UNCOVERING THE ECOSYSTEM OF INTELLECTUAL PROPERTY CRIME

A focus on enablers and impact

A joint EUIPO-Europol strategic analysis report produced under EMPACT - October 2024

EMPACT

Catalogue number: TB-01-24-002-EN-N ISBN: 978-92-9156-365-4 DOI:10.2814/1947113

Your feedback matters

By clicking on the following link or scanning the embedded QR code you can fill in a short user survey on this strategic report.

Your input will help us further improve our products.

https://ec.europa.eu/eusurvey/runner/eus_strategic_reports

Table of contents

Foreword by the Executive Directors

Catherine De Bolle

Executive Director of Europol

João Negrão

Executive Director of the EU Intellectual Property Office (EUIPO)

Intellectual property lies at the heart of creativity and economic growth. It fuels our economies, our societies and drives innovation. Protecting intellectual property rights ensures that those who created and drive our society forward are rewarded and fosters an environment of development and progress. However, also intellectual property is vulnerable to criminal networks. This report confirms that counterfeiting remains an enduring challenge, with criminal networks often 'pulling the strings' and benefiting financially.

Therefore, this report prepared by EUIPO and Europol once again puts the spotlight on the complexity of the ecosystem of intellectual property crime. It sheds a light on how criminal networks systematically thrive on opportunities of advanced technologies, globalisation and digital interconnection, facilitated by a sustained demand for counterfeit goods.

Understanding the enablers of IP crime is essential to combatting this threat effectively. By identifying the technologies, networks, and systems that facilitate these illicit activities, we can develop strategies to prevent IP crime and dismantle the criminal processes behind it. This report offers a detailed examination of the enablers of IP crime and the various methods that criminals employ to evade detection and enforcement.

Looking forward, it is crucial that we adopt a multi-faceted approach in addressing the future threats posed by intellectual property crime. This requires fostering collaboration between law enforcement, policymakers, the private sector, and the public. Intelligence sharing, especially on evolving enablers, must become a cornerstone of our enforcement efforts.

Both EUIPO and Europol, in particular the European Financial and Economic Crime Centre (EFECC), play a crucial role in the protection of intellectual property rights and fighting those networks harming these rights. Only by working together we can safeguard innovation, protect consumers, and maintain the integrity of our economies and societies.

We are confident that this report will be a vital tool in shaping our fight against intellectual property crime and strengthening our defences against those who aim to exploit it.

Introduction

Intellectual property (IP) crime refers to the theft, infringement and unauthorised use of intellectual property ([1]) such as copyrights, designs, trademarks, patents, and geographical indications of origin, and crimes related to trade secrets. Common types of IP crime include counterfeiting (the manufacture, importation, distribution, storage and sale of goods that falsely carry the trademark of a genuine brand without permission) and piracy (the unauthorised copying, use, reproduction, and distribution of materials protected by intellectual property rights).

IP crime continues to pose a threat to the EU's internal security ([2]). The harm produced by IP crime is more significant than it appears at first sight. Not only because of its adverse economic effects, but especially in terms of impact on consumers' health and safety, and on the EU's natural environment. Criminal actors operating in IP crime are very adept at exploiting opportunities and loopholes, posing challenges to right holders, law enforcement and other relevant authorities.

The scale of crime remains considerable. In 2022, approximately 86 million fake items were seized in the EU, with an estimated value exceeding EUR 2 billion. The most common products seized were games ([3]), packaging materials, toys, cigarettes, and recorded CDs/DVDs. 60 % of the goods were detained within the EU, and 40 % at the EU's borders ([4]). The illegal trade in counterfeit goods was estimated to represent 5.8% of imports to the EU ([5]).

IP crime thrives because it fulfils a worldwide demand for low-priced goods, which is satisfied by criminal actors and networks operating across continents. Despite prevention campaigns to expose the health and safety dangers of purchasing and consuming counterfeit goods, besides the severe consequences for the industries and companies targeted, counterfeiting keeps appealing to or misleading consumers.

IP crime entails a complex criminal process involving multiple steps and various actors. The infringement of intellectual property rights is only the initial stage of IP crime, as the final objective of counterfeiters is to profit as much as possible from the subsequent illicit sale of the fake goods introduced into the consumers' market. IP crime relies on a multitude of enablers that make this criminal activity particularly successful and at the same time difficult to tackle. These enabling factors can be crimes in themselves, but can also be lawful activities misused for facilitating IP crime.

This report explores the ecosystem of IP crime and its interactions with developments in our society. At the core of the report is a description of the criminal process by which the various types of IP crime are committed and the steps it entails. It assesses which key catalysts in today's EU and global society drive IP crime, making it an area of opportunity for criminal actors. It zooms in on those factors – be they criminal acts or lawful activity misused for criminal purposes – that enable IP crime. At the same time, it considers how IP crime can function as an enabler of other serious and organised crimes. Ultimately, it describes IP crime's harmful impact on EU citizens and businesses.

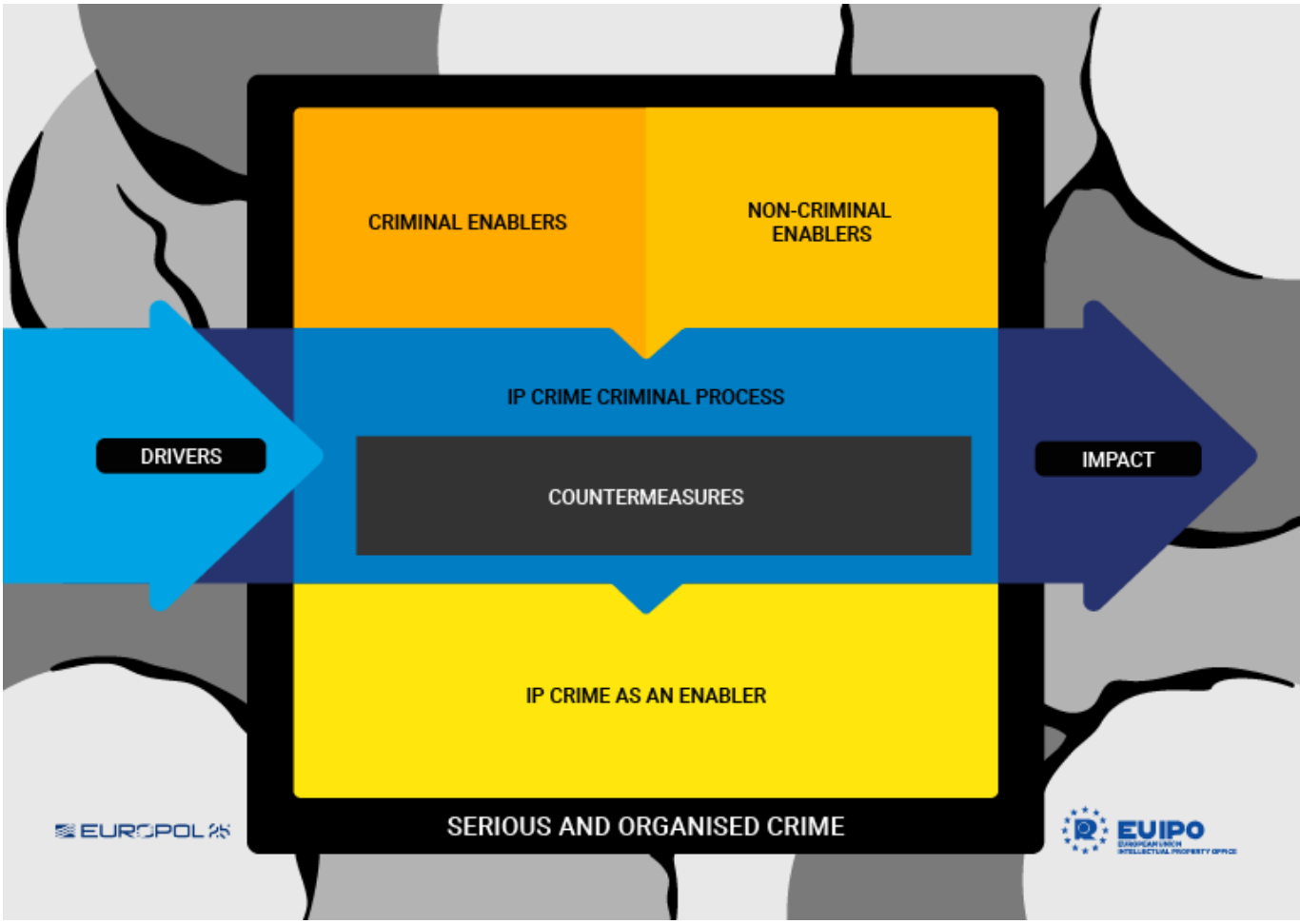

Figure 1. The complex ecosystem of IP crime, its interactions and impact

This report uses operational data from investigations contributed to Europol. The EUIPO has also collected contributions by the private sector. Case examples are used throughout the report as illustrations. Where relevant, open-source intelligence has been used to corroborate analytical findings.

The focus on enablers invites law enforcement authorities (LEAs), legislators, relevant stakeholders and the public to work even more closely to reduce the harm of IP crime and identify the criminals behind it. A cohesive response by all stakeholders, both within and outside the EU, is a prerequisite toward the detection and dismantling of the criminal networks involved.

AN EMPACT DELIVERABLE

This report is a deliverable in the EMPACT Operational Action Plan to tackle Intellectual Property Crime, Counterfeiting of Goods and Currencies.

EMPACT stands for the European Multidisciplinary Platform Against Criminal Threats. It introduces an integrated approach to EU internal security, involving measures that range from external border controls, police, customs and judicial cooperation to information management, innovation, training, prevention and the external dimension of internal security, as well as public-private partnerships where appropriate.

EMPACT has a clear methodology for setting, implementing and evaluating priorities in the fight against organised and serious international crime. It aims to tackle the most important threats posed to the EU in a coherent, methodological way by improving and strengthening cooperation between the relevant services of the Member States, EU institutions and EU agencies, as well as third-party countries and organisations, including the private sector where relevant.

More information is available at https://www.europol.europa.eu/crime-areas-and-statistics/empact and at https://home-affairs.ec.europa.eu/policies/law-enforcement-cooperation/empact-fighting-crime-together_en.

Key Findings

- **Intellectual property (IP) crime remains a consistent threat to the EU due to its scale, demand and impact.** Billions of euros in seizures occur in the EU annually. High demand, profit potential and low risk attract criminal networks, resulting in harming the economy, citizens' health and safety, and the natural environment.

- **IP crime functions as a complex ecosystem in which criminal and abused legal aspects are intertwined.** It operates in a global environment where both illicit and licit enablers support (parts of) the criminal process, while IP crime in itself also facilitates other types of crimes.

- **Criminal networks involved in IP crime evolve with new technologies and societal changes, including demand.** The rise of social media, influencers and online commerce have changed consumers' behaviour, increasing their appetite for IP infringing goods or content, while having a low awareness of risks. In addition, a global trade characterised by interconnected infrastructures, both offline and online, drives further opportunities for global actors in IP crime.

- **There is a narrow link between IP crime and other types of organised crime which function as enablers.** These include document fraud, corruption, labour exploitation, environmental crime, cybercrime and money laundering. Some crimes facilitate the complete criminal process of IP crime. In its turn, IP crime also enables some criminal activities, such as cybercrime, VAT and excise fraud, fraudulent schemes, environmental crimes and money laundering.

- **Legal business structures and the expertise they hold, are directly interconnected with IP crime and misused by criminal networks throughout the criminal process.** At the same time, established and new technologies like 3D printing and AI-driven marketing also play a role in aiding IP crime.

- The IP crime ecosystem is intricate, and with actors often active outside the EU, information on **some enablers** of IP crime, and on IP crime as an enabler, **is often partial or unavailable.**

Part I: Drivers, process, and impact of IP crime: Unveiling the mechanics and consequences of IP crime

This chapter explores some of the underlying forces driving intellectual property (IP) crime, the processes criminals use, and the broader impacts, especially in the context of modern technology and global developments.

Catalysts of change: key drivers fuelling developments in IP crime

IP crime is a type of organised crime that is closely interlinked with developments in our world and that caters to citizens' needs and desires. The key driving forces fuelling developments in IP crime nowadays are shaped by technological, economic and social trends, or a combination of these.

The transformation of consumer behaviour linked to the expansion of e-commerce drives an increased demand for low-priced goods, fuelling IP crime. Moreover, relatively low penalties for the perpetrators of IP crimes serve as powerful incentives and make it a low-risk, high-benefit criminal activity.

Digital acceleration and the role of social commerce

Social media has revolutionised online communication. In 2023, almost two out of three EU citizens had an account on the mainstream social media platforms ([6]). On average, each EU citizen spends 1 hour and 48 minutes per day on social media ([7]). In this context, social commerce emerged as a key platform from which counterfeiters could attract consumers ([8]).

Social media platforms continue to invest in technology through machine learning and artificial intelligence (AI) to reach users with customised ads that address their personal interests and preferences. Automation is also used to review and remove posts and ads, after the detection of terms and conditions breaches, usually based on suspicions concerning brand names, logos, prices, discounts, and other indicators.

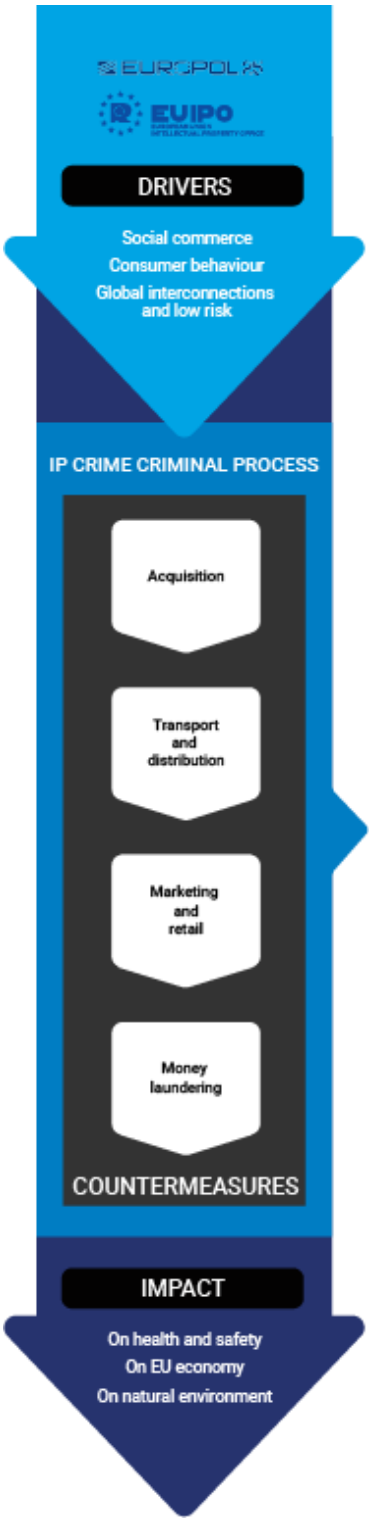

Figure 2.: How drivers, the IP crime criminal process, and its impact intertwine

The key driving forces fuelling developments in IP crime nowadays are shaped by technological, economic and social trends, or a combination of these.

In the world of social commerce, influencers play a critical role in spreading adverts and promoting brands on both end-to-end encryption (E2EE) applications and social media platforms. Through their channels, influencers may direct customers to product listings on online stores that evade security protocols about counterfeit adverts. Despite social media terms and conditions, which include strict policies against users posting illicit content featuring counterfeit goods, they often endorse counterfeit goods alongside genuine brands. Social media influencers target high numbers of relatively young consumers, who are likely to purchase counterfeit products due to their trust in influencers combined with their low-risk awareness, high risk appetite, and tendency to rationalise counterfeit goods purchases ([9]).

In the context of pharma crime, social media influencers who endorse and promote counterfeits (often knowingly) as well as genuine brands through their own 'dietary and nutrition' channels, are becoming a major marketing vehicle for pharmaceutical substances ([10]).

CASE EXAMPLE: CRIMINAL NETWORK USES INFLUENCERS TO MARKET ILLICIT HORMONAL SUBSTANCES

CRIME: IP crime – Pharma crime | IMPACT: consumer health and safety

A criminal network, dismantled in 2023, produced and distributed illegal pharmaceuticals and anabolic steroids across the EU using popular social media influencers to promote the fake performance-enhancing substances. Network members had close ties with gymnasiums in Romania, which the networks supplied with the illegal goods. Amongst their clients were social media influencers with popular dietary and nutrition channels. One clandestine laboratory was dismantled, with over 1 million pills found at the production site ([11]).

Figure 3: Clandestine laboratory for illicit hormonal substances marketed via influencers (Source: Europol with Moldovan and Romanian police)

Analysis of social media usage also reveals how widespread users' interest in IP-infringing products is – with a significant share of social media conversations potentially related to counterfeit goods (particularly clothing, footwear and jewellery) or to digital piracy of e-books, TV shows, and music ([12]).

Counterfeiters exploit peak sale seasons (e.g., sporting events, Black Friday, Cyber Monday, and holidays) to increase their presence (particularly through online ads), sales and profit. This is particularly relevant in the case of clothing, sportswear, electronics, and toys ([13]).

High consumer demand and limited consumer awareness

In the current cost-of-living crisis, and further fuelled by the developments in social commerce (see above), counterfeit goods and piracy are in high demand with consumers. Consumers often still lack awareness of the actual dangers that counterfeit goods may pose to their health and safety, or the consequences of counterfeiting and piracy on the economic system (see also the section on 'The impact of IP crime' below). They may simply be unaware of the fact of purchasing a counterfeit product and are lured by low prices, without considering the quality. For this reason, prevention campaigns to inform the general public remain relevant ([14]).

In parallel, this high demand presents profit incentives to criminal networks, who see opportunities to obtain high illicit proceeds with limited investment and risk.

CASE EXAMPLE: COUNTERFEIT OLIVE OIL

CRIME: IP crime, food fraud | IMPACT: consumer health and safety, economy

In 2023, an investigation into counterfeit olive oil revealed that a criminal network had used so-called 'lampante oil', a lower-quality variant of olive oil, to dilute their product. Lampante oil is of inferior quality, with an acidity of more than 2 % and no fruity characteristics or substantial sensory defects. It is not intended for marketing on the retail market, but rather refined or used for industrial purposes. More than 260 000 litres of olive oil unfit for consumption were seized.

A mix of various factors, such as the general inflation of prices, reduced olive oil production, and increasing demand, have created the perfect breeding ground for fraudulent producers. Mixing consumer-grade olive oil with lower-grade alternatives allowed the criminals to offer competitive prices while infiltrating legal supply chains. This illegal practice caused a public health risk, and can undermine consumer trust, thus entailing further economic repercussions ([15]).

Global interconnections drive global crime and reduce risks for organised crime

The interconnected nature of global trade provides opportunities to insert counterfeit goods into the legal supply chain, conceal counterfeit products (or parts of them), and disguise their origins.

Being engaged in what is inherently a cross-border criminal activity, counterfeiters exploit the differences among legal frameworks and jurisdictions. They carefully assess which countries have less strict IP crime legislation and locate the relevant steps of the criminal process there, whether production, assembly or distribution.

CASE EXAMPLE: A GLOBALLY CONNECTED CRIMINAL NETWORK

CRIME: IP crime – commodity counterfeiting, money laundering | IMPACT: consumer health and safety, economy

A Senegalese criminal network was settled in Spain and involved in the import and sale of counterfeits from China, masking the illegal origin of the profits in order to integrate them into the legal economic and financial systems, both in Spain and in third countries, including Senegal. The leader of the organisation had managed to obtain a Chinese residence permit, which made it easier for her to contact the suppliers of clothing and other counterfeit goods in China directly ([16]).

In the context of online distribution and sale, the abuse of loopholes in marketplaces' terms and conditions and the ability of online service providers (OSPs) to identify illicit content both drive initiatives by counterfeiters.

CASE EXAMPLE: OPERATION HEXAGONAL

Crime: IP crime – digital piracy | Impact: financial

Between 2020 and 2023, the Irish authorities, supported by Lebanon and Europol, investigated an illicit streaming service (ISS) run by a Lebanese suspect and his Irish associate, operating through a website as supplier of wholesale streaming content protected by copyright such as sport events, movies but also TV channels from several countries. The individuals collected criminal proceeds in joint Irish bank accounts, which amounted to EUR 750 000 ([17]).

A key EU instrument to counter online threats is the EU Digital Service Act, which entered into force on 17 February 2024 ([18]). This EU Regulation aims to provide a safer experience for everyone within the online ecosystem by prompting digital services operating in the EU to improve transparency and accountability. The DSA is addressed to online platforms, search engines, hosting services, and intermediary services offering network infrastructure, and it sets out a number of ways to counter illegal content, goods and services. These include, amongst others, the obligation upon online marketplaces to improve their KYC practices, and the introduction of a system of trusted flaggers for counterfeit and unsafe goods, thus, also improving the protection of brands and consumers.

The scope of IP crime and applicable sanctions regimes differ significantly across the EU Member States. This potentially serves as a pull-factor for criminals to set up (part) of the criminal process in the countries with lower sentencing. Nevertheless, a majority of EU Member States consider IP crime a serious crime and align maximum years of imprisonment accordingly, exceeding four years of imprisonment ([19]).

The European Commission recommendation of 19 March 2024 on measures to combat counterfeiting and enhance the enforcement of IP rights encouraged EU MS to review their national criminal measures in order to ensure adequate criminal measures are in place, especially for trademark counterfeiting and copyright piracy, by considering the principle of proportionality of the penalty to the crime ([20]).

The mechanics of IP crime: breaking down the criminal process

The criminal process refers to the sequence of steps that allow a crime to materialise. By dividing the actions involved in the commission of an IP crime into different steps, it becomes easier to take in the full ecosystem of IP crime, and what facilitates each of these steps.

> IP criminals know how to exploit the weak links in global supply chain and to abuse varying legislative frameworks, especially when the process involves multiple jurisdictions, importers, retailers and distributors

Criminal actors involved in the trade in counterfeit goods in the EU operate in a networked environment, where cooperation is fluid and resembles legitimate business structures. Associates are allocated to the various steps of the process and are spread across the operational route. IP criminals know how to exploit the weak links in global supply chains and to abuse differing legislative frameworks, especially when the process involves multiple jurisdictions, importers, retailers and distributors ([21]). As most of the counterfeit commodities traded within the EU originate from abroad, the detection of full criminal networks is challenging. Combined with the shift to online

distribution, the distance between criminals and their commodities has become even larger.

The masterminds behind the trade in counterfeit goods in the EU are often located outside the EU and rely on intermediaries, either internal or outsourced, who ensure the smooth running of the criminal process while providing the leadership with a shield to cover the upstream part of the chain. The engagement of crime-as-a-service providers is common ([22]).

These actors are key players within a structured ecosystem, characterised by a decision-making hub and multiple levels. They utilise intermediaries or subcontractors, either to perform a hierarchical function or to facilitate substitution across the network, ensuring the continuity. This structure provides operational autonomy and resilience to the criminal process, making it challenging to prosecute the crimes committed and increasing the potential for damage.

Infringing IP rights: the acquisition phase

The infringement of IP rights is the first and most important stage of IP crime. It may involve counterfeiting or piracy, depending on the type of product or service in question. In this phase, IP rights are purposefully violated with the objective of gaining illicit proceeds. The IP may be infringed by producing, by stealing or by diverting from the legal chain.

Production and assembly

A range of counterfeit products, such as luxury goods, clothing, toys, and electronics, are produced with replicated brand logos.

China, including Hong Kong, and Türkiye remain the main source regions for counterfeit commodities, as well as for raw materials ([23]).

EU-based criminal networks involved in the importation and distribution of counterfeit products are also implicated in operating facilities that assemble counterfeit commodities ([24]). Criminal networks involved in IP crime seek ways to enhance their operations by setting up laboratories, manufacturing facilities, and assembly points within the EU. These are usually on a smaller scale than the large-scale production sites situated outside the EU, particularly in China, and are therefore harder for law enforcement to detect. However, these clandestine EU assembly points consolidate the illegal cross-border operations and distribution.

Criminal actors continue to import raw materials and mix them with other – sometimes forbidden – substances to produce substandard or falsified pharmaceutical products. These are produced in illegal laboratories, which are unhygienic, unregulated and pose dangers to the health and safety both of consumers and the individuals producing them. Materials such as labels and holograms for counterfeit clothing products, on the other hand, are often shipped separately to these assembly points to avoid customs detection. These are then assembled to manufacture counterfeit products. Machinery, printing technologies and fabricated moulds are often used to create and manufacture

counterfeit automotive spare parts, such as wheel rims, brake pads, and other related goods.

Theft and diversion from the legal supply chain

Pharma crime is one sub-type of IP crime that poses a growing threat in the EU. Criminal networks, sometimes with the support of colluding employees, are involved in theft or diversion or from the legal supply chain. Legitimate products may be stolen from warehouses, during transportation, or from pharmacies or hospitals ([25]). Genuine prescriptions may also be stolen or falsified.

In the case of diversion, legally manufactured goods are rerouted from their legitimate distribution channels to illicit markets using false statements and declarations. This step in the criminal process is linked to specific types of goods, such as pharmaceuticals, and is driven by market needs, the cost of medicines, and legal supply vulnerabilities.

CASE EXAMPLE: THEFT OF MEDICAL PRESCRIPTIONS

Crime: IP crime – pharma crime | Impact: financial | consumer health and safety

In the 2022 edition of Operation SHIELD, French authorities targeted a criminal network trafficking psychotropic drug. The drugs were collected in legal pharmacies in Rhône-Alpes (France) using stolen and falsified medical prescriptions from doctors all over the country. The criminal network was located in France, with offshoots in Austria, Germany, and North Africa. Key members regularly travelled abroad to obtain the drugs (mainly in Belgium and the Netherlands) ([26]).

Moving the goods: the transportation and distribution phase

Once the illicit goods are acquired or created, criminal networks distribute them through various channels, both in physical and in online spaces.

For wholesale distribution, the logistical sector is again exploited by criminal actors to transport counterfeit goods from one country or continent to another.

CASE EXAMPLE: INTERNATIONAL DISTRIBUTION AND SWIFT NATIONAL SUPPLY

CRIME: IP crime – commodity counterfeiting | IMPACT: consumer health and safety

In 2021, when a criminal network involved in counterfeit goods trafficking, including counterfeit perfumes, was dismantled, the international dimension of the supply chain was highlighted. The counterfeit cosmetics and perfumes were produced in countries neighbouring the EU. The criminal network operated throughout Italy, maintaining close links to producers in countries neighbouring the EU. The goods were shipped via the Balkan route and disseminated in the Italian market. The criminal network imported perfumes in bulk in tanks and then packed them in an illicit assembly plant. Products were packed rapidly before being shipped to the customers, reducing the chance of detection by avoiding large stockpiles. The underground production point of the fake perfumes was difficult to detect because the counterfeiters had created a sophisticated supply chain: customers were shown the full counterfeit goods only hours before they were delivered.

A clandestine site used for the packaging of cosmetics was dismantled, and 2 000 counterfeit items, including several perfumes, famous brand labels and cash as well as components needed for production, were seized ([27]).

Selling the goods: the marketing and retail phase

Online marketplaces and social media, both on the surface web and the dark web, continue to be fundamental to the trade in counterfeit goods such as pharmaceuticals, clothing, automotive spare parts, games and toys, and other luxury goods. These platforms provide various degrees of anonymity and target large audiences, making it challenging to identify the criminal actors involved. As for piracy, file-sharing networks are key to the distribution of copyrighted content. These channels exist alongside traditional retail outlets and open markets.

Retail distribution to customers often takes place through couriers or postal services. The physical trafficking of pharmaceutical products, such as tablets (which may either be genuine or counterfeit), is another means of illegal distribution, with individuals tasked with driving them from one country to another or transporting them by air. These are often criminal actors who form part of the criminal network, or other individuals enticed for financial reasons.
The infiltration and abuse of legal business structures also remains a significant part of the IP crime process in both the offline and online domains. Counterfeit goods may also be introduced into the legal chain for retail purposes.

Dealing with profits and risks: the money-laundering and countermeasures phase

Criminal networks involved in IP crime hope to obtain monetary gain via these illicit activities. These illicit proceeds, once obtained, need to be laundered or reinvested in a criminal financial system, or in the further development of their criminal portfolio.

Money laundering and criminal finances are therefore a key step at the end of the criminal process, and may indeed trigger a new cycle of criminal activity.

Criminal networks develop concealment strategies as part of their modus operandi to protect their trade and the identities of their members. Illicit goods, for example, can be concealed in shipping containers by covering them with non-infringing goods. Small parcel deliveries following e-commerce purchases, as well as the splitting of larger parcels into smaller shipments, are another key aspect of counterfeit trade, impeding customs controls. Counterfeit trademarks are sometimes hidden by a sticker or coloured tape (on electronic products, auto parts, etc.) ([28]).

Networks basing their activities online hide their traces by employing multiple web services (e.g. domain registration and web hosting services), delivered by providers residing in different countries. Encrypted instant messaging platforms are used by networks both to sell to customers and to communicate among their members ([29]).

Document and identity fraud, including the use of false identities or false addresses, is prevalent, for example in renting facilities under fake identities and registering website domains where illicit goods are to be sold.

The impact of IP crime

Intellectual property crime has substantial and wide-ranging consequences, both direct and indirect.

Substandard or falsified pharmaceuticals are often produced in clandestine laboratories using harmful substances, with workers exposed to serious health dangers.

Economically, as commercial companies are the primary target, the illicit sale of counterfeit products generates significant losses in terms of business profits, including those of small and medium enterprises ([30]), and government tax revenues. Hand in hand with private business, intangible assets such as inventions, artistic and cultural creations, brands, software, know-how, business processes, and data are the cornerstones of today's global economy ([31]). As intellectual property management and brand protection are key to any successful business strategy, all industries relying on IP rights aim to protect their strategies and assets from competitors in the global market. IP rights infringement damages fair competition and creates market distortions, hampering investments in research and innovation, as well as distorting the job market.

Equally significant is the substantial threat of IP crime to the **health and safety** of consumers. Substandard or falsified pharmaceutical and healthcare products, food and beverages, electrical household goods, automotive spare parts, and – especially –

fake toys pose grave dangers to end users. Such products are often made using toxic ingredients, and some are even faulty, which increases the chances of dangerous misuse.

CASE EXAMPLE: COUNTERFEIT LAW ENFORCEMENT PROTECTIVE EQUIPMENT

CRIME: IP crime, document fraud | IMPACT: consumer health and safety, security

In March 2022, the US District Court of Oregon convicted a proprietor of a trading company that sold ballistic personal protective equipment (BPPE), with fraudulent certifications and misleading country of origin markings, to the detriment of law enforcement agencies across the United States to the sum of over EUR 1.3 million (USD 1.5 million).

Over 1 000 substandard Chinese-manufactured BPPE items were removed from service from US law enforcement services. It involved counterfeit goods that had entered the US government supply chain. These uncertified BPPEs posed a significant health and safety threat, potentially having catastrophic outcomes. These outcomes imperilled the safety of the service members and public safety professionals by lacking crucial features that rendered the material unsafe for ballistic use, exposing individuals to undue peril ([32]).

IP crime also has severe **environmental** consequences. Legitimate companies are bound by national laws and EU frameworks on environmental protection, especially when hazardous manufacturing materials are used, from cradle to grave ([33]). Criminal actors involved in IP crime, on the other hand, show a total disregard for the environmental costs of their activities.

For instance, substandard or falsified pharmaceuticals are often produced in clandestine laboratories using harmful substances, with workers exposed to serious health dangers. Counterfeit pesticides are generally placed on the market without sufficient testing and quality control ([34]), with harmful residues dispersing in the air and depositing in the soil, damaging crops and food and polluting waterways. Counterfeit car parts pose significant dangers to the environment due to non-compliance with environmental protection standards and waste management regulations ([35]). Ultimately, the same can be said of all types of IP crime that contribute to environmental harm by improperly disposing of chemical waste ([36]). The detection of counterfeit goods by customs and law enforcement authorities in the EU also poses additional challenges and health risks following their destruction by the authorities, adding to the overall waste produced in the EU ([37]).

CASE EXAMPLE: ILLICIT PESTICIDES USED IN PROTECTED AREAS

CRIME: IP crime – illicit pesticides | IMPACT: environment, consumer health and safety

In a 2024 investigation into the import of illicit pesticides into Spain, laboratory tests on the illegal products revealed that they contained illegal substances, one of which was Chlorpyrifos, an organophosphate insecticide which has been banned in the EU since 2020.

The banned pesticides were used in various farming facilities, some of which were located in protected areas, such as the Doñana National Park (World Heritage). This national park is one of the most significant in Spain. The illegal use of pesticides posed a significant threat to this park's habitat, wetlands, and underground water reserves ([38]).

Part II: Enablers of IP crime: Understanding the factors that facilitate IP crime

This chapter identifies and explains the various conditions, systems and mechanisms that enable criminal networks to commit IP crime. They may enable the criminal process in general, or they may be involved in a specific phase of the criminal process. They may be acts that are crimes in themselves or acts that are legal, but misused to commit crimes.

This chapter also considers how IP crime can potentially function as a criminal enabler in itself, furthering other types of serious and organised crime.

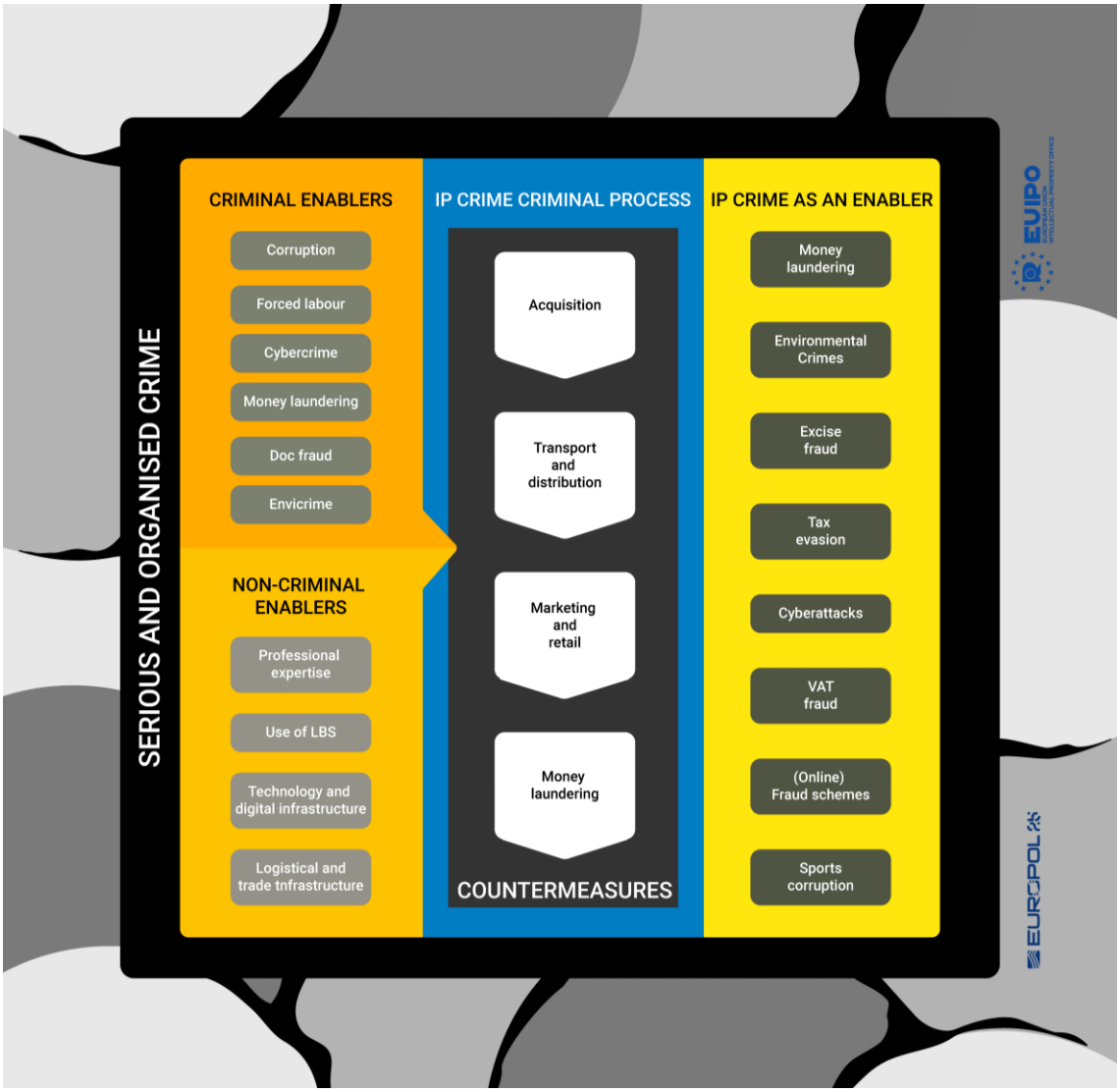

Figure 4. How the IP criminal process is enabled, and enables other crimes

How other types of organised crime enable IPC

A variety of supportive criminal acts facilitate counterfeiters in their illicit activities. The most common IP crime enablers are document fraud, cyber-enabled crime and cybercrime, corruption, money laundering, and labour exploitation.

Cybercrime facilitates IP crime in many ways. Criminals involved in IP crime make use of digital technologies combined with criminal techniques and tools at various stages of the criminal process.

Document fraud

Document fraud is a critical enabler of IP crime, as criminal actors make use of a variety of fraudulent documents throughout the various steps of the criminal process.

In the **acquisition phase**, fake packaging, logos and certifications are used to imitate the genuine products. Moreover, fraudulent documents such as customs declarations and sale or purchase invoices enable criminal actors to acquire intellectual property illegally. Copyright notices may be fabricated, fraudulently proving ownership of the product or transferring ownership of the intellectual property without the consent of the right holder ([39]).

In the context of food products that infringe a protected geographical indication, falsified documents are used to facilitate the insertion of substandard food products into the legal supply chain.

CASE EXAMPLE: DOCUMENT FRAUD IN THE CONTEXT OF FOOD FRAUD

CRIME: IP crime, food fraud, document fraud | IMPACT: consumer health and safety, economy

A criminal network was detected producing ham that was marketed as Italian prosciutto, but in reality, came from Denmark. The criminals operated their own slaughterhouse and used falsified documents, fake stamps and industrial tattoos to pass the pork meat off as a local Italian breed. They also fed the animals forbidden products and used forged documents to obtain a subsidy from the Italian state to renovate their slaughterhouse.

Criminal networks have also been found to use false invoices to certify olive oil coming from Greece, Morocco and Spain as the more desirable extra virgin olive oil with the label 'made in Italy' ([40]).

In the context of pharma crime, criminal actors use fake prescriptions to obtain genuine medicinal products from pharmacies for illicit onward resale, sometimes even

at a higher price ([41]), exploiting the general market shortage of medicines across countries. Simultaneously, counterfeiters often introduce into the market substandard and falsified versions of genuine products, often fraudulently relabelling these versions.

CASE EXAMPLE: FALSIFIED PACKAGING AND DOCUMENTATION FOR PHARMACRIME

CRIME: IP crime – pharma crime, document fraud | IMPACT: consumer health and safety

In 2023, the Irish authorities investigated the misuse of Semaglutide injection pens bearing a renowned pharmaceutical trade name (Company A). Semaglutide is commonly misused by people seeking immediate weight loss. An increase in sales led to global shortages of the product, and the introduction of substandard or falsified versions into the market. Investigations revealed that these versions were fraudulently relabelled under the trademark of Company A, but did not include the active ingredient Semaglutide; instead, they contained insulin glulisine, which led to a Type 2 diabetes patient falling into a coma. These substandard or falsified pens have been discovered in multiple countries outside the EU ([42]).

In the **transport, distribution and retail phase**, criminals conceal the counterfeit goods' origin or their own business activity by producing false documents including invoices and customs declarations.

Counterfeit pesticides are generally placed on the market using false documentation, without having been officially tested and authorised. They, and often contain cheaper ingredients that are less active, while in other cases the ingredients may exceed toxicity limits ([43]).

The falsified documentation not only deceives suppliers, monitoring authorities, and distributors, but ultimately (and most importantly) end-consumers, who often unknowingly purchase counterfeit goods or medicines, putting their health and safety at risk.

Document fraud is also prevalent as a **countermeasure**. Counterfeiters use false identities to rent production or storage facilities, or to register website domains where illicit goods are to be sold. Domain Name System (DNS) Abuse is intimately linked to the trade into counterfeit goods in the EU marketplace ([44]).

Corruption

Corruption comprises a wide variety of illicit methods through which criminals co-opt others into the criminal process, targeting individuals in positions of power or those who are in possession of sensitive information, in order to obtain a specific power

and/or information in exchange for money or other benefits. Corruption is a widespread phenomenon that afflicts both the public and private sectors; it harms political, social and economic stability while undermining the rule of law. Together with money laundering, corruption functions as a critical part of the engine of organised crime ([45]). It is in fact an indispensable instrument for organised crime, with 60 % of the criminal networks operating in the EU – and 71 % of the EU's most threatening criminal networks – using corruptive measures to achieve their illicit objectives ([46]).

Corruption in the form of bribery is used by IP criminals as an enabler ([47]) at all stages of the criminal process from control over transport to retail, money laundering and countermeasures.

In the **acquisition phase**, IP criminals target officers working in regulatory bodies enforcing intellectual property rights, agents working on licenses and certifications, and professional experts such as technicians and lawyers, as well as suppliers and manufacturers.

In cases of diversion or theft of pharmaceutical products, criminals target pharmaceutical factory employees, doctors, and pharmacists to illicitly obtain prescription medicines ([48]). In the **transportation** phase, corrupt associates in various countries are used to coordinate and enable the trafficking chain at entry, transit and exit hubs. For example, criminal networks engage in corruption to control critical infrastructure, such as ports, to ensure that incoming shipments are successfully received by criminal customers. Police officials, customs officers, security staff, and other personnel at sensitive transportation hubs and at border control points are approached to provide information and ensure trafficked goods can pass unimpeded.

As a **countermeasure**, law enforcement officers and judicial authorities are vulnerable targets for corruption with the purpose of obtaining information on and obstructing law enforcement or judicial proceedings ([49]).

Labour exploitation

Labour exploitation is a serious and organised crime area that is specifically related to the **production phase** of counterfeit products.

Most of the counterfeited items marketed in the EU are produced abroad. In many reported cases, the process involves labour-intensive work, unhygienic conditions, insufficient health and safety measures, and underpayment.

However, investigations into assembly points in the EU have also revealed cases of labour exploitation within EU territory. The criminal network may be directly involved in the recruitment of the workers or may rely on other criminal networks for the supply of an irregular workforce.

Figure 5: Seized counterfeit clothes produced in a situation of labour exploitation (Source: Guardia di Finanza)

CASE EXAMPLES: LABOUR EXPLOITATION FOR THE PRODUCTION OF COUNTERFEITS

CRIME: IP crime – commodity counterfeiting, trafficking in human beings – labour exploitation | IMPACT: consumer health and safety, security

In May 2023, Italian authorities carried out an operation in Naples targeting an underground factory for counterfeit clothing branded 'Made in Italy' – a certified denomination for which, in this case, the relevant documentation was missing. Seven persons were employed on the site in precarious working conditions and without any workplace safety provisions ([50]).

In June 2023, Spanish authorities investigated a website offering counterfeit luxury brands through various social networks. The counterfeit clothes were transported from Romania into Spain, with four individuals employed at the illicit production site, who were subjected to exhausting working hours in manufacturing the counterfeit goods ([51]).

Environmental crime

Criminals producing fake goods at clandestine laboratories and/or assembly points may need to engage other criminals operating in the illegal waste management business, in order to conceal the production waste accumulated.

Cyber-enabled crimes and cybercrime

Cybercrime facilitates IP crime in many ways. Criminals involved in IP crime make use of digital technologies in combination with criminal techniques and tools at various stages of the criminal process.

In the **acquisition phase**, cyber-enabled criminal activities such as phishing, social engineering, and malware attacks facilitate the theft or infringement of IP rights and data. Hacking techniques and tools for cyber-espionage are also used in the context of industrial and other business data theft, including trade secrets. Criminals use phishing services to distribute emails containing documents with malicious macros, infected container files, or URLs that lead to webpages that initiate a drive-by download of malware. Interacting with these sources often results in a dropper ([52]) being introduced into the victim's system ([53]).

In the **retail phase**, cyber-enabled criminal activities facilitate the online advertising of fake goods. Cybersquatting is a common technique used by IP criminals in which domains identical or similar to those of well-known brands and trademarks are registered in order to trick buyers into believing that they are on the original online stores. For the distribution of their illicit goods, counterfeiters may use mass-mailing techniques to attract potential buyers.

One of the main manifestations of distributed cyber-enabled crime is digital piracy, entailing the unauthorised reproduction and distribution of copyrighted digital content (i.e. films, music, e-books, software, etc.), through file sharing platforms, torrent networks, and dark web marketplaces ([54]). This includes the illegal streaming of internet protocol television (IPTV) content, which has become increasingly popular, especially during major sporting events. Digital piracy is a lucrative business. Pirate websites often generate significant revenue through advertising, affiliate marketing, and even direct sales of pirated content. These websites can attract millions of visitors, making them highly attractive to advertisers ([55]). The criminal process and its online nature allow easy access and are more convenient for the criminal actors involved than producing, copying and distributing hardware content such as traditional DVDs or physical equipment.

Furthermore, payments for illegal services and purchases of other counterfeit commodities are often made through online payment platforms, which again facilitates the criminal process, making it more cyber-oriented.

CASE EXAMPLE: THE DISTRIBUTION OF PROTECTED DIGITAL CONTENT

CRIME: IP crime – digital piracy, cybercrime | IMPACT: consumer security – personal data

In 2023, a criminal network was dismantled that was distributing protected digital content across Europe and third countries through a network of resellers.

The criminal network had created an illegal company data centre for broadcasting the illicit content. They also provided the infrastructure as a service to other criminal networks. Some 85 % of the 800 servers owned by the company were used for criminal purposes. The criminal networks making use of the infrastructure were involved in intellectual property crimes, but also in other computer crimes.

The head of the criminal network was associated to other individuals in different European countries, which were used as cash collectors or resellers for the streaming services. It is estimated that the digital streaming platform had more than 1 000 000 final users, offering 10 000 live TV channels and more of 15 000 films or TV shows ([56]).

Money laundering

Money laundering is a pivotal activity for organised crime ([57]). Money laundering allows criminal actors and networks to clean their illicit profits and reintroduce them into the legitimate financial system, while disguising the origin of the funds. Money laundering is a critical component of the engine of organised crime, which allows criminal networks to cover their operational costs and to increase their assets, giving them the opportunity to thrive. This also applies to criminal networks involved in IP crime, where money laundering is the final phase in the criminal process.

Information on money laundering in relation to IP crime is often missing, as not all criminal investigations run in parallel with financial investigations into the money flows. However, criminal networks involved in IP crime mostly use traditional, unsophisticated money laundering techniques such as bank transfers, physical movement, and investments in real estate, luxury goods, or companies, as well as trade-based money laundering ([58]).

CASE EXAMPLE: CHINESE MONEY-LAUNDERING CRIMINAL NETWORK ALSO LAUNDERING IP CRIME PROCEEDS

CRIME: IP crime – commodity counterfeiting, money laundering | IMPACT: economy

Following an initial investigation and the seizure of more than half a million euro in cash in 2021 by the French authorities, investigations by the French and Spanish authorities led to a crackdown on a Chinese money-laundering criminal network, which potentially had the capacity to smuggle over 1 million euro in cash per day.

The network had allegedly been operating across Europe since 2019. The illicit proceeds originated from the trafficking of counterfeit goods, tax and customs fraud, and prostitution. The criminal network relied on a sophisticated network of logistics experts who facilitated the movement of the cash across Europe ([59]).

As cryptocurrencies are more and more frequently encountered as a means of payment for counterfeit commodities (e.g. pharmaceuticals or doping substances ([60]) or digital piracy ([61]) (file sharing or IPTV ([62]), cryptocurrency exchanges are also used to launder IP crime profits.

As an alternative to laundering the proceeds, criminal networks may use the illicit funds to strengthen their criminal activity, such as by reinvesting it in raw materials or in their infrastructure: depending on the type of IP infringement in question, this may be production sites, assembly sites, or digital infrastructure.

CASE EXAMPLE: REINVESTMENT OF IP CRIME PROCEEDS IN ENHANCING COUNTERFEITING INFRASTRUCTURE

CRIME: IP crime – digital piracy, criminal finances | IMPACT: internal security data

An investigation in 2022 concerned a case related to the provision of both foreign and Bulgarian television programmes to end users without the legal consent of the right holders. Investigations revealed that the criminal network had gained an illegal profit of EUR 600 000 over a 2-year period. Three illegal servers were seized and the digital channels shut down. Additionally, the cash received enabled the criminal actors to reinvest in and conceal their illicit activity by upgrading their digital infrastructure as well as the criminal network's overall business infrastructure ([63]).

How legal systems enable IP crime

Criminal networks involved in IP crime rely on a series of non-criminal services or providers that facilitate their illicit activities. As much as criminal enablers, these actors are pivotal to the criminal process, from acquisition to laundering and countermeasures.

Unaware consumers are more tricked than ever, and recognising counterfeit items has become a technical task that requires specific knowledge and an expert eye

Abuse of legal business structures

Organised crime frequently misuses legal business structures (LBS) to provide their illicit operations with a façade of legitimacy, facilitate their criminal activities, and launder their criminal proceeds. In the EU, 80 % or more of criminal networks misuse LBS to facilitate their activities ([64]).

IP crime relies on a large variety of abused LBS in both the offline and online domains. Legal businesses may be set up ad hoc by criminals or may be infiltrated, and they may be misused systematically or just temporarily. To avoid suspicion, LBS are spread across different countries along the operational routes, with multiple intermediaries and collaborators in charge. Legitimate employees involved in IP crime can be found at all levels of the legal supply chain: manufacturers, importers, transporters, stockists, distributors and traders.

LBS are critical to the perpetration of IP crime. From production to distribution, criminal networks may either set up or infiltrate a series of business entities, which enables them to portray a façade of legitimacy while carrying out their criminal activity. Specific LBS may be linked to one or more parts of the criminal process: criminal counterfeiting networks use LBS to facilitate the production and movement of goods and as a retail channel, to launder illegal profits, or to conceal the criminal activity.

In the **acquisition phase**, legitimate businesses, including factories, may be set up to hide illicit production. In the specific context of pharma crime, the infiltration and abuse of pharmaceutical companies and pharmacies is critical, especially when the modus operandi involves the diversion or theft of legitimate goods.

In the **transport phase**, commercial warehouses, transport companies, and shipping services, for example, may be relevant. In the retail phase, any physical store or retail outlet may be involved, as well as online web stores, marketplaces, social media, and E2EE applications.

CASE EXAMPLE: SPANISH COMPANY IMPORTING ILLEGAL PESTICIDES

CRIME: IP crime – illicit pesticides, environmental crime | IMPACT: health and safety, environment

A Spanish company purchased Portuguese pesticides banned in Spain. The ensuing investigation found that the suspects had imported over 12 tonnes of toxic substances banned in Spain, many of which were also banned across the EU, with a potential illegal turnover of up to EUR 7 million.

Two legal entities were investigated in connection with this trafficking. The company covered the product with the names of products and substances registered in Spanish databases, to create the appearance of legal merchandise. They also purchased legal pesticides to hide the additional, illegal pesticides ([65]).

Engaging professional expertise

Throughout the various phases of the criminal process, criminals rely on a variety of professionals to carry out specific tasks that require particular expertise. These experts are sometimes recruited as crime-as-a-service providers, while at other times they may be permanent members of a criminal network. Medical specialists, pharmacists, technicians, IT staff, graphic designers, financial advisors and lawyers are often co-opted in IP-related crimes ([66]).

The employment of such professional experts is linked not only to their specific skills or competencies, but also sometimes to the abuse of the legal business where they are employed for other criminal purposes, such as the use of their legitimate business activity as cover or for money laundering ([67]). In the context of the sale of illicit hormonal substances, the criminal engagement of fitness professionals has been observed, among whom the use of such products is common ([68]).

CASE EXAMPLE: PHARMACIST IN CHARGE OF PHARMACEUTICAL TRAFFICKING

CRIME: IP crime – pharma crime | IMPACT: health and safety

In 2022, Europol received intelligence from the French authorities concerning pharmacies purchasing excessive volumes of prescribed medications from legal suppliers for trafficking to countries outside the EU, in particular Vietnam. Investigations revealed that a pharmacist (who was also the owner of a pharmacy) in France was the organiser of the criminal network involved in trafficking legal medication to Vietnam. The medications were then smuggled by couriers (in one case, a family accompanied by their 2-year-old child) to Asia ([69]).

In digital piracy, criminals usually rely on the expertise of technicians who know how to build, operate and optimise the software and digital infrastructure of internet protocol television (IPTV) systems.

The abuse of technology

Organised crime makes excellent use of innovation. With technology constantly evolving, IP criminals are adept at exploiting the most innovative technologies to their advantage, particularly in the production phase of IP crime. As sophisticated technologies are used to replicate holograms, logos and packaging, unaware consumers are more likely than ever to be deceived, and recognising counterfeit items has become a technical task that requires specific knowledge and an expert eye ([70]). The abuse of tools such as 3D printing and AI is also expected to grow in the near future, as they are set to enhance counterfeiting techniques even further, reducing the risk of human error and facilitating automated production ([71]). This poses significant challenges to law enforcement and monitoring authorities. 3D-printed fakes represent a significant danger to industries like fashion, pharmaceuticals, and consumer electronics, as counterfeiters can easily access digital files containing 3D-scanned images, posing a threat to trademark, patent, and design right holders. However, embedding products with near-field communication (NFC) ([72]) or QR ([73]) codes can validate their authenticity and thus help to identify counterfeits ([74]).

CASE EXAMPLE: INDUSTRIAL-SCALE PRODUCTION SITE FOR AUTOMOTIVE SPARE PARTS

CRIME: IP crime – commodity counterfeiting, money laundering | IMPACT: health and safety

In 2024, the Italian authorities led an investigation into the production of counterfeit automotive spare parts led to seizures of close to 400 000 items with an estimated value of more than EUR 2 million, as well as more than 200 moulds with a commercial value of EUR 180 000. The network employed several production sites. During the investigation, the suspects were found to have continued their illicit operations during the liquidation of the investigated companies by creating new entities and fraudulently transferring business assets.

To prevent further operations, the production sites of the two main companies involved were seized, including 13 production lines consisting of 13 items of industrial machinery, 25 screen-printing frames, and 175 industrial moulds for wheel trims, with a total commercial value of EUR 4 712 500. The industrial machinery, screen-printing frames and industrial moulds relied extensively on technology and expertise in the operation of the production line ([75]).

Artificial-intelligence tools help law enforcement, brand owners and online market places to flag suspicious products by comparing existing data collections (collection, provided by the brand owners) against scanned images of the products being

advertised ([76]). However, it is also being exploited by criminal networks, with AI revolutionising criminal operations, enhancing their efficiency, sophistication, and scalability, while enabling them to evade detection and attribution.

Misuse of logistical and trade infrastructure

The misuse of logistical and trade infrastructure is entwined with the exploitation of LBS, and is encountered in the transportation phase of physical goods counterfeiting. As the principal source country for counterfeit products remains China, followed by Türkiye. Transport across air, sea and land hubs is often combined. To avoid detection, criminal networks involved in clothing counterfeiting often separate the fake garments and their labels and other brand-related markings across different shipments, for later reassembly within the EU.

CASE EXAMPLE: MISUSE OF STORAGE FACILITY BY CRIMINAL NETWORK

CRIME: IP crime – commodity counterfeiting, money laundering | IMPACT: health and safety, economy

In 2021 the Belgian authorities conducted investigations on counterfeit electronic goods being sold on the Belgian markets. Following a raid on the storage facility of the supplier, a hidden warehouse was discovered and being used by another wholesaler. During the operation, large quantities of counterfeit goods were seized from within the hidden warehouse.

Financial investigations revealed bank transactions to a known company selling counterfeit goods and the use of forged invoices. Legal businesses were used to support illegal activities.

CASE EXAMPLE: COUNTERFEIT SHOES TRAFFICKED BETWEEN ITALY AND SPAIN

CRIME: IP crime – commodity counterfeiting, money laundering | IMPACT: health and safety, economy

In 2021, a transportation company was suspected of trafficking counterfeit goods and cash between Italy and Spain. A search of the cargo and cabin resulted in the discovery of 168 pairs of counterfeit shoes and 3 travel bags containing bundles of banknotes wrapped in foil amounting to more than half a million euro ([77]).

CASE EXAMPLE: DYNAMIC GLOBAL SUPPLY CHAINS FOR COUNTERFEIT ALCOHOL

CRIME: IP crime, food fraud | IMPACT: consumer health and safety, economy

In 2021, a criminal network imported empty bottles from China via companies based in the EU. When several loads of bottles were damaged during transport, the network swiftly changed their supply chain and purchased bottles from neighbouring countries instead. The bottles were filled with alcohol in the EU. Further investigations led to the interception of an export shipment destined for South Korea. The shipment contained 15 502 counterfeit bottles. This finding is indicative of the high risk of counterfeit alcoholic beverages for export ([78]).

Postal and express couriers continue to be the most widely abused means of transportation for the distribution of counterfeit goods within the EU ([79]). Global digitalisation has shifted the distribution of counterfeit goods and services online, drastically reducing the number of physical retailers. Online distribution further distances criminal actors from their commodities, enabling them to operate from outside the EU and to rely on a network of intermediaries and front companies ([80]).

CASE EXAMPLE: COUNTERFEITING CRIMINAL NETWORK OWNS COURIER COMPANIES

CRIME: IP crime – commodity counterfeiting, money laundering | IMPACT: security personal data

In June 2022, the Greek authorities conducted investigations into a criminal network involved in trading counterfeit luxury goods through a website and 13 social media profiles. The group was composed of both male and female Greek nationals and had been operating since February 2020, during which time it had managed to distribute over 364 000 parcels to customers and obtain more than EUR 18 million in illicit profits, laundered via other business companies owned by the network. The group also owned two courier companies that would exchange goods and money multiple times to avoid detection and conceal their criminal activities. On the action day, 3 603 counterfeit products, 335 parcels containing counterfeit products, EUR 11 837, 1 vehicle, multiple telephone devices used for the management of the social media profiles, and other documents were found ([81]).

How IP crime enables other types of organised crime

The connections between IP crime and other criminal or non-criminal activities are not a unidirectional phenomenon. While IP crime is enabled by a number of activities and systems, IP crime in its turn also facilitates other types of serious and organised crime. The commission of IP crime may further other forms of serious and organised crime, such as cyber-attacks, online fraud, VAT and excise fraud, sports corruption, money laundering.

Criminal actors make customers believe they are on a legitimate web shop while they are on a fake web shop that not only is going to deliver a counterfeit good to the victim but also steal their payment credentials

Cyber-attacks

IP crime, particularly digital copyright piracy, can enable – and has been found to run in parallel with – cyber-attacks. Digital piracy platforms are often used to distribute malicious software, such as viruses, spyware, and ransomware. Pirate websites are notorious for spreading malware, which can be hosted on a separate server, and which can infect users' devices and compromise their personal information. This poses a significant security risk to individuals and organisations alike, as data is increasingly illicitly traded as a commodity in the cybercrime realm and often forms part of crime-as-a-service business models ([82]).

(Online) fraud schemes

Among the most threatening criminal networks affecting the EU, among those engaging in fraud schemes as their core business, some 30 % combine this with other main activities such as counterfeiting or property crime ([83]). As such online fraud, e-commerce fraud can be directly linked to IP crime and may be conducted during the online commercial transaction through which the counterfeiters sell their products to the consumers.

Criminal actors make customers believe they are on a legitimate web shop, when in fact while they are on a fake web shop that not only is going to deliver a counterfeit product to the victim but also steals their payment credentials. This data can then be further exploited in financial operations or sold on illegal credentials marketplaces. These fraudulent schemes often economically damage both merchants and buyers, especially when counterfeiters abuse legitimate marketplaces and online stores.

Both illicit stores and illicit online platforms offering counterfeit goods and pirated content increasingly replicate the layout and structure of legal platforms, thereby deceiving consumers. A common modus operandi to attract customers (both online and in physical stores) is to offer the goods at a price close to but lower than that of the genuine products, resembling a fake discount ([84]).

In other cases, fake web shops are created to conduct so-called 'triangle fraud', which entails selling fake products at very low prices, stealing customers' credit card data, and then ordering the goods from the genuine shop – causing a loss of money to both purchaser and merchant, and a reputational risk to the legitimate shop ([85]).

Sports corruption

The use of illicit hormonal substances, which may be counterfeited or diverted from the legal supply chain, in sports competitions may also give rise to sports corruption, which results in a person/s obtaining an undue advantage for themselves or for others. Sports corruption may also be linked to match-fixing and betting fraud ([86]).

Money laundering is a consequential criminal act linked to IP crime. Money laundering may be carried out by the same criminal network involved in counterfeiting or outsourced to professional crime-as-a-service providers.

VAT and customs import fraud

The sale of counterfeit goods via illicit trade networks by definition evades duties, customs taxes, and VAT. Various types of tax fraud may also make use of counterfeit goods to facilitate the specific fraud. When it comes to transnational trafficking, counterfeiting networks may resort to the fraudulent use of customs regime 42. In this context, the goods are often destined for fictitious companies that disappear without paying VAT, and the counterfeit goods are not always shipped to the declared destination ([87]).

Excise fraud

The illicit production of counterfeit tobacco products is an inherent enabler in the process of excise fraud. This business has grown in the EU and provides a lucrative criminal income, as demand is high, particularly in countries that apply high excise and VAT rates ([88]).

CASE EXAMPLE: COUNTERFEIT TOBACCO PRODUCTS WORTH EUR 17 MILLION SEIZED IN FRANCE

CRIME: IP crime – commodity counterfeiting, excise fraud - tobacco | IMPACT: health and safety, economy

In 2023, French authorities raided an underground factory manufacturing counterfeit tobacco. The factory had three separate zones. One was dedicated to the processing of raw tobacco to produce boxes of cigarettes labelled as well-known brands and sold on the legal market. Another zone was dedicated to the storage of large boxes of counterfeit cigarettes. The third zone was used as a living area for the workers, with 15 beds, a kitchen, and a living room. This allowed the workers to live at the factory, completely cut off from the outside world.

During the raids, the officers seized more than 100 tonnes of illegal products, including 55 tonnes of cigarettes in boxes (19.4 million cigarettes and 15 tonnes of cut tobacco); 50 tonnes of packaging materials such as paper, filters and labels; and 18 tonnes of waste from the cigarette production process. The estimated value of the seized tobacco was about EUR 17 million, with further seizures of vehicles, factory machinery, and electronic equipment ([89]).

Conclusion: Mitigating the impact of IP crime

The harms caused by the global counterfeiting market necessitate a comprehensive understanding of the interplay between policy and culture ([90]).Counterfeiting and piracy subcultures play an important role in understanding the phenomenon and require a more in-depth analysis of the cultural distinctions between various countries. Despite significant global progress toward stronger IP protection, enforcement legislation and infrastructure, there are still a number of problematic hotspots which are the source of counterfeit production. Therefore more law enforcement and judicial action is warranted. Nevertheless, right holders remain crucial to supporting law enforcement both within the EU and in key jurisdictions around the world.

Law enforcement actions, monitoring and sharing of intelligence across all stakeholders remains vital in preventing and detecting IP crime

Technology will continue to change the digital landscape, with the quality of counterfeit electronic goods improving and detection becoming more challenging. Copyright-protected digital content will continue to be a problem, fluctuating according not only to the schedule of major sports events but in relation all types of online digital content. The same holds true for counterfeit clothing and other counterfeit commodities. Addressing the role of influencers and the online marketing and sale of counterfeit products requires education and awareness campaigns, as well as legal tools to deal with any person or company who participates in the marketing of counterfeit goods. Understanding and mitigating risks associated with counterfeit purchases is crucial for consumers and society.

The case examples throughout this report open the reflection of the true nature of various criminal and non-criminal enablers driving IP crime, as well as the role of IP crime in supporting other serious crimes. IP crime will continue as long as demand remains high and accepted by society and criminal actors continue to consider IP crime a low-risk, high-profit endeavour. Despite the EU's legal IP protection mechanisms and robust legal framework ([91]) on pharmaceuticals, the recreational misuse of medicines and social media and e-commerce will continue to encourage and sustain the illicit market for substandard or falsified pharmaceuticals and other commodities.

ABOUT EUROPOL AND EFECC

Europol is the EU's law enforcement agency and it assists the Member States in their fight against serious international crime and terrorism. Established in 2000, Europol is at the heart of the European security architecture and offers a unique range of services. Europol is a support centre for law enforcement operations, a hub for information on criminal activities, and a focal point for law enforcement expertise.

The European Financial and Economic Crime Centre (EFECC) was established in June 2020, as Europol's answer to the growing threats posed to the economy and integrity of financial systems. These threats include counterfeiting, money laundering, corruption, fraud and tax fraud schemes that target individuals, businesses and public institutions. EFECC enhances Europol's operational and strategic support by preventing and combating financial and economic crime in the European Union. EFECC promotes the consistent use of financial investigations and asset forfeiture, while forging alliances with public and private entities.

ABOUT EUIPO

The European Union Intellectual Property Office (EUIPO) is the European Union (EU) agency responsible for managing the EU trademarks (EUTMs), the registered Community designs (RCDs), the Geographical Indications (GIs) for craft and industrial products and the European and international cooperation in the field of intellectual property (IP), as well as the European Observatory on Infringements of Intellectual Property Rights.

The European Observatory on Infringements of Intellectual Property Rights is a network of experts and specialist stakeholders that provide facts and evidence, tools and resources for enforcement and awareness on the importance and impact of IP. It works in collaboration with EU partners to provide support to national enforcement authorities and the judiciary as well as businesses and other related partners in their fight against IP crime and infringements.

Law enforcement agencies, judiciary, governments, and the industry itself must remain proactive, implementing automated tools to facilitate the detection of counterfeit goods both online (through social marketplaces) and at border controls. Law enforcement actions, monitoring and intelligence sharing across all stakeholders remains vital in preventing and detecting IP crime. Investigations should go beyond

goods being stopped and destroyed and should focus in parallel on following the money, as well as the criminal networks behind the visible crime. Education and raising awareness of the seriousness of IP crime, as well as the dangers it poses to consumer health and safety, should remain a key priority.

Europol and EUIPO continue their engagement in the fight against IP crime, by supporting law enforcement agencies both within the EU and beyond, through public awareness, trainings, development systems, and evidence-based data on IP protection and enforcement, together with the support of right-holders and third-party stakeholders.

This report would not have been possible without the valuable support of law enforcement authorities and their active contribution sharing real cases.

Endnotes

([1]) Intellectual property refers to '"creations of the mind, such as inventions; literary and artistic works; designs; and symbols, names and images used in commerce'", as defined by the World Intellectual Property Organisation (WIPO).

([2]) Europol (2023), European Financial and Economic Crime Threat Assessment 2023 – The Other Side of the Coin: An Analysis of Financial and Economic Crime, Publications Office of the European Union, Luxembourg.

([3]) 'Games' refers to electronic game consoles, video games, puzzles and other games.

([4]) European Commission and EUIPO (2023), EU enforcement of intellectual property rights: results at the EU border and in the EU internal market 2022, accessible at https://taxation-customs.ec.europa.eu/document/download/67bd3b33-c597-47d5-aae9-c7336f60d6fe_en

([5]) EUIPO and OECD (2021), Global trade in fakes: a worrying threat, accessible at https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2021_EUIPO_OECD_Report_Fakes/2021_EUIPO_OECD_Trate_Fakes_Study_FullR_en.pdf.

([6]) Eurostat (2023), 59% of EU individuals using social networks in 2023, accessible at https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20240319-1.

([7]) Kemp S. (31 January 2024), Datareportal: The time we spend on social media, 31 January 2024, accessible at https://datareportal.com/reports/digital-2024-deep-dive-the-time-we-spend-on-social-media.

([8]) EUIPO & Europol (2022), Intellectual Property Crime Threat Assessment, accessible at https://www.europol.europa.eu/publications-events/publications/intellectual-property-crime-threat-assessment-2022.

([9]) Shepherd, D. et al. (2023), 'The Impact of Deviant Social Media Influencers and Consumer Characteristics on Purchasing Counterfeit Goods', Deviant Behavior, 44(12), pp. 1746–1760, accessible at https://www.tandfonline.com/doi/full/10.1080/01639625.2023.2233041.

([10]) Ibid.

([11]) Europol (30 March 2023), Gym doping bust: traffickers selling steroids to influencers, accessible at https://www.europol.europa.eu/media-press/newsroom/news/gym-doping-bust-traffickers-selling-steroids-to-influencers

([12]) EUIPO (2021), Monitoring and analysing social media in relation to IPR infringement report, accessible at https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2021_Monitoring_and_analysing_social_media_in_relation_to_IPR_Infringement_Report/2021_Monitoring_and_analysing_social_media_in_relation_to_IPR_Infringement_Report_FullR_en.pdf.

([13]) EUIPO-Europol (7 March 2022), Intellectual Property Crime Threat Assessment 2022, accessible at https://www.europol.europa.eu/publications-events/publications/intellectual-property-crime-threat-assessment-2022.

([14]) E.g. here is one from Europol on counterfeit toys and one from the EUIPO on counterfeit automotive spare parts:.

https://www.euipo.europa.eu/de/news/euipo-highlights-risks-of-counterfeit-automotive-spare-parts; https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/how-to-recognise-fake-and-hazardous-toys#:~:text=Substandard%2C%20illicit%20toys%2C%20including%20those,hazards%20as%20well%20as%20toxicity.

([15]) Europol (4 December 2023), 11 olive oil counterfeiters arrested following Operation OPSON, accessible at https://www.europol.europa.eu/media-press/newsroom/news/11-olive-oil-counterfeiters-arrested-following-operation-opson

([16]) Information contributed to Europol and EUIPO in the context of EMPACT IPCCGC.

[17]) Information contributed to Europol and EUIPO in context of EMPACT IPCCGC.

([18]) Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), accessible at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065&qid=1726253352230.

([19]) EUIPO (2024), Legislative measures related to intellectual property infringements – Phase 3, accessible at https://www.euipo.europa.eu/en/publications/legislative-measures-related-to-intellectual-property-infringements-phase-3.

([20]) European Commission, Commission recommendation of 19 March 2024 on measures to combat counterfeiting and enhance the enforcement of intellectual property rights, accessible at https://single-market-economy.ec.europa.eu/publications/commission-recommendation-measures-combat-counterfeiting-and-enhance-enforcement-intellectual_en.

([21]) Europol (2023), European Financial and Economic Crime Threat Assessment 2023 – The Other Side of the Coin: An Analysis of Financial and Economic Crime, Publications Office of the European Union, Luxembourg.

([22]) Ibid.

([23]) Taxation and Customs Union, news article, '86 million fake items with a value of more than EUR 2 billion detained in the EU in 2022', accessible at https://taxation-customs.ec.europa.eu/news/86-million-fake-items-value-more-eur-2-billion-detained-eu-2022-2023-11-27_en.

([24]) TAXUD & EUIPO (2023), Joint report: EU enforcement of intellectual property right: results at the EU border and in the EU internal market 2022, accessible at https://www.euipo.europa.eu/en/publications/eu-enforcement-of-iprs-results-at-the-eu-border-and-in-the-eu-internal-market-2022-november-2023.

([25]) EUIPO-Europol (7 March 2022), Intellectual Property Crime Threat Assessment 2022, accessible at https://www.europol.europa.eu/publications-events/publications/intellectual-property-crime-threat-assessment-2022.

([26]) Europol (29 September 2022), Medicine traffickers faced with undesirable side effects, accessible at https://www.europol.europa.eu/media-press/newsroom/news/medicine-traffickers-faced-undesirable-side-effects

([27]) Europol (23 June 2021), 'Fake perfumes assembly site dismantled in Italy', accessible at https://www.europol.europa.eu/newsroom/news/fake-perfumes-assembly-site-dismantled-in-italy.

([28]) Information contributed to Europol.

([29]) Information contributed to Europol.

(30) EUIPO and OECD (2023), Risks of illicit trade in counterfeits to small and medium sized firms, accessible at https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/Risks_of_Illicit_Trade_in_Counterfeits_to_SMEs/Risks_of_Illicit_Trade_in_Counterfeits_to_SMEs_FullR_en.pdf

(31) European Commission (2023), 'Commission releases its Report on the Protection and Enforcement of Intellectual Property Rights in Third Countries'. Accessible at https://policy.trade.ec.europa.eu/news/commission-releases-its-report-intellectual-property-rights-third-countries-2023-05-17_en.

(32) Information contributed to EMPACT IPCCGC OA 1.3

(33) A cradle-to-grave assessment considers each stage of a product's lifecycle, from the time natural resources are extracted from the ground and processed, through each subsequent stage of manufacturing, transportation, product use, and ultimately disposal; information accessible at https://www.eea.europa.eu/help/glossary/eea-glossary/cradle-to-grave.

(34) Europol, (2022), 'Environmental crime in the age of climate change: Threat Assessment 2022', accessible at https://www.europol.europa.eu/publications-events/publications/environmental-crime-in-age-of-climate-change-2022-threat-assessment#downloads.

(35) Ibid.

(36) EUIPO-Europol (7 March 2022), 'Intellectual Property Crime Threat Assessment 2022', accessible at https://www.europol.europa.eu/publications-events/publications/intellectual-property-crime-threat-assessment-2022.

(37) Europol, (2022), 'Environmental crime in the age of climate change: Threat Assessment 2022', accessible at https://www.europol.europa.eu/publications-events/publications/environmental-crime-in-age-of-climate-change-2022-threat-assessment#downloads.

(38) Europol (18 July 2024), 'Hit against fake pesticides across South-Eastern Europe', accessible at https://www.europol.europa.eu/media-press/newsroom/news/hit-against-fake-pesticides-across-south-eastern-europe.

(39) Information contributed to Europol.

(40) EUIPO-Europol (7 March 2022), 'Intellectual Property Crime Threat Assessment 2022', accessible at https://www.europol.europa.eu/publications-events/publications/intellectual-property-crime-threat-assessment-2022.

(41) Information contributed to Europol.

(42) Information contributed to EMPACT IPCCGC OA 1.3.

(43) Europol (2022), 'Environmental crime in the age of climate change: Threat Assessment 2022', accessible at https://www.europol.europa.eu/publications-events/publications/environmental-crime-in-age-of-climate-change-2022-threat-assessment#downloads.

(44) European Commission, Directorate-General for Communications Networks, Content and Technology, Paulovics, I., Duda, A., Korczynski, M., January 2022, 'Study on Domain Name System (DNS) abuse', Publications Office of the European Union, accessible at https://data.europa.eu/doi/10.2759/616244.

(45) Europol (2023), 'European Financial and Economic Crime Threat Assessment 2023 – The Other Side of the Coin: An Analysis of Financial and Economic Crime', Publications Office of the European Union, Luxembourg; Europol (2024), 'Decoding the EU's most threatening criminal networks', accessible at

https://www.europol.europa.eu/publication-events/main-reports/decoding-eus-most-threatening-criminal-networks#downloads.

([46]) Ibid.

([47]) Ibid.

([48]) Europol (2020), '48 arrested and 6 organised crime groups dismantled in medicine trafficking operation', accessible

at https://www.europol.europa.eu/newsroom/news/48-arrests-and-6-organised-crime-groups-dismantled-in-medicine-trafficking-operation.

([49]) Europol (2023), 'European Financial and Economic Crime Threat Assessment 2023 – The Other Side of the Coin: An Analysis of Financial and Economic Crime', Publications Office of the European Union, Luxembourg.

([50]) Information contributed to EMPACT IPCCGC OA 1.3.

([51]) Information contributed to EMPACT IPCCGC OA 1.3.

([52]) Droppers: programs designed to deliver malicious software to a device. They usually do not have malicious functions themselves and are designed to evade and de-activate the system's security features (e.g. anti-virus, endpoint detection) before installing malware and other malicious tools (i.e. payloads). See Europol (2023), 'IOCTA Spotlight report: Cyber Attacks: The Apex of Crime-as-a-service', accessible at https://www.europol.europa.eu/media-press/newsroom/news/iocta-spotlight-report-malware-based-cyber-attacks-published.

([53]) Europol (2023), 'IOCTA Spotlight report: Cyber Attacks: The Apex of Crime-as-a-service', accessible at https://www.europol.europa.eu/media-press/newsroom/news/iocta-spotlight-report-malware-based-cyber-attacks-published.

([54]) Information contributed to Europol.

([55]) Information contributed to Europol.

([56]) Europol (23 May 2023), One of Europe's biggest pirate IPTV services taken down in the Netherlands, accessible at https://www.europol.europa.eu/media-press/newsroom/news/one-of-europes-biggest-pirate-iptv-service-taken-down-in-netherlands

([57]) Europol (2023), 'European Financial and Economic Crime Threat Assessment 2023 – The Other Side of the Coin: An Analysis of Financial and Economic Crime', Publications Office of the European Union, Luxembourg.

([58]) EUIPO-Europol (7 March 2022), 'Intellectual Property Crime Threat Assessment 2022', accessible at https://www.europol.europa.eu/publications-events/publications/intellectual-property-crime-threat-assessment-2022.

([59]) Europol (5 July 2024), 'French and Spanish authorities crack down on Chinese money laundering gang', accessible at https://www.europol.europa.eu/media-press/newsroom/news/french-and-spanish-authorities-crack-down-chinese-money-laundering-gang.

([60]) Information contributed to Europol.

([61]) Ibid.

(62) Ibid.

(63) Information contributed to EMPACT IPCCGC OA 1.3.

(64) Europol (2023), 'European Financial and Economic Crime Threat Assessment 2023 – The Other Side of the Coin: An Analysis of Financial and Economic Crime', Publications Office of the European Union, Luxembourg; Europol (2024), 'Decoding the EU's most threatening criminal networks', accessible at https://www.europol.europa.eu/publication-events/main-reports/decoding-eus-most-threatening-criminal-networks#downloads.

(65) Europol (18 July 2024), 'Hit against fake pesticides across South Eastern Europe', accessible at https://www.europol.europa.eu/media-press/newsroom/news/hit-against-fake-pesticides-across-south-eastern-europe.

(66) EUIPO-Europol (7 March 2022), 'Intellectual Property Crime Threat Assessment 2022', accessible at https://www.europol.europa.eu/publications-events/publications/intellectual-property-crime-threat-assessment-2022.

(67) Europol (2023), 'European Financial and Economic Crime Threat Assessment 2023 – The Other Side of the Coin: An Analysis of Financial and Economic Crime', Publications Office of the European Union, Luxembourg.

(68) Shepherd, D. et al., 2023, 'The Impact of Deviant Social Media Influencers and Consumer Characteristics on Purchasing Counterfeit Goods', Deviant Behavior, 44(12), pp. 1746-1760, accessible at https://www.tandfonline.com/doi/full/10.1080/01639625.2023.2233041.

(69) Information contributed to EMPACT IPCCGC OA 1.3.

(70) Europol, (2023), 'European Financial and Economic Crime Threat Assessment 2023 – The Other Side of the Coin: An Analysis of Financial and Economic Crime', Publications Office of the European Union, Luxembourg.

(71) Abbasi I, (February 2023), Azo Materials, accessible at https://www.azom.com/article.aspx?ArticleID=22451.

(72) Near-Field communication. NFC is part RFID (radio-frequency identification) and part Bluetooth. Unlike RFID, NFC tags work in close proximity, giving users more precision. NFC also does not require manual device discovery and synchroniszation, as Bluetooth Low Energy does. The biggest difference between RFID and NFC is the communication method, (information accessible at https://www.nomtek.com/blog/what-are-nfc-tags).

(73) A quick- response code is a type of two- dimensional (2D) bar code that is used to provide easy access to online information through the digital camera on a smartphone or tablet, (information accessible at https://www.techtarget.com/whatis/definition/QR-code-quick-response-code).

(74) Gan J, (2024), '3D-printed Counterfeits on the Rise: How to protect your brand', accessible at https://www.nanomatrixsecure.com/3d-printed-counterfeits-on-the-rise-how-to-protect-your-brand/.

(75) Information contributed under EMPACT IPCGC OA 1.3

(76) EUIPO, (2022), 'Study on the Impact of Artificial intelligence on the infringement and enforcement of copyright and designs', accessible at https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2022_Impact_AI_on_the_Infringement_and_Enforcement_CR_Designs/2022_Impact_AI_on_the_Infringement_and_Enforcement_CR_Designs_FullR_en.pdf.

(77) Information contributed to EMPACT IPCCGC OA 1.3.

(78) Information contributed to Europol.

(79) Europol (2023), 'European Financial and Economic Crime Threat Assessment 2023 - The Other Side of the Coin: An Analysis of Financial and Economic Crime', Publications Office of the European Union, Luxembourg, chapter on IP crime.

(80) Europol (2023), 'European Financial and Economic Crime Threat Assessment 2023 – The Other Side of the Coin: An Analysis of Financial and Economic Crime', Publications Office of the European Union, Luxembourg, chapter on IP crime.

(81) Information contributed to EMPACT IPCCGC OA 1.3.

(82) IOCTA 2024, AAPA, 'Study on malware and audio-visual piracy highlights significant risks to European consumers', 19 September 2022, accessible at https://www.aapa.eu/study-on-malware-and-audiovisual-piracy-highlights-significant-risks-to-european-consumers.

(83) Europol (2024), Decoding the EU's most threatening criminal networks, accessible at https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20report%20on%20Decoding%20the%20EU-s%20most%20threatening%20criminal%20networks.pdf

(84) Information contributed to Europol.

(85) Europol (2023), 'European Financial and Economic Crime Threat Assessment 2023 – The Other Side of the Coin: An Analysis of Financial and Economic Crime', Publications Office of the European Union, Luxembourg.

(86) EUIPO & Europol (2020), 'IP Crime and its link to other serious crimes: Focus on Poly-Criminality'.

(87) Information contributed to Europol.

(88) Europol (2023), 'European Financial and Economic Crime Threat Assessment 2023 – The Other Side of the Coin: An Analysis of Financial and Economic Crime', Publications Office of the European Union, Luxembourg.

(89) Europol (16 January 2023), 'Counterfeit tobacco products worth EUR 17 million seized in France', accessible at https://www.europol.europa.eu/media-press/newsroom/news/counterfeit-tobacco-products-worth-eur-17-million-seized-in-france.

(90) Roediger, R. (2018), '"The Culture of Counterfeiting: the Interplay of Social Norms in the Regulation and Creation of Counterfeit Goods'" (2018),. *International Immersion Program Papers*,. 75,. accessible at: https://chicagounbound.uchicago.edu/international_immersion_program_papers/75.

(91) Directive 2011/62/EU of the European Parliament and of the Council of 8 June 2011 amending Directive 2001/83/EC on the Community code relating to medicinal products for human use, as regards the prevention of the entry into the legal supply chain of falsified medicinal products, accessible at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32011L0062.