-border cybercrime. We were delighted to hear about the decision to temporarily deploy a US cyber prosecutor to The Hague to work closely with J-CAT, EC3 and Eurojust. He has already taken up his duties and we are very happy to have him on board and draw upon his expertise.

Operational priorities

In the coming months, we will be focusing on the identified need to ensure that J-CAT’s operational priorities are derived from the current trends. ID theft, banking malware, man-in-the-middle attacks, DDoS extortion campaigns, illegal Clearnet and Darknet marketplaces, payment fraud and money mules, as well as Botnet activities are just a few of the latest areas that organised cybercriminal groups are currently exploring and that the J-CAT will support the fight against.

Carsten Meywirth started his law enforcement career in 1984. After graduating from the German Police University in Münster in 2002, he underwent different senior management assignments both in the Criminal Investigation Department and Organised Crime Division of the BKA. In 2005, he transferred to the Information Technology Division and headed the CIO-staff as chief superintendent from 2008 until 2013. In late 2013, Carsten was appointed head of the subdivision focused on cybercrime.

On behalf of Germany, I am delighted to have been nominated as the new J-CAT Chairman, as of January 2016. I am taking over a taskforce that has been exceptionally led by the UK Chairmanship ever since its inception, thus I have big shoes to fill. We will do our utmost to steer the taskforce in the right direction as we go forward and continue to achieve operational successes. As the new Chairperson, I would like to seize this opportunity to share with you some conceptual reflections.

The vision behind J-CAT is based on sustainable cooperation management that I call the ‘orchestra approach’. A strongly unified police network is crucial in ensuring comprehensive cooperation in fighting cybercrime. This entails the existence of a proper architecture of communication and cooperation platforms at an international level, with a linking operational purpose leading to common success. Under the orchestra approach, there must be cooperation of international platforms and integration of a variety of experts in order to better fight cybercrime and to improve the network of existing partnerships. 
It is fair to say that over the past few years digital forensics has developed from a niche area to a subject of rapidly growing interest and importance for law enforcement. As our lives are becoming increasingly digitised so is crime and, as a consequence, most criminal cases now have a digital component – be it a smartphone, laptop, car navigation system or games console. Moreover, with criminals abusing the Internet for both cyber-enabled and cyber-facilitated crime, digital forensics is becoming increasingly important in law enforcement investigations.

Simply put, digital forensics is about the collection and investigation of electronic evidence stored on digital devices. It is a branch of forensic science that involves a wide range of tools and techniques and requires specialised knowledge, skills and expertise.

Technological advancements, together with wider and faster adoption rates of technology, create more criminal opportunities and require law enforcement to constantly update and develop their digital forensic capabilities. It goes without saying that this requires significant resources in terms of training, education and, most importantly, tool support. While there are a variety of commercial digital forensics tools available on the market, licensing tends to be costly and can make a significant dent in already-stretched law enforcement budgets. Furthermore, some of these tools do not meet the specific needs of investigators.

The project
The FREETOOL project, which was jointly funded by the European Commission’s DG HOME and University College Dublin’s Centre for Cybersecurity & Cybercrime Investigation (UCD CCI), aimed to address law enforcement’s need for low-cost digital forensics software with a focus on investigative requirements. It was a collaborative effort between law enforcement agencies across Europe and software developers to create a range of open-source, validated software tools to assist law enforcement in the field of digital forensics and cybercrime investigations.

After running for about two years, the project delivered six tools for Live Forensics, Digital Forensics, First Responder and Artefact Analysis.

After running for about two years, the project delivered six tools for Live Forensics, Digital Forensics, First Responder and Artefact Analysis. These tools are now freely available to the global law enforcement community via EC3’s Secure Platform for Accredited Cybercrime Experts (SPACE). All tools come with user manuals, and some also have developer guides and test plans. Through its functionalities, SPACE helps in providing support for feedback and exchange between law enforcement users.

For further information about FREETOOL please contact freetool@ucd.ie. Applications (law enforcement only) to use the tools developed so far can be sent to freetool@europol.europa.eu.

The VGT Environmental Scan was released on 21 December 2015. The report was produced by Europol’s European Cybercrime Centre (EC3) and identifies the methods used by offenders to solicit their victims and avoid detection when sharing child sexual abuse material (CSAM) online, as well as challenges faced by law enforcement in combating these crimes.

Findings
- Another issue to have emerged is that online grooming and solicitation for sexual purposes, live streaming of child sexual abuse, use of encryption, peer-to-peer (P2P) and other security methods to distribute CSAM are no longer emerging trends, but established realities.
- Also, the use of The Onion Router (Tor) in the proliferation of CSAM remains a key threat, with restricted areas where it is likely that more CSAM of an extreme nature, often created on demand, is being requested and shared.

Conclusions
The concluding remarks include advice for all involved stakeholders, emphasising the need for cooperation among them and experience sharing. An international and coordinated approach for major operations together with global initiatives in specialised training, should always be taken into consideration in terms of law enforcement interventions.

The Environmental Scan has been commissioned by the Board of Management (BoM) of the Virtual Global Taskforce (VGT) and sets its strategic priorities for the next four years. The release of the public version of the VGT CSE Environmental Scan was decided during the VGT BoM meeting which took place in the United Arab Emirates (UAE) in November 2015, followed by the second #WePROTECT Summit. This Summit ended with a declaration calling for a ‘model national response’ to prevent and tackle child exploitation. Backed by Europol, the model national response outlines best practices for countries developing their national capacity and capabilities needed to combat this crime.
The solution is dynamic and evolving so new functionalities can be constantly introduced. EMAS 2.0 became live in December 2015 and is fully automated. It has been made available to authorised law enforcement cyber investigators, allowing them to upload malware samples and receive the results directly via the Internet, with Siena messages created in the backend.

The submitted malware is crosschecked inside EMAS and also with the Europol databases to identify connected investigations.

The main requirements for the files include that:
- the malware comes from ongoing investigations,
- it is of interest to a law enforcement agency, and
- all information submitted is classified as Europol Basic Protection Level.

EMAS Workshop in Colombia

EMAS v2.0 was promoted during a workshop organised at the Colombian Police Headquarters on 24 and 25 of February 2016, counting with the presence of 35 representatives from law enforcement, CERTs and the private sector in Colombia and other countries in the AMERIPOL community.

Currently, the EMAS is also being shared with law enforcement from non-EU countries that Europol has signed an operational agreement with, including Colombia. CERTs and private sector companies from Colombia, as well as from other AMERIPOL countries, cannot directly access the EMAS, having to rely instead on the liaison officer representing Colombia in the J-CAT. The workshop offered the participants an overview of how to deal with malware, while explaining the capabilities that the solution and Europol have to offer in this regard.

The first day was an open session for all participants and included examples of malware intelligence analysis and expertise exchange among the different participants. Day two of the workshop, for law enforcement only, also included a hands-on malware forensics and analysis session. It gave the police representatives the opportunity to set up EMAS accounts, upload malware and receive the analysis results, while understanding the way the sandbox environment works and becoming more confident in using the tool.

The EMAS Workshop in Colombia

EMAS 2.0 was promoted during a workshop organised at the Colombian Police Headquarters on 24 and 25 of February 2016, counting with the presence of 35 representatives from law enforcement, CERTs and the private sector in Colombia and other countries in the AMERIPOL community.

Currently, the EMAS is also being shared with law enforcement from non-EU countries that Europol has signed an operational agreement with, including Colombia. CERTs and private sector companies from Colombia, as well as from other AMERIPOL countries, cannot directly access the EMAS, having to rely instead on the liaison officer representing Colombia in the J-CAT. The workshop offered the participants an overview of how to deal with malware, while explaining the capabilities that the solution and Europol have to offer in this regard.

The first day was an open session for all participants and included examples of malware intelligence analysis and expertise exchange among the different participants. Day two of the workshop, for law enforcement only, also included a hands-on malware forensics and analysis session. It gave the police representatives the opportunity to set up EMAS accounts, upload malware and receive the analysis results, while understanding the way the sandbox environment works and becoming more confident in using the tool.

The solution is dynamic and evolving so new functionalities can be constantly introduced. EMAS 2.0 became live in December 2015 and is fully automated. It has been made available to authorised law enforcement cyber investigators, allowing them to upload malware samples and receive the results directly via the Internet, with Siena messages created in the backend.

The submitted malware is crosschecked inside EMAS and also with the Europol databases to identify connected investigations.

The main requirements for the files include that:
- the malware comes from ongoing investigations,
- it is of interest to a law enforcement agency, and
- all information submitted is classified as Europol Basic Protection Level.

EMAS Workshop in Colombia

EMAS v2.0 was promoted during a workshop organised at the Colombian Police Headquarters on 24 and 25 of February 2016, counting with the presence of 35 representatives from law enforcement, CERTs and the private sector in Colombia and other countries in the AMERIPOL community.

Currently, the EMAS is also being shared with law enforcement from non-EU countries that Europol has signed an operational agreement with, including Colombia. CERTs and private sector companies from Colombia, as well as from other AMERIPOL countries, cannot directly access the EMAS, having to rely instead on the liaison officer representing Colombia in the J-CAT. The workshop offered the participants an overview of how to deal with malware, while explaining the capabilities that the solution and Europol have to offer in this regard.

The first day was an open session for all participants and included examples of malware intelligence analysis and expertise exchange among the different participants. Day two of the workshop, for law enforcement only, also included a hands-on malware forensics and analysis session. It gave the police representatives the opportunity to set up EMAS accounts, upload malware and receive the analysis results, while understanding the way the sandbox environment works and becoming more confident in using the tool.

The solution is dynamic and evolving so new functionalities can be constantly introduced. EMAS 2.0 became live in December 2015 and is fully automated. It has been made available to authorised law enforcement cyber investigators, allowing them to upload malware samples and receive the results directly via the Internet, with Siena messages created in the backend.

The submitted malware is crosschecked inside EMAS and also with the Europol databases to identify connected investigations.

The main requirements for the files include that:
- the malware comes from ongoing investigations,
- it is of interest to a law enforcement agency, and
- all information submitted is classified as Europol Basic Protection Level.
Within EC3

EC3 cooperation with Academia: Understanding Cyber Behaviour

Many security and police professionals spend their time analysing the technical and mechanical aspects of cybercrime, dissecting malware and exploit tools, forensically analysing code and techniques. However, few actively focus on its social and psychological aspects – in other words, who is the attacker and more importantly why do they do it? What do we know about online victimisation? Understanding the behavioural and developmental aspects of cyber criminality is becoming increasingly important, and underlies a shift from reacting to actively intervening, protecting and focusing on victims.

Cyberpsychology is the study of the impact that technology has on human behaviour - an advanced discipline within the behavioural sciences. There are now over 1000 papers published yearly, and more than 30 academic journals on cyber behaviour. It is predicted that the subject will enjoy exponential growth due to the rapid acceleration of Internet technologies and the pervasive and profound influence of the Internet on human beings. My area of specialisation is forensic cyberpsychology, which focuses on the specific aspects of behaviours facilitated by evolving technology, namely criminality and victimology.

As a member of the Academic Advisory Network at EC3 (EC3 AAN), my aim is to promote cooperation between Europol, academia, relevant authorities and the private sector to address technology-facilitated criminal behaviour.

In 2015, a UK telecommunications company had a security breach and lost valuable data. Five suspects were arrested in connection with the investigation, all aged between 15 and 20 years old. In a separate case, a British teenager who worked as a ‘hacker for hire’ was spared a prison sentence after having orchestrated cyber attacks targeting global institutions from his bedroom. This teenager was just 13 when he joined a network of online hackers. While some were surprised by the young age of those arrested in these cases, it wasn’t that unforeseen at all. As behavioural scientists, we know that impulsivity and risk-taking behaviour increases within the formative teenage years. Indeed, there have been reports of the increasing involvement of youth in criminal activity online for some time now. In 2015, the Australian Bureau of Crime Statistics and Research reported that cyber fraud offences committed by people under 18 years of age had jumped by 26 per cent in the previous two years, and 84 per cent in the previous three years. In a recent survey conducted by an online security company roughly one in six teenagers in the US, and one in four teenagers in the UK, reported that they had tried some form of Internet ‘hacking’.

The research project

Together with a number of fellow academics at the EC3 AAN, Professor Julia Davidson (Criminologist: Middlesex University School of Law), Professor Steve Chan (Network Scientist: MIT, Harvard, Swansea & Hawaii Pacific Universities), and Europol’s EC3, we are working on a cutting edge research project that will investigate evolving online criminal behaviour. Our project is called ‘Youth Pathways into Cybercrime’ and will explore the trajectories and pathways that lead to ‘cyber juvenile delinquency’, cyber-criminality and online victimisation. The research will integrate theoretical frameworks from criminology, psychology and cyberpsychology. It is envisaged that our research findings will facilitate informing the work of professionals within key infrastructures under threat from particular types of cyber-criminality (i.e. fraud and financial crimes against the banking industry), will contribute to educational awareness in schools and colleges for vulnerable young people, as well as inform the development of training and best practice for police across a range of roles and cyber-offences.

I see enormous value in EC3 AAN’s project researching youth pathways into cybercrime. I am continually saddened by the arrest of tech talented children who drift into cybercrime. These children have unique and often self-taught skills, they are immensely talented, and need mentoring in order to be guided in the right direction. They can be a valuable asset for Europe and society in general, they are capable of immensely talented, and need mentoring in order to be guided in the right direction. They can be a valuable asset for Europe and society in general, they are capable of filling a significant skills gap in the cybersecurity industry. We need to proactively work with schools and the education system to assess and identify this talent at an early stage and encourage the positive aspects of cyber before they potentially progress into criminality.‘

Steven Wilson, Head of EC3

---

3 http://www.dailystandard.co.uk/news/story/1620448379e30ab46f17493e404757
The opening of the Europol office at the INTERPOL Global Complex for Innovation (IGCI) in Singapore is providing Europol’s European Cybercrime Centre (EC3) with the unique opportunity to support operational cooperation with the INTERPOL Digital Crime Centre (IDCC) and strategic coordination with the INTERPOL Innovation and Outreach Directorate in the fight against cybercrime.

The recent Dorkbot botnet takedown led by the US’ FBI and supported by EC3 is an example of the benefits of such cooperation. It involved coordinating actions between the three centres, EC3/ICAT, IGCI/IDCC and I4C to collectively achieve our objectives in partnership with the private sector - Microsoft in this case. Other ongoing initiatives were concluded during the last Europol-INTERPOL Cybercrime Conference in September 2015, and work is in progress in the area of the abusive use of virtual currencies, the preparation of a cyber compatibility chart and the standardisation of the cybercrime course curriculum. All are good examples highlighting the complementarity developed between both centres regarding strategic matters.

The posting of a Liaison Officer (LO) to the IGCI is one of the ways to reach out to countries which are of specific interest considering the global scale of activities developed by organised crime groups (OCGs) and existing interactions between the EU and Asia. In that regard, the INTERPOL Sub-directorate for Asia & South Pacific based in the IGCI is a key partner, complemented by promising collaboration with ASEANAPOL. This regional body is in charge of cooperation between police forces in the ASEAN region1, representing a population of approximately 625 million people.

Activities developed in the area of payment card fraud (PCF) reflect the importance of the multi-stakeholder approach that we are supporting from Singapore. In November 2015, EC3 in cooperation with INTERPOL and ASEANAPOL organised the first strategic meeting on PCF. The meeting brought together 18 experts from EU Member States, including Bulgaria, France, Germany and Romania, and the ASEAN countries Indonesia, Philippines, Thailand and Vietnam. During this two-day event, investigators focused on PCF overseas and money withdrawal in the extended South East Asian region. As a result, connections were identified between EU and Asia in relation to Bulgarian and Romanian OCGs, who are developing their illicit activities in Indonesia, Thailand, Taiwan and Sri Lanka. On 22 and 23 March 2016, the second meeting involving all ASEANAPOL countries plus Macao/China, will take place in Kuala Lumpur, Malaysia.

Within EC3

Within EC3

Update from the Europol LO to the IGCI

Within EC3

Europol’s EC3 training course - COSEC

The opening of the Europol office at the INTERPOL Global Complex for Innovation (IGCI) in Singapore is providing Europol’s European Cybercrime Centre (EC3) with the unique opportunity to support operational cooperation with the INTERPOL Digital Crime Centre (IDCC) and strategic coordination with the INTERPOL Innovation and Outreach Directorate in the fight against cybercrime.

The recent Dorkbot botnet takedown led by the US’ FBI and supported by EC3 is an example of the benefits of such cooperation. It involved coordinating actions between the three centres, EC3/ICAT, IGCI/IDCC and I4C to collectively achieve our objectives in partnership with the private sector - Microsoft in this case. Other ongoing initiatives were concluded during the last Europol-INTERPOL Cybercrime Conference in September 2015, and work is in progress in the area of the abusive use of virtual currencies, the preparation of a cyber compatibility chart and the standardisation of the cybercrime course curriculum. All are good examples highlighting the complementarity developed between both centres regarding strategic matters.

The posting of a Liaison Officer (LO) to the IGCI is one of the ways to reach out to countries which are of specific interest considering the global scale of activities developed by organised crime groups (OCGs) and existing interactions between the EU and Asia. In that regard, the INTERPOL Sub-directorate for Asia & South Pacific based in the IGCI is a key partner, complemented by promising collaboration with ASEANAPOL. This regional body is in charge of cooperation between police forces in the ASEAN region1, representing a population of approximately 625 million people.

Activities developed in the area of payment card fraud (PCF) reflect the importance of the multi-stakeholder approach that we are supporting from Singapore. In November 2015, EC3 in cooperation with INTERPOL and ASEANAPOL organised the first strategic meeting on PCF. The meeting brought together 18 experts from EU Member States, including Bulgaria, France, Germany and Romania, and the ASEAN countries Indonesia, Philippines, Thailand and Vietnam. During this two-day event, investigators focused on PCF overseas and money withdrawal in the extended South East Asian region. As a result, connections were identified between EU and Asia in relation to Bulgarian and Romanian OCGs, who are developing their illicit activities in Indonesia, Thailand, Taiwan and Sri Lanka. On 22 and 23 March 2016, the second meeting involving all ASEANAPOL countries plus Macao/China, will take place in Kuala Lumpur, Malaysia.

Another added value of the LO’s presence in this region is the Airline Cybercrime Course held in Seoul, South Korea, at the beginning of June this year.

1 This area is made up of 10 countries: Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar/Burma, Philippines, Singapore, Thailand and Vietnam.

Within EC3

Europol’s EC3 training course - COSEC

The 16th Europol training course on ‘Combating the Online Sexual Exploitation of Children on the Internet’ (COSEC), held in Sehm, Germany at the LAFP-NRW Police Academy, concluded on 13 October 2015.

This 10-day course provided training for 63 representatives from EU Member States, non-EU States (Australia, Canada, Norway, Colombia, New Zealand, Turkey, Serbia, Former Yugoslav Republic of Macedonia) and INTERPOL. Principally aimed at law enforcement investigators, the course was also attended by a number of prosecutors from the Member States.

The course follows a collegial approach, with trainers and investigators working in the field of child sexual exploitation coming together to network and exchange experiences. The main objective is to enhance the expertise of those working in this crime area in the EU and beyond, so that they are better able to investigate and dismantle child sex offender networks on the Internet, with the rights and safety of the children involved being a priority. This year the course was extended and provided extra victim identification training to investigators. In addition to lectures, ranging from perpetrator psychology and the latest online investigation techniques to international cooperation, the course programme included a wide range of hands-on exercises with the intention of aligning law enforcement investigation standards.

Since the first course took place in 2000, approximately 730 law enforcement officers and members of the judiciary have been trained.