Knowledge and Awareness Building Conference
Toys and Videogames
Jointly Chaired by EUIPO, Europol and Eurojust
EUIPO, Alicante
Knowledge and Awareness Building Conference
Toys and Videogames
The Director of the Observatory gave a warm welcome to all participants gathered at the ninth knowledge building seminar in the series held by EUIPO, chaired in cooperation with Europol and Eurojust. Participants from across 25 Member States and 8 non-Member States including the US attended the seminar, with the aim of consolidating enforcement’s response to the growing illegal trade in counterfeit and dangerous toys and videogames in Europe. Officers from Customs, the police, ICE, members of the prosecution and the private sector contributed to the three-day event held in Alicante.

The Director introduced the topic which is complex by nature because many IPRs apply to toys, including trade marks, copyright and design rights, and patents – and one which poses major implications on the safety of children and European citizens owing to the use of toxic and substandard materials. Notably, over 90% of toys are currently produced in Asia and transported to the European market.

The IP Contribution Study1, developed in conjunction with EPO reveals that patents are used intensively in the toys and games industry, alongside trade marks and designs. The EUIPO’s sectorial study, “The Economic Cost of IPR Infringement in Toys and Games”2 reveals the European industry’s estimated value of EUR 10.6 billion in 2012, and with 53,000 employees. Germany is a significant producer country which generates 14% of the total revenue, and more than EUR 1 billion each year. Notably, the toy industry has a strong predominance of SMEs – 99% of the sector consists of small businesses, with an average of 10.2 workers each, which makes them particularly vulnerable to attack by organised counterfeiting and piracy. Annual losses due to imports of counterfeits goods in this sector in the EU amount to 6,150 jobs lost directly and indirectly, and EUR 370 million of lost government revenue.


INTRODUCTION TO THE PROGRAMME – EUIPO
Knowledge and Awareness Building Conference - Toys and Videogames

The Observatory gave an overview of the three-day seminar and its primary aims - to amalgamate European enforcement officers, including Customs, police and prosecutors, in order to agree on common objectives, to learn from other Member States' best practices, to discuss different operational and strategic scenarios within two workshop sessions, and to improve interagency cooperation.

SETTING THE SCENE; “IPR INFRINGING TOYS AND GAMES, SEIZURES, STUDIES AND STATISTICS” - EUIPO

The Observatory gave a presentation on the scale of counterfeiting and piracy within the European toys and videogames sector, and its grave economic consequences. They highlighted the “2014 EU Border Recoveries of IPR infringing Toys and Games” study carried out by the EUIPO which is based on 2014 external border seizure data collated by DG TAXUD. Each year, EUR 11 billion is generated by the toys and games industry – of which 10% of revenue is lost due to counterfeiting, with a consequential loss of EUR 1.4 billion in tax. The overall damage to the EU economy is estimated at EUR 2.3 billion each year. DG TAXUD seizure figures (which exclude sporting goods) reveal an average shipment caseload of 2000 units per month, consisting of high unit volumes with low unit value. Consignments are sent from three main Asian countries of provenance - Singapore, China and Hong Kong – and transported via bulk ship containers, (opposed to the preferred method of airfreight for many sectors of counterfeit goods) which suggests that some countries are targeted as points of entry for larger container shipments, whose contents will subsequently be divided and distributed throughout Europe.

“A Framework to Reduce IP Infringements in Europe – Digital Games Study” created in conjunction with the EUIPO and UK IPO underlines the current models present within the illegal supply chain, and the levels of infiltration at wholesaler, manufacturer and retailer level.
The supply chain model for online games differs to the traditional supply chain because the role of author, supplier and publisher are removed. Illegal file sharing websites steal content, and illegal gamers access content directly - which negates payment to the author; instead, payment is increasingly made through malware infection and via advertising through intermediaries. Notably, there is little danger of infringement from the illegal online gaming into the legal supply chain, but there is a real and present risk of consumer confusion owing to misleading information by advertisers. The IP Perception Study (2013) carried out by the EUIPO underlines that 9% of EU citizens have wondered whether a site for downloading music or videos was legal - and for those aged 15 to 24, this number rose to 42%.

The Observatory’s presentation concluded by highlighting the role of agorateka, which has been created by the EUIPO to offer Member State citizens a European portal with which to access legal online content, including national offers of music and books.

Session 1: Physical Games and Toys

THE INDUSTRY’S PERSPECTIVE AND CHALLENGES – TOY INDUSTRIES FOR EUROPE

Founded in 1991, Toy Industries for Europe (TIE) is a trade association which represents the European Union toy industry (and includes non-European based companies with European sales), and 9 national association members. Notably, the toy industry is founded on SMEs - 88% of which are microenterprises.

The presentation focused on three main topics - why enforcement work is important to the European toy sector, specificities of the sector, and how industry can support enforcement efforts. Saliently, 12.3% sales in the sector (EUR 13,168 direct and indirect lost sales) are lost due to counterfeiting, with a consequential loss of 6,150 direct jobs. Importantly, the toy industry is amongst the most IPR-intensive sectors. The speaker underlined the tangible damage to the reputation of genuine companies, the loss of reputation to the sector as a whole, the loss of sales of popular, genuine and safety-checked products, and the dangers posed to consumers owing to substandard, toxic (including carcinogenic), faulty and unsafe counterfeit items.
The specificities of the market were highlighted, including its vulnerable consumer group, which predominantly consists of young children. Substantial investment is committed by the toy industry into safety checks – which, for example, account for approximately 10% of revenue for a SME in the textile toy industry. Additionally, trends in toy sector categories are influenced by films, celebrity endorsement and music, which requires the industry to make large and often seasonal investments into innovation - including research and safety checks into new and quickly changing trends in toy products.

Parasitic and lookalike copies pose a major problem for the toy industry. Producers of parasitic copies manage to avoid infringement claims but carry out unfair commercial practice, by manipulating adult purchasers’ confusion (who buy goods for child consumers), regarding the products in terms of genuine brands and their appearance.

The presentation concluded by underlining the scale of the problem and attempts by SMEs to work closely with law enforcement authorities (LEAs) to facilitate seizures, including raising awareness of Customs and consumer groups, and committing substantial efforts to monitor emerging trends in counterfeiting, and by investigating prior to placing the goods on the market. However, the pursuit of civil litigation poses tangible hurdles in terms of finances and resources for SME producers, who concentrate on efforts on working alongside trusted retailers - including online retailers. The rapidly growing problem posed by online counterfeits offered on platforms including alibaba and amazon was stressed: TIE has signed an MoU with the European Commission in order to tackle the issue.

EUIPO underlined that the toy industry could use practical and legal instruments including the EUIPO’s Enforcement Database (EDB), and EU Design Law which provides for packaging protection regarding lookalikes, and health and safety legislation. EUIPO expressed their wish to amalgamate national and EU associations in order to support dialogue regarding future collaboration. The specific problem of copying in the toy industry was highlighted – often by producers’ main partners (including retailers and distributors) which results in a general reluctance to pursue cases by many producers. Toys Industries for Europe agreed that there is more work to be done in this area, but noted that European producers no longer display their designs at large toy fairs in Hong Kong, in order to establish levels of confidentiality within the industry.

**LACK OF SAFETY STANDARDS FOR COUNTERFEIT TOYS – TRADING STANDARDS, UK**

The presentation underlined strong multiagency cooperation which has been established in the UK between Health and Safety authorities, police, Customs officers and Trading Standards – the latter of which has responsibility for counterfeit goods.
The 2016 UK IPO study “Counting the Cost of Counterfeit Goods” highlighted Manchester as a centre for counterfeit toy sales in the UK, and the presentation focused on a 2014 case which resulted in prosecution in Manchester. The investigation resulted in a high-volume seizure of items, the majority of which were counterfeit and substandard, and did not comply with the Toy Safety Directive 2009/48. The seller’s paperwork revealed a lack of importer, distributor and manufacturer details, and when challenged, the seller produced incorrect licence documents. The speaker detailed Trading Standards officers’ systematic production of evidence to the Crown Prosecution Service, including photographic evidence, information from the Anti-Counterfeiting Group (ACG), and information and witness statements collated from working alongside the infringed brands. Additionally, public analysts and test houses were used to check toys suspected of being unsafe, including carcinogenic and faulty parts, which are covered under UK legislation.

However, the procedural obstacles to prosecution were highlighted including the difficulty in obtaining a letter of authority prior to interview, a general lack of communication and engagement by brands - and a lack of cooperation by the sellers, including submission of incorrect documents to the court, and disclaimers regarding unknowingly selling counterfeit and substandard items. The prosecution took account of the previous criminal history of the sellers, the volume of counterfeit goods seized, and the lack of adherence to toy safety regulations. Notably, UK case-law dictates that a judge cannot impose a high fine if it will cause the offending company financial difficulties - which results in reliance on the seller’s financial documents. In this case, the judge stressed the safety risks to children connected with counterfeit toys and acknowledged the loss to legitimate business.

EUIPO underlined the low level of fines provided by the judge, in comparison to the scale of seizures and gravity of the health risks posed. They commented on the limits to prosecution, and the reality that sellers of infringing items can re-establish their business models rapidly, or relocate. UK IPO explained that the overall strategy in the UK regarding enforcement against illegal sales is consolidated by the model of illegal businesses eviction from markets, and replacement with legitimate traders.

Workshop 1: Effective Law Enforcement Response in a Case Concerning Non-Original Toys and Pirated Videogames

All participants were divided into four simultaneous workshops which focused the following questions in order to discuss how interagency and multidisciplinary level cooperation could be enhanced:


“BENDING BANANAZ” CASE STUDY

1. What are the possible options for reaction to IPR infringement threats?
2. How can cooperation between involved agencies best be established?
3. What are the obstacles to effective action?

The bullet points from the workshop discussions are collated in the Annex to this document.

THE ENFORCEMENT RESPONSE TO TOYS AND GAMES – HUNGARIAN NATIONAL TAX AND CUSTOMS ADMINISTRATION (NTCA)

The NTCA was formed in 2011 in order to amalgamate Hungarian Customs and Financial Control into one body. The organisation has over 26,000 staff and also has competence for
criminal affairs. Within the NTCA, there are three departments which have competence for IPR issues – the Criminal Affairs Department, Enforcement and Customs – the latter of which oversees controls at external borders and carries out in-depth controls by mobile units on main transport routes.

The most popular counterfeit goods in Hungary were identified as clothing, perfumes, washing powder, medicines and food supplements, and toys. Notably, low Hungarian salaries drive the demand for counterfeit products. A case study was given regarding a 2015 investigation into fake toys sold by Chinese vendors in a Budapest shopping centre. Officers discovered a large amount of fake Lego products and a criminal investigation was launched. The case is ongoing but is based on national legislation against infringement of industrial property rights. The presentation underlined the importance to distinguish between the available Hungarian sanctions for crime and misdemeanour (the latter of which is normally punished by a fine), and small and medium amounts of IPR infringing products (those which fall under EUR 350).

The speaker explained that Customs has competence for IPR crimes whilst cybercrime elements are investigated by the police – which poses problems for the prosecution when a complex case involves both approaches.

**CASE STUDIES FROM IRELAND - AN GARDA SIOCHANA, IRELAND**

The An Garda Siochana’s presentation clearly highlighted the need for multiagency communication on every level in order to effectively fight IPR crime, owing to the intrinsic link between IPR crime and the trafficking of illicit goods, and the funding of serious and organised transnational crime and terrorism. The speaker referred to the need to raise awareness amongst not only the General Public, but also the judiciary regarding the gravity and consequences of IPR crime.

The organisation provides a national point of contact and liaison, and works closely with other police authorities inside and outside Ireland. The Garda and Customs have worked hard to establish a strong and mutually beneficial relationship. The IP Crime Unit (IPCU) amalgamates the two bodies on an individual case basis to benefit from extensive Customs’ knowledge regarding illicit border supply chains and IPR crime trends. In 2016, there are 11 ongoing combined operations into counterfeit physical products, including toys. Information is passed to the IPCU via the National Bureau of Crime Investigation. The IP Regional Enforcement Group is established in each region to raise awareness within the Garda regarding IP crime trends, and the body carries out test purchases and controlled deliveries, and issues search warrants. Notably, many right holders have agreed to cover the often, extensive costs of storage through this initiative.
Additionally, there is close collaboration with the Food Safety Association and the Health Products Regulatory Authority (HPRA), and it was highlighted that the most effective method of progressing enforcement’s operational and strategic efforts is via the establishment of close working relationships.

Case studies on counterfeit videogames and toys underlined the successes of the interagency approach described, and in contrast, the agility of organised crime groups’ (OCGs) attempts to avoid detection, including changing distribution routes and delivery addresses when under surveillance. The presentation underlined that the expected profit from an individual shipped container from China is approximately EUR 25,000, many of which are sold through street markets in Dublin. Parcels also continue to be transported via small air consignments from China. The scale of financial rewards described by the speaker reveals why OCGs are willing to take risks in importing goods from Asia. The business model diversity of criminal networks was highlighted by the case studies, who spread the risk involved in their activities into other sectors of counterfeit goods, smuggling, and into reinvestment into associated criminal activity. The speaker emphasised the need to establish and maintain sustainable relationships with the private sector on a broad and holistic level: such cooperation would allow the collation of concrete evidence by industry, and result in more rapid and comprehensive investigations. The final case study given underlined the potential for enforcement to adapt to volatile OCG movements when in possession of vital information gathered and presented by right holders. The presentation concluded by emphasising the emergence of online infringements as a major cause for concern - in particular, the purchase of infringing content online by the younger generation.

CASE STUDIES FROM THE US – US IPR CENTER, USA

U.S. Immigration and Customs Enforcement (ICE) is an American federal law enforcement agency under the United States Department of Homeland Security (DHS), responsible for identifying, investigating, and dismantling vulnerabilities regarding the nation’s border, economic, transportation, and infrastructure security. The National IPR Center is led by ICE and amalgamates 23 federal and international partner agencies including the Canadian Mounted Police, Europol and Eurojust. The majority of operations carried out by Homeland Security Investigations (HSI) focuses on trade fraud. The presentation underlined the threats to US security posed by IP crime, including transnational money laundering, human trafficking, threats to public safety, and infiltration of the national military supply chain.

A case study was presented which highlighted the huge financial gains made through IPR violations, and the intensely organised structure in which such illicit activities are carried out. It also underlined that the distribution and sale of IPR infringing merchandise is a vessel increasingly
used to move illicit money from one country to another. The case study focused on a Chinese
national who managed to infiltrate the USA via Paraguay, and set up a Miami-based ware-
house business selling counterfeit and substandard, infringing and toxic toy products which
were imported in bulk from China. Through HSI interagency cooperation with Customs and
Border Protection (CBP), the Food and Drug Administration (FDA), Consumer Products Safety
Commission (CPSA) and the right holders affected, an effective operation was carried out which
included undercover purchases, search warrants, affidavits, and the establishment of the re-
commended commercial sale price of products. Computer forensics and forensic accounting
revealed the extent of the criminal, business network which stretched to China and South
America. The OCG had bypassed the US financial system by instructing its clients to transfer
payments totalling USD 3.5 million directly to Chinese banks. Additionally, the OCG had set up a
scheme to simulate that a business loan was being repaid to a Chinese individual – rather than
funds to a company. The network was subsequently charged with a variety of crimes. The main
actor was sentenced to 3 years’ imprisonment and a USD 1.1 million forfeiture (calculated by
the Asset Forfeiture Department) based on the seizure of assets, which included property be-
cause the funds could not be seized from Chinese bank accounts.

Session 2: Videogames Apparatus and Accessories

THE INDUSTRY’S PERSPECTIVE AND CHALLENGES – INTERACTIVE SOFTWARE FEDERATION
OF EUROPE

The Interactive Software Federation of Europe (ISFE) was established in 1998 to represent the
interests of the sector to the EU and international institutions. Initially founded by national
interactive software trade associations in the United Kingdom, France and Germany, ISFE
expanded in 2002 to include any company representing the industry within the Member
States, in addition to Norway, Iceland, Switzerland and Liechtenstein. Today, ISFE membership
comprises 16 major publishers of interactive software and trade associations in 18 countries
throughout Europe. The ISFE has no operational anti-piracy role but lobbies for sound and
practical enforcement of the sector within a robust IP framework.

The interactive software industry, representing publishers and developers of video games, is the
fastest growing sector of the European content industry, with consumer spending estimated at
more than EUR 20 billion in 2015, out of a global market of EUR 68 billion.

The presentation underlined the new forms of piracy designed to exploit cloud based content,
and the emergence of unauthorised private servers. Consumers are also exposed to piracy due
to a reduced diversity and availability of legal offers in some Member States. This renders them
at higher risk of malware infections, of phishing scams to steal account details and funds, and
other cybercrime activities when they access infringing games or are involved in file sharing.
The industry’s reactive and proactive response relies on the ability to develop disruptive technologies and business models, and their use of technological protection measures (TPMs) to prevent the copying and playing of pirated content – and it has served to reduce infringements to a certain degree. However, many piracy models remain robust to enforcement efforts, and many online platforms display agile circumnavigation software. Notably, the financial loss to industry is difficult to calculate in a rapidly changing environment and across many diverse platforms. The software industry, as a whole, does not support suing end users but sends take-down notices in order to deter pirated downloads, and engages in indirect site disruption methods and local content protection programmes. The industry works directly with LEAs including London Police’s Intellectual Property Crime Unit (PIPCU) which is a specialist national police unit dedicated to protecting the UK industries that produce physical goods and online and digital content from intellectual property crime.

Videogame piracy levels have fallen over recent years, and use of technological protection measures (TPMs) and digital rights management (DRM) schemes to restrict usage of proprietary hardware and copyrighted works have played a major role. Additionally, videogame manufacturers use higher levels of encryption. However, the presentation concluded by citing the threat of new infringing business models displayed by the activities of unofficial app stores, which pose new challenges to effective enforcement.

THE INDUSTRY’S PERSPECTIVE AND CHALLENGES – PARADOX INTERACTIVE

Paradox Interactive is a developer and publisher of games, primarily for PCs but increasingly for mobile use, with over 5 million games worldwide. The speaker explained that the development of a single videogame can require up to 4 years’ research in addition to significant investment by the company – including their workforce of 30 developers, a team of lawyers, and a product marketing team.

The presentation focused on the threats posed by IP infringements and unauthorised sales of videogame products, both of which damage the reputation of their brand and result in a loss of sales. Additionally, consumer security can be endangered by malware which is injected in copied games. The presentation highlighted that infringers violate all types of IPR in order to make financial gain - domain names can be pirated, trade marks violated, music can be copied, and copyright infringement of the game theme, style and setting is carried out. To compound the issue and complicate the pursuit of criminal proceedings, if the game is copied but the copy is slightly different - or the primary game does not have many identifiable original features - it is very difficult to prosecute.
The company uses a range of protection efforts including registration of trade marks, within Europe via the EUIPO, and within the US. They also carry out systematic monitoring of online platforms, use the DMCA\(^7\) and pursue take-down notices, make systematic contact with Internet Service Providers (ISPs) regarding suspecting infringing activities, and use online dispute resolution services. The company views unauthorised sales to include sales of physical games including ancillary products, and online copies. Saliently, it is estimated that a fifth of games in the US and Canada are pirated, and an increasing grey market of unauthorised distributors selling games with a heavy discount is evolving.

Many software companies react by limiting the number of resellers and creating a selected distribution system, but this method is less effective with regard to online products. Increasingly, attempts to geoblock and control sale prices are favoured, but this option is not possible in many cases. The presentation concluded by detailing the range of legislative and procedural solutions available including collaboration with Customs regarding enforcement of physical products, pursuing injunctive relief, and final court proceedings. However, the *UsedSoft v Oracle*\(^8\) decision laid down by the EUCJ in C-128/11, which stated that “developers cannot use copyright to prevent the resale of second hand copies of software downloaded from the internet” was considered a detrimental judgment for the industry.

The speaker stated that *Facebook* is responsive to requests for take-down and removal actions, if it can be proven that the IPR is being infringed – but this must be approached on a page by page basis. Europol noted that there have been mixed reports regarding *Facebook’s* response to reports of IPR infringement.

**WORKSHOP 2: “COOPERATION BETWEEN LAW ENFORCEMENT BODIES IN DIFFERENT MEMBER STATES IN A CASE CONCERNING DANGEROUS VIDEOGAME CONTROLLERS”**

All participants were divided into four simultaneous workshops which focused the following questions in order to discuss how interagency and multidisciplinary level cooperation could be enhanced:

---

\(^{7}\) The Digital Millennium Copyright Act (DMCA) criminalises the production and dissemination of technology, devices, or services intended to circumvent measures that control access to copyrighted works. It also criminalises the act of circumventing an access control, whether or not there is actual infringement of copyright itself and heightens the penalties for copyright infringement on the Internet.

\(^{8}\) Judgment of the Court (Grand Chamber) of 3 July 2012; *UsedSoft GmbH v Oracle International Corp.* Legal protection of computer programmes - Marketing of used licences for computer programmes downloaded from the internet - Directive 2009/24/EC - Articles 4(2) and 5(1) - Exhaustion of the distribution right - Concept of lawful acquirer.
EXPLODING CONTROLLERS CASE STUDY

LAW ENFORCEMENT IN COUNTRY A IS INVESTIGATING A CASE OF SERIOUS INJURY OF A CHILD AFTER THE EXPLOSION OF AN UNBRANDED REPLICA OF A CONTROLLER USED FOR A POPULAR GAME CONSOLE.

1. What should Customs authorities of countries A, B, and C do?
2. What should be done to secure evidence, finalise investigations and start criminal proceedings in countries A, B, C, and D?
3. How can right holders support the authorities of countries A, B, C, and D?

The bullet points from the workshop discussions are collated in the Annex to this document.
THE INDUSTRY’S CHALLENGES – NINTENDO

The presenter explained the products developed by Nintendo - namely videogames and videogame consoles - and their aim to target audiences not reached by other videogame companies, including women and younger children. The company has many well-known brands and products including Super Mario, Pokemon and Wii which can be used on portable consoles and via mobile apps.

In order to protect the company’s IPR, Nintendo operates a holistic approach in four main areas – policy, technology, enforcement, and awareness. Technological protection measures are inbuilt by engineers in Japan in order to reduce piracy risks and to reduce the availability of circumvention devices. Nintendo also works to reduce the availability of pirated games files online, and to reduce physical counterfeit products. Hardware piracy is carried out through dedicated e-commerce sites and also through physical stores. Online sellers of pirated products are located by the company via regular monitoring, who are increasingly placing infringing products on platforms including Amazon and eBay. Additionally, internet tutorials on how to hack genuine products are regularly featured on YouTube. The company prioritises the identification of linking websites (peer-to-peer linking) and ones through which pirates gain the highest amounts of profits - including torrent sites. In some Member States, there are effective administrative and civil procedures in place to rapidly take-down or block infringing sites, so that national consumers can no longer view the pirated content. In other countries, it is much more difficult for a rights holder to remove infringing content from the internet.

The company supports public awareness campaigns regarding genuine products, managed through trade associations. It was confirmed that overall, the levels of European IPR infringement have reduced during recent years owing to industry efforts, but also owing to the different trends in console popularity. However, peaks in piracy clearly follow the release of a new type of console.

Europol reminded participants of the success of their joint and ongoing online initiative with ICE (via the National Intellectual Property Rights Coordination Center), called “Operation in Our Sites” which focuses on the take-down of sites offering 100% illegal content.
THE ENFORCEMENT RESPONSE – MALTESE CUSTOMS

Malta is placed in the middle of the Mediterranean, 300km from northern Africa, and the port manages major shipping lines owing to its status as a transit country. The terminal has become steadily larger and currently handles 3.5 million units per year a team of only 230 officers. Customs work daily under tight time and human resources constraints due to rapid cargo turnaround times. Risk analysis tools form the initial basis of surveillance checks in the busy port. Customs officers scan containers based on suspect bills of lading and declared weight information which does not match the description of products.

The presentation focused on the domestic importation of videogames and hardware, and on IPR infringements in transit countries. It highlighted Maltese Customs' effective working relationship with right holders, and highlighted the advantages of rapid right holder cooperation including the production of affidavits concerning genuine and infringing products, especially in cases in which the seized products are of high quality and there are questions regarding their authenticity. Maltese Customs uses the databases of the EUIPO including the EDB and ACIST in order to ascertain certain features of brands and their genuine products, and statistics on seizures.

Notably, if an agreement can be reached between the parties, Maltese Customs will not pursue the simple procedure, but in the absence of such an agreement, their preferred route is to pursue Civil Court proceedings. Under Customs Regulation 608/2013, the right holder is able to pursue a criminal action, and it is common that a Customs' pursued civil judgment is subsequently used by right holders to support their criminal action.

THE ENFORCEMENT RESPONSE REGARDING VIDEOGAMES – CITY OF LONDON POLICE, UK

Funded by the UK IPO, the City of London Police's Intellectual Property Crime Unit (PIPCU) was founded in 2013 and focuses on the protection of UK industries which produce legitimate and high quality physical goods and digital content. The unit is dedicated to tackling serious and organised IP crime (counterfeit and piracy) with a focus on offences committed using online platforms. The unit is based within the Economic Crime Directorate of the City of London Police, which is the National Lead Force for Fraud. There are two dedicated teams - the Disruption Team and the Enforcement Team – the latter of which works closely with stakeholders and in liaison with foreign LEAs. Forensic, cybercrime, surveillance, and financial analysts and researchers support the work of detectives and industry liaison officers.

The Disruption Team focuses on domain suspension, payment service removal, and restricting advertising revenue. Operation Ashiko was set up in 2013 in response to the emergence of IP cybercrime, and in cooperation with Nominet, the official registry for .uk domain names. An
effective MoU (Memorandum of Understanding) is in place to suspend illicit websites within .uk parameters without the need for a court order. Criminals can be charged under the Proceeds of Crime Act (“POCA” - 2002), the Fraud Act (2006), Trade Mark Act (1994), and the Money Laundering Regulation (2007). Analysis of the Financial Information Gateway allows pre-court order financial enquiries on suspects, which can be compounded by arrest and prosecution. Notably, referrals regarding IP crime are increasing each year but the unit must realistically take on cases which are in the Public Interest and of which there is a chance of successful prosecution.

The presentation focused on two case studies and the Enforcement Team's strategies. Operation Finder, a 2016 investigation, targeted the distribution and sale of devices used to circumvent protection technology imbedded in videogames. Infringing products were advertised and sold via eBay, and transported via small consignment packages across the UK. Investigations by PIPCU resulted in the identification and location of the seller, and arrest under the Copyright, Design and Patents Act (1998). A PIPCU banner was placed on the offending website. In the second case, a referral was made from United Kingdom Interactive Entertainment (UKIE) regarding a torrent website which was extensively used for illegal downloads. PIPCU gathered a comprehensive profile package and pursued suspension of the website.

PIPCU works closely with right holders and trade associations in order to raise awareness amongst citizens and industry. Notably, responses from Facebook are inconsistent and PIPCU expressed a wish to develop a closer working relationship with social media platforms.

Europol gave a brief presentation on their Platform for Experts (EPE) which is a secure online platform focused on IP crime, in which members can share non-current operational information, make direct contact with other members, and access training on specific topics including pharmacrime and cybercrime.

Session 3: EU Agencies’ Efforts to Support Enforcers and Right Holders

WHAT CAN EUROJUST DO FOR YOU? - EUROJUST

Eurojust is the EU’s judicial cooperation unit which aims to protect European interests by overcoming operational and procedural delays and conflicts of jurisdiction, owing to the lack of a harmonised substantive and procedure laws across the Member States. Eurojust is able to assist in criminal cases which involve two or more Member States and it aims to solve the difficulties posed to national judicial systems which deal with serious and cross-border crime. In such cases, immediate action is required which, at times, is prevented owing to the disparities in national systems, including the admissibility of evidence. Eurojust works to define a common
strategy of connected investigations and prosecutions, for example, it helps to establish joint investigation teams (JITs).

On a practical level, for example, it also assists in the receipt and execution of Mutual Legal Assistance (MLA) that involves multiple sub-requests which different authorities might be competent to execute. Additionally, there are differences in approach to tracing money, freezing money and assets (especially in relation to non-conviction based freezing orders), money laundering and tax fraud across Europe, and whether a crime is punished as a criminal act - some Member States do not approach dual criminality in the same manner. A lack of common ground makes use of investigative measures including controlled deliveries very difficult.

The presentation illustrated the background of the organisation and explained Eurojust’s competencies and mission, “to support and strengthen coordination and cooperation between national investigating and prosecuting authorities in relation to serious cross border crime affecting two or more Member States. As for the future, according to the Lisbon Treaty, in order to combat crimes affecting the financial interests of the Union, the Council, by means of regulations adopted in accordance with a special legislative procedure, may establish a European Public Prosecutor’s Office from Eurojust”.

Eurojust, seated in The Hague, consists of 28 National Members of the College of Eurojust, seconded by the Member States. The organisation has also been active in negotiating cooperation agreements with Third Countries and other EU agencies, allowing the exchange of judicial information. Agreements have been concluded with, for example, Europol, FRONTEX, OLAF, EMCDDA and EUIPO, as well as states including Norway, Iceland, the USA, Switzerland, and the Former Yugoslav Republic of Macedonia. In addition to cooperation agreements, Eurojust also maintains a network of contact points worldwide. College and national members can act by requesting the authority of a Member State to investigate or prosecute a specific act, following the decision on which state is in a better position to prosecute. It is possible to coordinate their efforts organising coordination meetings via Eurojust, which can also request information from the judicial authorities that should systematically provide reports on criminal acts involving conflict of jurisdiction, controlled deliveries, and repeated refusals of judicial requests when more than two Member States are affected. Importantly, Eurojust informs the competent national authorities and facilitates their cooperation to ensure that Member States inform each other regarding relevant investigations.

Eurojust organises coordination meetings and centres, which offer platforms for strategic and tactical cooperation between the national authorities. Coordination meetings enable national prosecutors and LEA members from each country to discuss cases (supported by translators), to find a commonly agreed solution. Coordination centres help action day activities when
simultaneous operations are carried out in multiple countries. In 2015, 2214 cases have rendered to Eurojust and, 274 coordination meetings took place. Unfortunately, very few involved IPR-related cases, which are usually predicate offences to other priority areas including organised cross-border crime, cybercrime and money laundering. Therefore, the reporting of activities of the national authorities to Eurojust are highly encouraged. These coordination meetings usually involve analysts from Europol. One hundred and twenty Joint Investigation Teams (JITs) were supported by Eurojust during the last 12 months. JITs are considered as a highly effective judicial cooperation tool. JIT members can carry out investigative measures outside their state of origin which enables a rapid and effective investigation and the streamlining of legal and procedural obstacles in transnational cases. In a JIT, in comparison to traditional MLA, there is no lead role and there is a single written agreement between those involved without the need to further supplement the requests for evidence or information exchange. A JIT also allows parallel proceedings during which the evidence gathered in another EU Member State’s territory is subject to mutual recognition. These advantages offer a dynamic solution to the dismantling of OCGs.

WHAT CAN EUROPOL DO FOR YOU? - EUROPOL

A presentation was given on the structure and background of Europol, which is situated in The Hague and employs 900 staff. According to the current EU framework, Europol is the European law enforcement agency which was founded “to support and strengthen action by the competent authorities of the Member States and their mutual cooperation in preventing and combating organised crimes, terrorism and other forms of serious crime”.

In 11 May 2016 owing to EU Regulation 2016/794, the role of Europol was extended to support all European law enforcement agencies (LEAs) including Customs. The national liaison desks act as a link between 28 Member States and enable direct operational communication between LEAs, using information communicated via SIENA and the Liaison Bureaux Network. There are 19 Member States Customs liaison officers in Europol and representatives from the Customs Cooperation Working Party within Focal Point (FP) Copy in order to exchange information.
and to become more effective in intelligence gathering. The incoming regulation will facilitate expansion of the relationships with Customs from each Member State.

Under the Economic Crime Group, FP Copy was created in 2008 and is competent for IPR infringement (except tobacco products). In 2013, FP Copy’s remit was extended to cover the general health and safety threat posed by IP crime via substandard and infringing products. FP Copy involves representation from 20 Member States, 3 non-EU Member States including 3 US agencies (FDA, DEA, ICE), and from Eurojust, OLAF and INTERPOL.

Europol is able to provide onsite support including mobile offices, access to the Europol Analysis System (EAS), technical expertise, forensic pre-analysis, chemical analysis, support regarding dismantling of illicit sites, collation of evidence, and training. They are also able to set up a joint investigation team (JIT) in conjunction with Eurojust. Major initiatives include Operation OPSON on counterfeit and substandard food and beverages; Operation Silver Axe on fake pesticides; and Operation In our Sites (IOS) in cooperation with US agencies and Third Countries including Hong Kong, on illicit internet activity.

The speaker explained the Intellectual Property Crime Coordinated Coalition (IPC3) to the assembled participants, which was established in conjunction with EUIPO in July 2016 to provide technical and operational support to internet crime, to monitor and report emerging online crime and OCG modus operandi, to coordinate cross-border operations, to harmonise and standardise all operational instruments, and to train LEAs in IP crime. IPC3 has 5 specialised IP analysts and 9 IP crime experts. Within IPC3, there is a Stakeholder Advisory Group including private sector representatives, EUIPO and the European Commission as well as academia, in order to maintain multidisciplinary, strategic steering advice with focus on a holistic, “follow the money” approach.

BITCOINS AND VIDEOGAMES – THREAT OR OPPORTUNITY? – EUIPO

The presentation underlined the potential legal and illegal applications of new technologies in relation to Bitcoins, videogames and blockchain technology. It was explained that Bitcoins are a potentially interesting currency for videogames because both exist in entirely virtual environments. Bitcoin forms a decentralised,
encrypted currency which is independent of any bank or central government, and exists via nodes, supported by strong computational power. Every 10 minutes, a new irreversible block containing the most recent transactions is added to the Bitcoin blockchain, whose transactions are entirely transparent and immediate. Notably, everyone who has access to a mobile phone or other internet connected device can install a Bitcoin wallet and is then able to use the currency system, which offers a high level of anonymity and a low transaction fee structure. However, the currency has a history of volatility in regards to the exchange rate between bona fide currencies and Bitcoins.

On a holistic level, blockchain technology offers a system of virtual registration in which ownership of items can be recorded – which has the potential for an immense spectrum of practical legal applications in various sectors including banking, insurance, security, and across industry procedures in general. It can also help industries to reduce resources whilst increasing the transparency of recorded data and transactions. The Observatory has started working with possible future projects concerning blockchain technology and IP, but no decision on future work has yet been taken.

However, alongside progress in technology comes the potential for criminality including the misuse of Bitcoin technology on Darknet. Studies indicate that 50% of activity on Darknet is illegal - most of which involves the illicit sale of pharma goods and narcotics. The largest categories of piracy on Darknet are e-books, databases, pirated software, and stolen or hacked access codes. Some vendors on Darknet are selling pirated and malware infected videogames. The Observatory is currently undertaking a study on malware threats connected to online copyrights infringements in cooperation with Europol and Unicri. Additionally, Bitcoin wallets can be hacked following infection by malware disseminated by way of content sharing.

Darknet market exit scams – in which the administrator of the marketplace steals the Bitcoins in the vendor bonds and in unfinished payments – was introduced. Some market places have now included the use of multi-signature Bitcoin wallets to prevent at least some of these scams. The potential for, and extent of money laundering activities in conjunction with Bitcoin transactions concerning theft of virtual videogame items and gold has been highlighted in a recent research study, “The Cybercriminal Roots of Selling Online Gaming Currency”11 which explains “one of the more popular ways cybercriminals hide or bury their money today is through the sale of online gaming currencies”; the process begins with phishing of access codes, and payments are made through Bitcoin tumblers, which renders the tracking of transactions almost impossible. The EUIPO explained that there are currently a number of start-up companies who are developing tools which can trace Bitcoin transactions to their original source, and which have been used recently in a criminal fraud case.
The presentation concluded with the notion that Bitcoin technology offers many potential benefits for legal markets, but also, potential for abuses.

The floor was opened for discussion and it was noted that although Bitcoin is recognised as a form of currency by the EUCJ in regards to VAT legislation, many national banks do not recognise Bitcoins as a currency as such. Many national banks (including the Hungarian bank) have issued communications detailing its instability and lack of regulation.

It was noted that LEA officers require training on identifying encrypted Bitcoin keys so that they will be able to seize Bitcoins as an asset, and transfer them to a government wallet.

The UK IPO underlined the possibilities of protecting IP via the blockchain, which includes the proof of ownership of content, such as games.

ROUND TABLE DISCUSSION

The floor suggested that practical sessions on cybercrime training would be useful, and it would be beneficial for participants to receive workshop scenarios in advance of the conferences, in order to prepare fully. They also suggested that more detailed training on topics including design rights would benefit participants. They suggested that workshops sessions within conferences could be more effectively facilitated by dividing participants into groups of Customs, prosecutors and police, who report in plenary sessions.

The EUIPO took good note of the suggestions and explained that their intention is to encourage spontaneous answers to the scenarios discussed during the workshops. They added that they have held, and will hold training sessions on Bitcoin, cybercrime and IP online infringements. They held a seminar during 2015 on designs, but noted that they could repeat the event in future.

Eurojust reminded the floor of their reliance on Member States’ communication in order to be able to effectively support them via the coordination of transnational operations.

CONCLUSIONS AND CLOSURE OF THE SEMINAR

The floor expressed their thanks to the EUIPO, Eurojust and Europol for organising and hosting the knowledge building conference. The Deputy Director of the Observatory praised the close working relationship between the three organisations and thanked all participants for their contributions. He underlined one of the major aims of the seminar, which was to consolidate relationships between participating enforcement bodies and the private sector. He
explained that it is important to link the knowledge building events with research carried out by the Observatory, including the study into online infringing business models and the sectorial studies, in order to achieve concrete results. He concluded by underlining that the knowledge building conferences have followed a sectorial approach to date, and suggested that future conference topics could include cooperation with Third Countries. The event was closed.
Workshop 1: Effective Law Enforcement Response in a Case Concerning Non-Original Toys and Pirated Videogames

All participants were divided into four simultaneous workshops which focused the following questions in order to discuss how interagency and multidisciplinary level cooperation could be enhanced:

“BENDING BANANAZ” CASE STUDY

1. What are the possible options for reaction to IPR infringement threats?
2. How can cooperation between involved agencies best be established?
3. What are the obstacles to effective action?

Question 1

- A simple initial option would be a written notice to the supplier rather than pursuit of the judicial process.

- The advertising of malware offers options to take down the website or target the adverts through a national Advertising Standards body to get it removed, thus taking away funds derived from the advertising that support the website. The UK can do this by placing the site on the U.K. infringing website list, which is a voluntary option established by the industry. Denmark’s normal practice is to take down infringing websites and investigate the implicated parties.

- It is vital to confirm the ID of the owner of the website and/or use a “follow the money” approach to follow up who is benefitting from the infringement; this information is vital in both criminal and civil proceedings.

- There are specialised units including cybercrime units in different Member States which are able to deal with online infringement cases.

- It was noted that a case focusing on organised crime activities would allow for additional means of investigation.
Customs are able to check physical goods on entry, to check that AFAs have been filed, or approach the case \textit{ex officio}. On basis of EU Regulation 608/2013 they are able to destroy counterfeit products. In some countries, such as Norway, Customs can initiate laboratory checks if the seized products contain heavy metals. Customs can also carry out controlled deliveries to gather information, such as locating the actors involved, who could be resident in multiple jurisdictions.

Once grounds for a criminal case a has been established, investigative means such as phone tapping and tracing the money flow will assist in mapping the landscape of the actors involved. In Denmark, it is possible to obtain a digital search warrant. Criminal activities can be tracked through digital anti-virus software barcodes.

Danish enforcement would initially use online tools including COPIS and the Enforcement Database (EDB) to investigate whether similar imports had occurred in other Member States, and in order to support subsequent cross-border efforts.

Seizure could occur, test purchases could be carried out, and an investigation to identify and locate online sellers and distributors should be carried out immediately. However, if the online distributor or seller of malware cannot be identified, or is located in another country, this poses tangible obstacles to prosecution. Ransomware criminals could be charged with extortion in Denmark. In the Czech Republic, the Budapest Convention allows prosecution of a cybercrime offence in the absence of evidence regarding physical products. The UK suggested locating consumers who have made electronic payments in return for release via ransomware, to build grounds around financial gains made by the actors, and search warrants could be ordered to locate the criminals’ computers.

Question 2

The working groups discussed ways to augment cooperation between agencies by involving authorities including Eurojust, Europol, OLAF and Interpol to establish joint investigation teams (JITs) whose resources are especially useful in cybercrime cases.

It was agreed that it is important to use the evidence gathered in the best manner, in terms of mutual legal assistance (MLA) orders and in order to present a comprehensive file to the prosecution.

In response to the fictitious case presented, the group agreed that the case should be approached on a holistic level to achieve a collaborative process of communication. They highlighted the need to increase levels of communication on a national level.
A main conclusion highlighted that IPR infringement should be viewed as part of a wider problem including human and drug trafficking activities, and investment into other crimes.

Groups discussed collaboration with stakeholders including trade bodies to assist in building intelligence and sufficient evidence, including intelligence regarding cases from other countries, and trends in Europe. For example, the International Anticounterfeiting Coalition (IACC) can assist with experts and rights holders’ ID.

The “follow the money” approach was highlighted as a vital route to pursue in a cybercrime case, because it facilitates the identification of the actors involved and allows the consolidation of evidence necessary for prosecution, subsequent to tracing payments.

Enforcement requires a system which enables different agencies to communicate effectively with each other, prior to the Public Prosecutor coordinating a procedure.

Fundamentally, cybercrime cases require expert training and involvement, and the establishment of national, specialised units. These could be supported by the resources and expertise of Europol and Eurojust when national structures or coordination is unavailable.

The group underlined the need for cooperation with the private sector in order to progress from the initial stages of an investigation. French Customs underlined that action from the outset requires strong cooperation with brand owners - who must comprehensively detail their copyright and actively pursue proceedings in cooperation with LEAs. Customs could create alerts regarding export routes, and set up risk profiles regarding similar shipments.

It was agreed that the easiest route to successful prosecution should be followed.

Hungary suggested the pursuit of a criminal action, if attempts had proven unsuccessful via the initial civil route. In Italy, the police would focus on counterfeiting via the criminal route; the Public Prosecutor is obliged to open an investigation. In the UK, the police would focus on removal of the counterfeit items followed by take-down of internet advertising. In cases which pose a threat to public health, removal of products from the market would be the focus of action – which would avoid the judicial route.

The group agreed that it is paramount to remove the generation of funds made from advertising, which supports the existence of an infringing website and is the basis for criminal activity.
It was agreed that it would be prudent to establish trend in imports and sales, to set up MOUs with various partners including online advertisers and with bodies including the International Anti-Counterfeiting Coalition (IACC).

USA underlined the efforts of right holders who carry out undercover purchases, which help to identify importers and sellers. The “follow the money” approach was also advocated by PIPCU who underlined the importance of tracing activities back to online sellers.

The UK IPO carries out an analysis of all border detentions through information provided by Customs, and this cooperation has been very useful. They underlined that it is imperative that different agencies communicate and cooperate. They also indicated that an intermediate agency can act between agencies in order to collect the necessary information to address this problem.

Portugal suggested the creation of risk profiles and the dissemination of his information across Member States agencies.

**Question 3**

Participants underlined the obstacles to working on a cross-jurisdiction case, especially when online sales are carried out by actors and proxy servers based in multiple Member States. Additionally, domain names can be registered by criminals in Third Countries with which LEAs find difficult to contact and secure cooperation.

 Attempts to seize bank accounts in non-EU countries is fundamentally impossible.

 Tracing Bitcoin payments is possible but it is difficult to identify to whom the money is paid. Generally, it is easier to identify larger Bitcoin transactions, which are more clearly visible.

 The groups noted differences in powers and procedures in each Member State; Applications for Action (AFAs) allow intervention, but in reality, practices differ greatly regarding seizures of lesser amounts of products. Some countries use seizures to proceed to a criminal investigation whilst in some countries, prosecution depend on the value of the goods, the amount detected, and potential links to further illegal sales.

 The general obstacles to communication were discussed – there is no legislative framework in some Member States to inform another authority about the discovery of counterfeit products.
The potential for a lack of cooperation at national level, owing to various threads involved in an IPR case were highlighted (IPR infringement, cybercrime, financial crime, human trafficking). In general, it was noted that cooperation is difficult to achieve between so many agencies, in practice.

A general lack of priority at national level regarding IPR crime was noted.

Fundamental practical obstacles in the case were discussed, such as a party pursuing a copyright claim or pursuing an AFA could be a licensee, but is not the owner. (In terms of videogames software, this issue is avoided because the companies are the owners, not individual creators). EU legislation on unregistered designs would offer protection for up to 3 years from creation in the case at hand, depending on the strength of evidence which could be gathered on either copyright or design violation, and depending on the Member State involved. In the UK, it is necessary to obtain a full statement package by the copyright owner to proceed in initial stages of proceedings.

The Greek Prosecution highlighted problems in communication between the different authorities involved, including police, Customs and other agencies - as well as with right holders.

A general lack of expertise regarding specific, infringed products results in a lack of evidence in many Member States.

Seizure thresholds differ across Member States and pose an obstacle to effective investigations.

Denmark explained that if 100% of the goods on infringing websites are counterfeits, a court order can be pursued. However, if a website sells both counterfeits and originals, they cannot act.

There is a general lack of synergy between agencies in different Member States.

Some groups reported that there is an adequate level of cooperation between authorities on a national level. However, Belgium explained that there is a lack of protocol regarding information flow across agencies; in general, there exists only unofficial communication across services.

Slovenia explained that the fictitious case is related to both IPR infringement and cybercrime, and the latter aspect is more complicated. There is a lack of knowledge and expertise regarding online infringements.
Serbia underlined that prosecutors are generally involved in larger crimes. Furthermore, and owing to elevated costs of procedures, Customs will not contact prosecutors with respect to small quantities.

If the right holder does not support or provide evidence of the infringement, this frustrates enforcement’s efforts.

Accessing domain registrations in uncooperative countries is in practice, unproductive.

Joining the dots in reality can be difficult - especially with regard to smaller seizures - but needs to be achieved to map the bigger picture.

It was discussed that current legislation does not give Customs the power to demand information from economic operators regarding where they bought the goods from. Additionally, the penalties are very modest in general. The group suggested the creation of an inventory across Member States to compare fines. Furthermore, the legislation does not give Customs the power to easily communicate and share information with other Member States.

Belgian Customs stated that the penalties in infringement cases are very modest, and that very few cases progress to court.

Croatia added that criminal procedures are limited in light of the elevated costs.

It was discussed that the police do not prioritise IP, because focus is generally placed on terrorism and gun crime.

The workshops also referred to political problems and competition across national agencies and bodies.

Working groups indicated the lack of a common, European database which renders it impossible to share information across agencies.

Workshops Day 2

All participants were divided into four simultaneous workshops which focused the following questions in order to discuss how interagency and multidisciplinary level cooperation could be enhanced:
Exploding Controllers Case Study

Law enforcement in country A is investigating a case of serious injury of a child after the explosion of an unbranded replica of a controller used for a popular game console.

1. What should Customs authorities of countries A, B, and C do?
2. What should be done to secure evidence, finalise investigations and start criminal proceedings in countries A, B, C, and D?
3. How can right holders support the authorities of countries A, B, C, and D?

Question 1

- Country A should inform other countries using the Rapid Information System (RIS) depending on the gravity of situation, and assess the response from other countries.

- Different options and procedures established in different Member States, with varied resources to tackle the problem would determine whether the case would focus solely on IP or whether the investigation would have a wider remit, based on product safety.

- It was agreed that Customs’ main focus would be to locate other shipments in order to manage risk and to stop infiltration into the European market. Customs would decide between a standard procedure or an ex officio procedure depending on whether an IPR infringement is found and an AFA has been filed by the right holder.

- Counterfeit video controllers are often found in small numbers in postal packages by Customs, generally displaying trade mark and design infringements. Maltese and French Customs explained that they would focus on IPR violations at the initial stages of investigation. French Customs reported huge quantities of fake videogames sold via discount stores, transported via shipping containers or via frequently sent small consignments.

- Montenegro emphasised that they would focus on design infringement (considering that the controller in the fictitious case presented does not include a label). In order to check whether it was protected, they would contact the general distributor of the original goods. In ex officio cases, they also contact the IPR office as a first step. In Denmark, the police, prosecutors, the IP Office, and Customs cooperate. Involving the IP Office from the outset is especially useful when it is unclear whether a product is counterfeit. Belgian Customs would check if there were previous, similar products imported from the same importer, and check the ship’s manifest the container to identify any similarities in other consignments. Latvia and Belgium indicated that in case they encountered a separate container which included
labels, they would also seize the labels: they emphasised that labels must be considered as part of a product. Lithuania and Montenegro gave examples of consignments sent with pressing machines, and labels of multiple brands sent separately – which highlights infringers’ aims to avoid detection and prosecution.

The UK and Hungarian Prosecution suggested that consumers who have already received the products should be contacted immediately owing to the danger risks, via the media. However, this would alert the criminals involved and possibly help them to avoid detection. This method of action could be executed simultaneously with premises searches and other investigative actions; a rapid response in this case would be vital. It was agreed that in cases which threaten public health, consumer safety would take priority over sensitivities regarding brand reputation.

Cooperation of the IPR holder, Customs, police and the prosecution is necessary in all complex cases – in short, a multidisciplinary approach must be secured.

It was agreed that use of COPIS and EDB would enable other countries to access vital data regarding infringed goods and associated product details, and countries of provenance.

It was noted that Customs’ objectives, police objectives and right holder objectives are often different and at times, non-complementary – the first group focuses on seizures, the second group focuses on pursuing the criminals involved and dismantling their (potentially transnational) *modus operandi*, and the third group focuses on protection of their brand, including avoidance of the occurrence being publicised. It was asked, how to marry the three approaches? The group agreed that Customs would try to stop the products entering the EU market; police would try to rapidly locate the actors involved in order to prevent future activities; whilst the right holder may initiate court proceedings from the outset - which would avoid the standard Customs procedure.

**Question 2**

A primary discussion focused on who has the competence to decide where to direct the case, and who to involve. Lithuania emphasised that it is important to decide on a coordinator for each case at an early stage.

The Naples II Convention was discussed, regarding mutual assistance and cooperation between Customs administrations.

EUROPOL suggested that the EDB be used by the enforcement officials concerned in order to identify original versus counterfeit products.
Sweden explained that if it is an infringement case, the shipment must be stopped in country C, but this poses problems because the products are unbranded. Collaboration from the private sector is needed to confirm that an infringement has occurred.

It was suggested to involve police trained in cybercrime in country B, or to carry out local investigations in country D.

Police in one Member State should communicate with police in another State, regarding injury and criminal negligence, which may elicit a JIT - but it was discussed that a JIT is primarily a judicial instrument rather than an investigative one.

Europol and Interpol should be contacted in order to inform provenance countries’ authorities via official channels, so that criminal cases can be initiated. Customs Regulation 608/2013 provides for the information gathered from right holders to be used for the specific purpose of the provision of information to other countries. However, it was noted that different countries have different protocol regarding the spontaneous sharing of information with Third Countries including China.

Participants discussed the importance to harvest all the different resources available on a national and international level, and the ways in which Customs, police, market surveillance, and the prosecution could more effectively communicate and cooperate with each other. Lithuania and the UK underlined that it is important to prove to a judge that the child’s injuries are attributed to the faulty and infringed controller. They stressed, however, that it is hard to prove the intention of the importer and whether he was aware of the health hazards of the product imported. Consequently, if more information is available regarding the entire supply chain, the easier is the prosecution.

Italy cooperates with companies in order to analyse the products and examine their safety. They explained a case of Barbie dolls that were imported from China, which included dangerous substances in the paint. However, the only action that was taken was seizure of the toys, and imposing a trivial penalty.

In the UK, prosecutors focus on the most serious offence involved in a case, and not the various offences involved.

The Maltese Police would target the IP aspect of a case, but other authorities would look into safety issues. Consequently, the case taken to court could include both IP and safety aspects.
Portugal emphasised that when issues are not of a political priority, information is not shared across the relevant agencies.

It was emphasised that a major challenge is the elevated financial costs of running an analysis on products.

It was agreed that the RAPEX system should be used in more cases.

There was a discussion in one group regarding products which are not branded, and possibilities to pursue other IPR violations, and product safety breaches. National laws and procedures provide options and autonomy in some countries, and pose obstacles in other countries.

The discovery of physical goods infringing IPR and substandard goods does not necessarily link easily into a cybercrime investigation, which uses very different techniques and requires the support of other enforcement bodies. The Italian Police underlined the difficulties posed regarding locating information on unknown ISPs and servers.

The need to improve sharing of information on a regular and systematic basis by LEAs – and by right holders who often garner very accurate and complete intelligence – is a main aspect to be addressed.

The Irish Police suggested that there would be simultaneous actions in multiple countries, including the possibility of criminal proceedings and the establishment of Joint Investigative teams (JITs). It was agreed that it is important to use the resources of European bodies including Eurojust and Europol owing to the different legislation and procedures in place in different Member States, including Mutual Legal Assistance (MLA). An expert cybercrime response could be facilitated by Europol.

The group concluded that other aspects must be considered in a complex case, including tax evasion, health and safety violations, and dangerous and substandard breaches – which would require involvement by various agencies and stakeholders.

Question 3

The involvement of rights holders is crucial for the success of pursuing a case, via both the civil and criminal routes. In the USA, authorities can use right holders’ information to support a criminal case.
Right holders have specialised knowledge concerning the products, and in some cases, possess specialised labs in which material can be analysed but it depends on each Member State, whether they can take part in a forensic investigation. They can provide training to LEAs regarding product specificities in order to help to identify infringing items at border entry points.

A question was raised whether the right holder can be asked to trigger international cooperation by sharing information they have on similar cases in other countries.

Protecting rights for smaller companies largely unknown by Customs proves more difficult, and underlines the need for Customs’ training by right holders.

It is important to ascertain whether the same OCG is behind the production and distribution of similar infringing goods which have been discovered. In order to secure evidence, it is also important to gather information on financial transactions by using forensic experts and cybercrime experts. Samples and photographic evidence from the right holder would effectively support a criminal investigation.

The need to raise levels of public awareness was highlighted, which could be assisted by brand owners.