Dear reader,

I am pleased to present the seventh issue of the Eurojust News, following the priorities set by the European Union to focus on the fight against terrorism, drug trafficking, trafficking in human beings, fraud, corruption, cybercrime, money laundering, and other activities related to the presence of organised crime groups in the economy.

This issue, the first I am introducing since I was elected President of Eurojust, is devoted to the increasingly serious phenomenon of cybercrime. Cyberspace is unfortunately uncontrollable, without borders, unsecured and available to everyone, thus providing ample opportunities for exploitation of people and infrastructure. The ability to exchange and share information immediately poses unique challenges and allows criminals to elude law enforcement and stay several clicks ahead of regulations, exploiting fully the technological advancements in IT just within the past 10 years. This newsletter highlights the actions taken by major players in the field, problems with terminology, obstacles and successes.

If you have any comments concerning this newsletter, please contact our Press & PR Service at info@eurojust.europa.eu.

Michèle Coninsx, President of Eurojust

Cybercrime

In the spring of 2007, Estonia fell victim to a significant act of so-called “cyber-terrorism”, posing an economic and political threat that no modern economy had previously experienced. A series of electronic bombardments struck down media, telecommunications, government and banking websites. Servers from Peru, Vietnam and the USA flooded Estonian websites. The attack disabled telephone exchanges for more than an hour, jeopardising emergency services. It also paralysed media and government portals. The attacks continued for two weeks, in three separate waves, affecting the ordinary tasks that fuel modern economies. Subsequent investigations and identification of those responsible have given rise to allegations and denials from all sides.
This was the first high-profile public incursion on the global telecommunications stage, bringing terms such as cyber-terrorism, crime, war, attack and their like into the vernacular.

Cybercrime is difficult to define, as it takes a number of forms. The term is normally used to describe an activity in which a computer or a network is an essential part of the crime:

- A tool of the criminal activity (e.g. spamming, copyright crime);
- A target of the crime (e.g. unauthorised access, malicious code);
- The place of the criminal activity (e.g. telecommunications fraud);
- Facilitates cybercrime (e.g. Nigerian fraud, hacking, phishing, child pornography, identity theft).

Cybercrime can be perpetrated by many individuals acting together to commit the same criminal activity, thus making it an organised crime. Cybercrimes can be located only with a great deal of diligence and, sometimes, luck. Cybercrimes have both an international as well as a national dimension. The theft of personal data, as well as the theft, exchange, sharing or falsification of identities, creates conflicts between the Member States and third States over issues of sovereignty.

The term cybercrime is conventionally used to describe a criminal activity in which a computer or a network plays an essential role; however, cybercrime is also used to include other traditional crimes in which computers or networks make the illicit activity possible. Therefore, cybercrime takes place when the computer is a tool of the criminal activity (e.g. spamming, copyright crimes perpetrated through peer-to-peer networks, etc.); cybercrime also occurs when the computer or the network is a target of the crime, such as unauthorised access, malicious code, or when the computer or the network is located where the criminal activity actually occurs, such as telecommunications fraud. Finally, cybercrime could be facilitated through the use of computers or networks (e.g. “Nigerian” fraud, hacking, phishing, child pornography, identity theft, etc.).

There are two main types of crime, when the computer and networks are the target, and when the computer and networks are the instruments utilised to commit crimes. Cybercriminals can be identified inter alia as either lone hackers, quasi-organised “hacktivist” groups, organised criminal gangs or state-sanctioned interference.

The complexity and nature of cybercrime are such that a single publication cannot cover all aspects in depth. However, one area of major international concern is the burgeoning presence of malware and its association with almost every area of cybercrime. The purpose of malware is to allow criminals to compromise and control computers, and is invariably malicious in intent. Malware is used in data theft, including credit card or bank account information, to be sold for profit. Often the criminal and the purchaser of the information will be in different countries, with the victim in a third country, demonstrating the need for international cooperation to combat the activities of these criminals.

Symantec, a large computer security company, conducted a study of the countries most responsible for the world’s cybercrime in 2011, and for the initiation of attacks. Not surprisingly, countries possessing high-speed internet connections are very attractive to cybercriminals due to constant connectivity. Topping the list are the USA, China and Germany, with the USA alone accounting for 23% of malware activity worldwide. The following factors were taken into account: malicious code, spam zombies, websites hosting phishing sites and bot-infected computers.

As individual governments struggle to keep pace with the technologies of crime, a key element in stopping the proliferation of malware is better information for computer users. Those using the internet need to be aware of the potential risk. Too often, advice and information for safe use of the internet are too technical or difficult for most computer users to properly understand and a “single source” of reliable information is as yet unrealised.
Do governments have a duty to protect their citizens from crime on the internet as they do on the streets? As a victim of cybercrime, does a citizen deserve any less redress, consideration or help?

McAfee, Norton and Commtouch, the major anti-virus/anti-malware software producers, issue periodic cybercrime reports:

- the McAfee Threat Report for the third quarter of 2011 shows that while mobile telephone malware has doubled since 2009 to 1200 types, the variants for PCs numbered 4 million. McAfee also estimated loss of income to businesses around the world of €600 billion in 2011;
- the Norton Cybercrime Report of September 2011 surveyed 24 countries and estimates the number of cybercrime victims per day at 1 million;
- the Commtouch Internet Trends Threat Report 2011 analyses over 2 billion e-mails per day. The report found that in March 2011 over 30% of e-mails analysed had malware attached.

The statistics quoted in these reports do not specify the harm and impact of malware and as such cannot be relied upon to provide a complete picture. They refer to situations where malware has been detected and, for the most part, thwarted. However, they do provide a powerful argument for the deployment of anti-malware products.

As international forecasters and specialists have realised, providing accurate figures on the economic impact of cybercrime is impossible. The financial implications of cybercrime tend to be subjective and speculative. Unreliable reporting of cybercrime, or a complete failure to report, will distort the actual financial cost. In a paper entitled *Cyber incident reporting in the EU* (August 2012), the European Network and Information Security Agency (ENISA) claims companies are failing to admit to security breaches, leaving billions of euro in losses or damages unreported.

The main focus of the world’s media is confined to large-scale attacks that damage or threaten infrastructure or national security. However, the majority of cybercrime is less dramatic but far more pervasive.

Of the various types of malware, Trojans make up almost 70% of attacks, allowing criminals access to targeted computers through the use of stealthy viral software. Commercial and free-to-download malware detection software attempts to combat the spread of an ever greater number of malicious products.

As recently as September 2012, Microsoft’s digital crime investigators discovered four “factory fresh” PCs that were pre-infected with malware. Cybercriminals have opened a new front in their battle to infect computers with malware, namely PC production lines. One virus detected by Microsoft, called Nitol, steals personal details to help criminals plunder online bank accounts. Further investigation revealed that the botnet behind Nitol was being run from a web domain that had been involved in cybercrime since 2008. Also on that domain were 70,000 separate sub-domains used by 500 separate strains of malware to fool victims or steal data. Keeping pace with the increasing sophistication and complexity of cybercriminals and the malware they employ remains, in the areas of detection eradication and prosecution, a Sisyphean task.

Various forms of crime have been transformed by their use of the internet; for example, credit card fraud can now take place

---

**Definitions**

**Trojans** *(source: Cisco.Com)*

A Trojan is another type of malware named after the infamous wooden horse used by the Greeks to infiltrate Troy. It is a harmful piece of software that looks legitimate. Users are typically tricked into loading and executing it on their systems. After it is activated, it can achieve any number of attacks on the host, from irritating the user (popping up windows or changing desktops) to damaging the host (deleting files, stealing data, or activating and spreading other malware, such as viruses). Trojans are also known to create back doors to give malicious users access to the system.

Unlike viruses and worms, Trojans do not reproduce by infecting other files nor do they self-replicate. Trojans must spread through user interaction such as opening an e-mail attachment or downloading and running a file from the internet.

**Botnet** *(source: Microsoft.Com)*

The term bot is short for robot. Criminals distribute malicious software (also known as malware) that can turn your computer into a bot (also known as a zombie). When this occurs, your computer can perform automated tasks over the internet, without your knowledge. Criminals typically use bots to infect large numbers of computers. These computers form a network, or a botnet.

Criminals use botnets to send out spam e-mail messages, spread viruses, attack computers and servers, and commit other kinds of crime and fraud. If your computer becomes part of a botnet, your computer might slow down and you might inadvertently be helping criminals.
on an industrial scale. Fraud is another growth area that provides anonymity for the perpetrator, creating new opportunities for organised criminal groups to finance their activities. Another crime type is that facilitated by the internet. The internet may be used to organise a range of offences such as drug dealing, people smuggling and child exploitation and to conceal them more easily from law enforcement agencies. By focusing their activity on areas offering the broadest opportunities, criminals increase their potential monetary returns and reduce the risk of exposure.

Information sources:
- Professor Peter Sommer, London School of Economics

More information:

Keeping pace with the increasing sophistication and complexity of cyber criminals and the malware they employ remains a Sisyphian task.
European counter-measures

Council of Europe

The Council of Europe Convention on Cybercrime (also known as the Budapest Convention or simply the Convention) of 23 November 2001, in force since 2004, and ratiﬁed by 35 Council of Europe Member States (as of September 2012), the USA and Japan, is the ﬁrst and only multilateral treaty to address computer-related crimes.

The Convention is one of few ofﬁcial documents to attempt a comprehensive deﬁnition of cybercrime. It outlines European policy against cybercrime and against each crime perpetrated via the use of the internet, networks and computers, with the goal of attaining rapid and well-functioning international cooperation in criminal matters and highlighting the need for cooperation between governments and private industry.

The Convention also provides for meetings of law enforcement experts, better coordinated ﬁnancial support for training activities, and monitoring of the evolving threat of cybercrime to evaluate the need for further legislation. Additional protocols have been added regarding other sorts of crimes related to cybercrime, such as racist and xenophobic acts and child abuse and exploitation.

European Union

A Council Framework Decision on attacks against information systems entered into force in 2005, covering, inter alia, illegal access to information systems, illegal system interference, and illegal data interference.

The EU Counter-Terrorism Strategy, approved by the JHA Council in 2005, has as one of its key priorities the development of common approaches to detect and tackle internet misuse.

Several EU bodies have been created to prevent cybercrime by promoting best practices and sharing information, such as the European Cybercrime Training and Education Group (ECTEG), which has run a series of common projects since 2000 with ﬁnancial support from the European Commission’s programs supporting the development of law enforcement excellence (FALCONE, AGIS, ISEC). Member States are invited to adopt a common approach and promote harmonisation of legislation.

To escape a total network crash and place increasing importance on internet security, the European Union must assess preparedness measures against cyberthreats, natural disasters, and technology failures. During simulation exercises organised by ENISA, weaknesses, interdependencies and training needs were identiﬁed. In addition, experts in several Member States are trying, via simulations, to counter potential attacks by hackers that can paralyse critical online services and network crashes.

European Commission

Ms Neelie Kroes, Commission Vice-President in charge of the Digital Agenda, seeks an integrated EU approach due to the international dimension of cybercrime. Her goal is to achieve a common consensus on the priorities in terms of public policy and operational deployment. Furthermore, this agenda contains key actions to allow faster reactions and combat cyberattacks against information systems. As Ms
Kroes said, to efficiently fight against cybercrime, we must foster cooperation between government and industry. Prevention is better than cure.

In particular, Ms Kroes has highlighted the vulnerability of the internet. She encourages everyone, at every level of society, to be safe online: “Cyber security is vital for the European economy, to protect the businesses and operations of ordinary citizens. Users must be safe and secure when they connect online.”

Eurojust

One of the main tasks of Eurojust is to facilitate better cooperation between Member States, especially through the exchange of information during coordination meetings, considering the potential speed at which cybercrimes can be committed.

In the “Communication from the Commission to the European Parliament, the Council and the Committee of the Regions: Towards a general policy on the fight against cyber crime”, dated 22 May 2007 (COM (2007) 267 final), Eurojust is described as a powerful instrument in the fight against cybercrime, offering a coordinated approach, such as at Eurojust’s strategic meetings.

Strategic meetings

In October 2008, Eurojust held a strategic meeting on cybercrime in Athens, Greece, supported by the Ministry of Economy and Finance of the Hellenic Republic, following on the international interest and concern about the topic and the cooperation and coordination activities carried out by Eurojust in fighting this criminal phenomenon.

Keynote speakers in the meeting were prosecutors, judicial and cybercrime specialists, university professors, and police officers from all over Europe and the USA. More than 120 participants were informed about the status of the fight against all forms of cybercrime and the available means to prevent and combat it.

Another Eurojust strategic meeting was held in September 2011, dealing with travelling child sex offenders, where national authorities and experts in the field met to share information and best practices.

In June 2012, Eurojust held a strategic meeting on "The phenomenon of the lone individual involved in terrorism (‘lone wolf’)" and "Social networks in a terrorism context", attended by police and judicial authorities from 24 Member States, Norway and Europol. The increasing role of the internet as a facilitator in these types of terrorist attacks was highlighted.

Figure 1 - Number of cybercrime cases addressed by Eurojust in the period 2004-2012 (source: Eurojust Case Analysis Unit)
**FEC Team**

The Eurojust Financial and Economic Crimes Team (FECT) is a source of cybercrime expertise and supports developments leading to the Council Conclusions on an action plan to implement a concerted strategy to combat cybercrime. The FECT is responsible for allocating Eurojust’s resources and expertise concerning its participation in the European Cybercrime Centre.

**Casework**

In the first half of 2012, Eurojust registered 24 cybercrime cases, involving 12 Member States. Seven of these cases are multilateral in nature (i.e. involving more than two Member States). Eurojust’s current casework numbers indicate that by the end of 2012, cybercrime may increase significantly in relation to 2011 statistics (see figure 1). The map on page 8 illustrates the relative volume of casework dealt with by Eurojust’s National Desks as requesting and requested countries. The size of the pie charts corresponds to the number of cases per country, with the colour coding reflecting the volume of requested and requesting instances.

**Other organisations**

The International Criminal Law Network (ICLN) will hold its annual conference, entitled “Combating Cybercrime: Legal and Technical Standardization and Cooperation on a National, European, and Global Scale”; in The Hague on 13 December 2012, addressing the need for commercial and non-commercial entities to cooperate in investigation and prosecution of cybercrime.

**Obstacles**

No harmonisation of cybercrime law has been undertaken. One of the main obstacles in cybercrime cases, unlike other types of crime, is the issue of territoriality. The exact location of the crime is almost impossible to determine. Law enforcement must act quickly to preserve electronic evidence. Given different time zones, a need exists for “around the clock” capability.

---

**Case illustration – “Operation Nanny”**

On 6 March 2012, Eurojust ran an Operational Coordination Centre at its premises in The Hague to coordinate in real time police and judicial actions in an international case of sexual abuse of children on the internet.

Eurojust was requested by the Public Prosecutor’s Office of Florence, Italy, to support the investigations and prosecution of a case of trafficking, marketing and distribution of pornographic material featuring minors via the internet, and specifically using a social network hosted on servers located in the USA. These social networks are frequented by followers from around the world, who are linked by a common interest in online child pornography and, in particular, in the exchange and dissemination of images and videos of minors under the age of 14 years. The manager of the social network in question was identified during the investigation as an Italian national.

Thanks to the US Naval Criminal Investigative Service (N.C.I.S.), the social networks were first frozen in the USA, and then seized by the N.C.I.S. while implementing a search order signed by a California judge. Users were identified via the IP addresses they used to carry out transactions such as uploading and distributing photos and/or videos of an illegal nature. IP addresses were identified and located in 12 Member States, the USA, Norway, Turkey and Ukraine as well as in Asia.

Eurojust was requested to coordinate search and seizure activities to be carried out in several Member States through international judicial cooperation tools, in order to preserve the evidence and to dismantle the network. Europol was involved as well from the outset to support the coordination of investigations, provide analysis and play an important role along with Interpol, whose liaison officer attended the coordination meetings and continually cooperated with Eurojust.

Coordination meetings were held at Eurojust in January and February 2012 to prepare the action day that took place on Tuesday 6 March with the valuable support of Eurojust’s Case Analysis Unit. During the action day, France, Portugal, Germany, Spain, Sweden and Italy were actively involved, supported by Eurojust, Europol and Interpol. As a result, many house searches took place; computers were seized; 10 suspects were arrested worldwide; many IP addresses were identified; and 112 people are under investigation for criminal association. A huge amount of child abuse images were found; one suspect’s computer yielded 2300 downloaded files, photos and videos.

After the successful action day, the Deputy National Member for Italy at Eurojust, commented: “Eurojust is committed to fight against child abuse, especially sexual child abuse on the internet. Children are amongst the most vulnerable of our citizens, and must be protected from those who prey upon them. Child abuse is a growing phenomenon, aggravated by the development of the internet. Since its establishment, Eurojust has played an active role in fighting crimes against children. The revised Eurojust Decision includes an obligation for the Member States to inform Eurojust about complex cross-border cases involving the sexual exploitation of children and child pornography. Since 2010, Eurojust has dealt with 64 cases concerning children. We will continue to fight against these horrible crimes.”
In addition, the EU Charter of Fundamental Rights, especially in the areas of freedom of expression and protection of personal data, must be respected when dealing with all forms of crime, including cybercriminality.

Conclusion

The Norton Cybercrime Report of September 2011 suggests that victims lose approximately €290 billion each year worldwide as a result of cybercrime. The US Federal Bureau of Investigation estimates that cybercrime could cost $67 billion per year in the USA alone. The loss is not only financial.

In the coming digital age, the European Union needs to treat cybercrime as a priority. Two of the main challenges are to harmonise legislation and encourage cross-border investigations against a type of crime which, by definition, knows no borders. Therefore, preventive measures are needed, including safer use of IT and training programmes.

Dialogue between Member States and industry is essential. Effective governance of the global internet is currently not feasible. WikiLeaks has proven that internet security is fallible.

Figure 2 - Relative volume of cybercrime casework addressed by Eurojust (source: Eurojust Case Analysis Unit)
European Cybercrime Centre

On 28 March 2012, a Communication of the Commission to the Council and the European Parliament stated its proposal to establish a European Cybercrime Centre (EC3), to be a part of, and located within, Europol, and to focus on four major aspects of cybercrime, namely its core functions: cybercrimes committed by organised crime groups, particularly those generating large criminal profits, such as online fraud; cybercrimes that cause serious harm to their victims, such as online child sexual exploitation; and cybercrimes (including cyberattacks) affecting critical infrastructure and information systems in the European Union.

Four core functions were identified for the EC3: to serve as an EU cybercrime information point (intelligence); to be the pool of EU cybercrime expertise (capacity-building and training); to provide support to Member States’ cybercrime investigations (operational); and to become the collective voice of EU cybercrime investigators and prosecutors across the European Union.

The first meeting of the Management Board of the European Cybercrime Centre, an implementation meeting, took place on 12 June 2012. In addition to two Eurojust National Members and a Case Analyst, in attendance were participants from ENISA, CEPOL, EU-CERT, EUCF, CIRCAM, European Multidisciplinary Platform Against Criminal Threats (Cybercrime EMPACT) and the Danish Council Presidency.

In accordance with the Communication from the Commission, Eurojust is tasked to participate in the Programme Board and is also invited to be directly involved in the activities of the EC3 and thus to contribute to its four core functions. Eurojust can provide added value to the operational and strategic work, as well as assist in the training activities for law enforcement and judiciary authorities.

EC3 will rely on Europol’s existing capabilities in technology for the present, including its ICT platform and core systems, and will initially be staffed by 30 Europol personnel. The Heads of Units of Cybercrime of the Member States will also be involved. For the time being, EC3 will perform within the current legal framework of Europol concerning exchange of information and data protection. Additional EC3 services may require changes in the legal framework, such as: information exchange with private parties and EC3 being a Central Office of the European Union for combating Cybercrime (based on the same model as Europol being the Central Office of the European Union for combating Euro counterfeiting). One of the major problems with the current provisions is that Europol cannot receive personal data directly from private parties. The information must be routed through the Europol National Unit (ENU).

Under EC3, all former cybercrime Analysis Work Files (Cyborg, Twins, Terminal) will be united. Eurojust’s contribution to the EC3 will be of added value for both Europol and Eurojust in the fulfilment of their tasks, and will cover from Eurojust’s side the following aspects:

Operational work:
- Facilitating the information exchange concerning prosecutions, investigations and proceedings where mutual legal assistance and mutual recognition instruments are used in cybercrime cases;
- Ensuring the information exchange on cybercrime cases (cross-checking) is in accordance with the agreement regulating the exchange of data between Eurojust and Europol;
- Providing coordination in cybercrime cases when parallel investigations take place, conflicts of jurisdiction arise, or coordinated execution of mutual recognition instruments are needed (e.g. European Arrest Warrants); and
- Organising coordination meetings at Eurojust and coordination centres for real-time support.

Strategic work:
- Providing legal advice in cybercrime investigations, including on the establishment of JITs and the funding of JITs;
- Collecting and disseminating best practices for prosecution of cybercrime;
- Establishing permanent contacts with judicial experts;
- Providing data for statistical purposes; and
- Organising strategic and technical meetings.

Training activities:
- Supporting CEPOL in the development of training modules for law enforcement and judicial authorities; and
- Contributing to judicial training by the European Judicial Training Network (EJTN).
Interview with Mr Troel Oerting
Assistant Director of Europol and Director of the EC3

Eurojust: Could you tell us something about your background and professional career?

Troel Oerting: “Back in Denmark, I was responsible for the Serious and Organised Crime Agency. This agency has a high-tech crime sector, so I was responsible for cybercrime at that time. Then I left for Europol to work as an Assistant Director in the ICT Department; then I moved to the Organised Crime Department and the Director gave me the opportunity to develop new things.”

What crimes fall under the cybercrime category?

“Cybercrime cannot be isolated. It is a huge facilitator for organised crime in many ways and is hijacked by organised crime groups. We base our definition on the definition of the European Cybercrime Convention, which also includes the use of credit cards in cybercrime (not just skimming).”

How important is the fight against cybercrime?

“The fight against cybercrime is even more important than the fight against other forms of organised crime, because it is an economic issue: 72% of the citizens of the European Union have an internet connection, in contrast to the world average, which is 34%. We, as a region in the European Union, have outsourced the more labour-intensive work to Asia, Africa and South America, as it is now too expensive to do it here. What we are good at in the European Union are innovation, marketing, branding, the supply chain ... All of these actions require a very strong infrastructure on the internet. And now we are actually facing a recession. Our only engine is completely dependent on the safety of the internet. So to go back to our prosperity and growth, we need also to protect the engine and the reliability of the internet. This is where invention, creation and innovation are carried out.”

“Secondly, the fight against cybercrime is about our core values: transparency, openness and democracy. The European Union is very transparent: we are accustomed to a vast amount of accessible information, including information about the decision-makers, the European Parliament, the police, etc, and we use the internet for this transparency. It is vital that we do not hamper this possibility.”

Europol is of course already working on cybercrime. Why set up a new centre; what is the added value?
“What we were doing in the crime centre until now was basically to facilitate operations. We were active in three areas: online child sexual abuse (AWF Twins), intrusion (the traditional core cybercrime area) (AWF Cyborg), and illegal use of credit cards (AWF Terminal). We also had limited forensic and training capacity. We actually provided a high level of operational assistance. These tasks should not be taken over by the EC3; we should coordinate them.”

“The security of the infrastructure should be enhanced, e.g. by anti-virus programmes. This is done by the owners, the “third community”; they see the attacks initially, so we need an exchange of information. This work is already done very well by ENISA and we foresee having a liaison officer from ENISA at Europol.”

Who will be working for the Cybercrime Centre and who will lead it?

“The Cybercrime Centre, as it exists now, will be transformed and will become the pillar. What we need is to scale up the capabilities. I will set it up and run this Centre of 25 people. The (independent) implementation team is 10 people; they are process managers and set up and steer the whole programme. In the meantime, we can increase our work at operational level, without being affected by the setting up. We cannot fight cybercrime without prosecution. Eurojust is of course one of the important stakeholders. We hope to have a Eurojust liaison officer based either full- or part-time at Europol, an expert with a prosecution background, as soon as possible. So we are not setting up a Europol entity, but a law enforcement entity, to avoid overlap and, for sure, duplication. We have a shared responsibility to prevent and disrupt cybercrimes and convict cybercriminals. If we can do this now, with this inclusive approach, we can gain in other areas as well.”

When will EC3 be operational?

“We commence operations as of 1 July 2012; we open the European Cybercrime Centre as of 1 January 2013, and we expect to be at cruising speed from 1 January 2014.”

You have already released two cybercrime prevention bulletins, reaching EU citizens directly.

“We have the expertise and the need to get information out; we have an obligation to provide dedicated input and guidance in areas that we think are very dangerous for the citizen. We can together generate a lot of expertise, but try not to frighten people. The advice we provide will help to avoid getting into trouble, such as how to avoid being traced on Facebook, the safe use of Twitter ... There are so many areas to explore!”
New President at Eurojust

The College of Eurojust elected Michèle Coninsx, Vice-President and National Member for Belgium, as President of Eurojust on 17 April 2012. Her mandate commenced on 1 May 2012, replacing Aled Williams, who retired.

Michèle Coninsx has had a career in the judiciary for almost 25 years. From 1997 to 2001, just before joining Eurojust, she was one of the three Belgian national prosecutors in charge of coordinating the fight against organised crime and terrorism at country-wide level, with full jurisdictional powers over the 27 Belgian chief prosecutors.

In 2001, Ms Coninsx joined Pro-Eurojust in Brussels as deputy prosecutor general and National Member for Belgium. As President of Pro-Eurojust during the Belgian Presidency of the European Council in 2001, she created the Eurojust team structure and organised one of the first press conferences. From 2001-2004, she chaired the Case-work Committee focusing on operational issues, and since 2004, she has chaired the Counter-Terrorism Team. The Counter-Terrorism Team at Eurojust is a centre of expertise at judicial level in the field of counter-terrorism.

Under the chairmanship of Ms Coninsx, the process of information-gathering of counter-terrorism-related issues has been streamlined, enabling Eurojust to contribute valuable judicial input to the TE-SAT report. Ms Coninsx also chairs all the strategic meetings on terrorism with a specific emphasis on confidence-building, networking and information-sharing among EU counter-terrorism practitioners.

In December 2007, after being elected Vice-President, she became a member of the Presidency Team, and from December 2009 to February 2010, she was acting President of Eurojust. In February 2011, she was re-elected as Vice-President of Eurojust.

Prior to joining Eurojust, Ms Coninsx was a National Prosecutor in Belgium, dealing with terrorism and organised crime at the national level. As Expert for the International Civil Aviation Organization (ICAO), she was in charge of training in aviation security in several countries, including Kenya, Thailand, Sri Lanka, China, Japan and New Zealand, and of anti-terrorism training related to aircraft sabotage and hijacking.

Ms Coninsx is the author of several publications, including Private Security Companies, The search of persons at airports, Judicial Handbook for Aviation Police Officers, Air Law for Air Traffic Controllers, and The fight against terrorism in the air. She was also keynote speaker at different international aviation security conferences dealing with terrorism in the air, airport security, human resources management and aviation security training for airport personnel.

Eurojust is a European Union body established in 2002 to stimulate and improve the coordination of investigations and prosecutions among the competent judicial authorities of EU Member States when they deal with serious cross-border crime.

Each Member State seconds a judge, prosecutor or police officer to Eurojust, which is supported by its administration. In certain circumstances, Eurojust can also assist investigations and prosecutions involving a Member State and a State outside the European Union, or involving a Member State and the Community.

Eurojust supports Member States by:

- coordinating cross-border investigations and prosecutions in partnership with judges, prosecutors and investigators from Member States, and helping resolve conflicts of jurisdiction;
- facilitating the execution of EU legal instruments designed to improve cross-border criminal justice, such as the European Arrest Warrant;
- requesting Member States to take certain actions, such as setting up joint investigation teams, or accepting that one is better placed than another to investigate or prosecute; and
- exercising certain powers through the national representatives at Eurojust, such as the authorisation of controlled deliveries.

© Eurojust 2012