# Crime in the Age of Technology

**Oldrich Martinu**
**Gary McEwen**
Europol, The Hague, Netherlands

**Abstract**
The serious and organised crime landscape in the EU has changed drastically in the past years - in large part due to advancements in technology. Criminals quickly adopt and integrate new technologies into their modi operandi or build brand-new business models around them. The use of new technologies by organised crime groups (OCGs) has an impact on criminal activities across the spectrum of serious and organised crime. This includes developments online, such as the expansion of online trade and widespread availability of encrypted communication channels, as well as other aspects of technological innovation such as more accessible and cheaper drone technology, and advanced printing technologies. Technology has become a key component of most, if not all, criminal activities carried out by OCGs in the EU and has afforded organised crime with an unprecedented degree of flexibility.

**Keywords**: card fraud, child sexual exploitation, crime-as-a-service, cybercrime, darknet, data, drones, drugs, encryption, Europol, firearms, human trafficking, illegal immigration, intellectual property, internet, malware, money laundering, online trade, organised crime, prevention, public-private partnerships, ransomware, technology.

## 1. Introduction

Serious and organised crime is a key threat to the security of the EU. Criminal groups and individual criminals continue to generate multi-billion euro profits from their activities in the EU each year. Some parts of the serious and organised crime landscape in the EU have changed drastically in recent years — in large part due to advancements in technology that have had a profound impact on the wider society and economy. While these advances have provided great benefit to society in general, they are often used, abused, or exploited for criminal intent. Technology is therefore now a key component of most, if not all, criminal activities carried out by criminal groups in the EU and has afforded organised crime with an unprecedented degree of flexibility. This flexibility is particularly apparent in the ease with which criminals adapt to changes in society. The vital role of technology for organised crime is clearly reflected in both the SOCTA 2017 (Europol 2017a) and IOCTA 2017 (Europol 2017b). The range and variety of technological advances that can be exploited by criminals is extensive, this article will therefore focus on some of the more noteworthy.

## 2. Crime and the internet

While many technological advances play an important role in a wide range of criminal activities, none has likely had greater impact or influence than the internet. Just as internet can be used to enhance and augment the daily lives of everyday citizens, and the functioning of businesses and services, it has not only given rise to a completely new form of crime, but can facilitate or assist criminality across almost all other crime areas.

The internet is of course fundamentally a source of information, and an environment where communities of like-minded individuals can meet. The list of information that could be used to assist criminals is essentially endless, but key examples include access to detailed map data, including satellite and street-views for reconnaissance, shipping routes and schedules, tutorials, guides and recipes for drugs or explosives, and tips on operational security.

### Cybercrime

Cybercrime is a global phenomenon, and is as borderless as the internet itself. The attack surface continues to grow as society becomes increasingly digitised, with more citizens, businesses, public services and devices connecting to the internet. Moreover, the potential for one attacker to affect many victims is scaling exponentially. The term 'cybercrime' encompasses a broad range of different criminal threats however. The most threatening aspects of cybercrime involve crimes such as the distribution of **ransomware** and other **malware**, **fraud involving non-cash payments** and the **online trade in child sexual exploitation material**.

### Cyber-dependent crime

Cyber-dependent crime can be defined as any crime that can only be committed using computers, computer networks or other forms of information communication technology (ICT). In essence, without the internet these crimes could not be committed. It includes such activity as the creation and spread of malware, hacking to steal sensitive personal or industry data and denial of service attacks to cause reputational damage.

A mature Crime-as-a-Service business model underpins cybercrime and provides easy access to tools and services across the entire spectrum of cyber-criminality, from entry-level to top-tier actors, or any other party, including those with other motivations such as hacktivists or even terrorists. The development and distribution of malware continues to be the cornerstone for the majority of cybercrime. Information-stealing malware, such as banking Trojans, represent a significant threat, although ransomware has become the leading malware in terms of threat and impact, as demonstrated by with the scale of the WannaCry and NotPetya attacks of mid-2017. Network intrusions that result in unlawful access to or disclosure of private data (data breaches) or intellectual property are growing in frequency and scale, with hundreds of millions of records compromised globally each year.

Cybercrime continues to expand in scope and impact. Digital economies and societies are an attractive target for cybercriminals. Technological innovation holds exciting prospects for businesses and citizens alike, but also creates new attack vectors for those criminals seeking to capitalise on these developments. Increasing internet connectivity by citizens, businesses and the public sector, along with the exponentially growing number of connected devices and sensors as part of the Internet of Things is creating new opportunities for cybercriminals.

### Cyber-facilitated crime

Cyber-facilitated crimes are crimes which can be conducted either online or offline. The role played by the internet is to increase the scale, geographic scope, and speed of these crimes. **Online child sexual exploitation** epitomises the worst aspects of cyber-facilitated crime. The hands-on abuse of vulnerable minors occurs very much in the real world, but it is captured, shared, distributed, encouraged and even directed over the internet. The internet provides offenders and potential offenders with an environment in which they can operate with an enhanced level of safety and anonymity; where they can research, target, and groom minors for abuse. Moreover, the Darknet hosts a growing number of forums dedicated specifically to the production, sharing and distribution of child sexual exploitation material. The internet additionally offers a wide range of internet-based applications, such as Peer-to-peer file sharing, and secure data storage, which facilitate this crime.

**Fraud involving non-cash payments** is an ever-present threat. Many aspects of this crime area are highly organised, highly specialised, and constantly evolving to adapt to both industry measures to combat it, and new payment technologies. This crime priority is divided into two, relatively distinct crime areas: card-

not-present (CNP) fraud, which occurs largely online and card-present fraud, which typically occurs at retail outlets and ATMs.

Fuelled by the availability of compromised card data stemming from data breaches, phishing, and malware, the fraudulent use of compromised card data to make purchases online continues to plague the e-commerce industry. The retail sector is predictably one of the hardest sectors hit; however, airline ticket fraud continues to have a high impact and priority across Europe. Fraud relating to accommodation (e.g. hotels booked using compromised cards) is on the increase. Both individuals and OCGs are involved in this type of activity. Where OCGs are involved, this crime is often linked to other crimes such as trafficking in human beings (THB) or drugs, and illegal immigration – crimes where transport and temporary accommodation is required to facilitate the criminal activity.

Technology is also providing criminals with new methods of intrusion into ATMs and similar systems. By drilling or burning small holes into an ATM case, attackers can reach the ATM's computer hardware components. The attackers use this access to control the ATM's operating system and force it to dispense cash.

Criminal groups involved in the theft of motor vehicles increasingly rely on high tech tools to gain access to vehicles and to overcome security measures. Information on how to overcome car security systems can be easily accessed via online messaging boards and websites. As vehicles increasingly rely on keyless entry systems and other new technologies to aid navigation, driving and entertainment, this trend is set to intensify over the coming years.

### The online trade in illicit goods

Online platforms operating in the legal economy have had a profound impact on business models, shopping experiences and customer expectations. The multiplication of sales platforms makes online trade easier, more accessible and cheaper. This development has been mirrored in the online trade in **illicit goods and services** as criminals, like legitimate traders, seek opportunities to grow their businesses. Illicit online markets, both on the surface web and Darknet, provide criminal vendors the opportunity to purvey all manner of illicit commodities. Many of these illicit goods, such as cybercrime toolkits or fake documents, are key enablers for further criminality.

The **drugs market** is undoubtedly the largest criminal market on the Darknet, offering almost every class of drug for worldwide dispatch. Earlier this year, the now defunct AlphaBay, one of the largest Darknet markets, had over 250 000 separate listings for drugs, accounting for almost 68% of all listings. 30% of the drugs listings related to Class A drugs. Prior to this year's law enforcement action, some studies suggest that the total monthly drugs revenue of the top eight Darknet markets ranged between EUR 10.6 million and EUR 18.7 million, when prescription drugs, alcohol and tobacco were excluded.

Infringements of **intellectual property rights (IPR)** are a widespread and ever-increasing worldwide phenomenon, exacerbated by online markets. The impact of counterfeiting is high in the European Union, with counterfeit and pirated products amounting to up to 5% of imports. Most counterfeit products can be sold on the surface web, being presented as (or mixed with) genuine products. Sale of counterfeit products on the Darknet tends to relate to those commodities that are explicitly illegal, such as counterfeit bank notes and fake ID documents.

Compromised **data** is another key commodity commonly traded online, and subsequently used for the furtherance of fraud. Typically, this is financial data such as compromised payment card data or bank account logins. However, any data that could be exploited to commit fraud or other crimes is also readily available for sale. This includes everything from lists of full personal details and scanned documents to email lists and online account logins.

Firearms are increasingly traded on online platforms including Darknet marketplaces. Both individual criminals and OCGs can obtain illegal firearms via these markets. This online trade allows individuals with no or limited connections to organised crime to procure firearms. Given the number of terrorist attacks throughout 2016/2017, the potential easy availability of firearms and explosives is a worrying trend.

## 3. Communications technology

There have been many developments in communications technology in the last few decades - innovations that have vastly improved the availability, speed, range, and security of channels of communication.

In parallel with this are developments in the devices through which these channels operate. As an example, the modern mobile phone is not simply a telephone, but a fully functional, internet-enabled computer. The internet, coupled with almost ubiquitous access via smart devices has spawned a myriad of communication applications and options, from text-based instant messaging to Voice-over-internet protocols (VoIP) and live video streaming.

Criminals make use of all and every communication channel available, not just for their own internal communication, but also to contact potential victims, which modern technology allows them to do in unprecedented numbers. For example, email can be used for phishing campaigns or to distribute malware, and social media can be used to find and groom victims for online child abuse.

Law enforcement is witnessing a transition into the use of secure apps and other services by criminals across all crime areas. The majority of the apps used are the everyday brand names popular with the general populace. As not only these applications, but also the devices they operate on, become increasingly secure, incorporating end-to-end encryption for example, they are readily adopted by criminals seeking reliable, secure communications. This creates additional challenges for law enforcement as it renders many traditional investigative techniques, such as wire-tapping, ineffective.

### Encryption

While the use of encryption is increasingly important to private citizens and industry for protecting their data, thereby denying it to criminals who desire it for criminal purposes, the growing use of legitimate anonymity and encryption services by criminals and other malicious actors poses a serious impediment to the detection, investigation and prosecution of crime. This is pertinent across all crime areas, including terrorism.

## 4. Criminal finances and money laundering

Criminal finance has benefitted greatly from technological innovation such as the shift to online solutions for most financial services provided for the legitimate economy. The emergence of new forms of payment such as cryptocurrencies and the appearance of a plethora of highly diverse and often difficult to regulate online payment and banking platforms has afforded criminals with new ways of financing and expanding their criminal businesses. The rapid processing of transactions across multiple jurisdictions and the proliferation of encryption and anonymisation tools represent some of the most significant obstacles encountered in increasingly complex and technically demanding financial investigations.

Sitting largely outside the regulated financial sector, cryptocurrencies are increasingly exploited by criminals. For the past few years, this has almost universally meant Bitcoin, the criminal abuse of which has grown in parallel with its general adoption and legitimate use. It is the most commonly used currency for criminal-to-criminal payments within cybercrime, for example when purchasing or renting cybercrime tools or services on the digital underground. It is the *only* currency accepted on most Darknet marketplaces and automated card shops, and is the currency required by almost all of today's ransomware and DDoS extortion demands. There are also a growing number of cases where it is used for crimes outside of cyberspace, as payment for ransom in kidnappings for example.

## 5. Industrialisation and manufacturing

Many crime areas have benefitted from developments in, or the increased availability of technology associated with manufacturing and the industrialisation of processes. One such area is the drugs market. The market for drugs remains the largest criminal market in the EU. 45% of the criminal groups active in the EU are involved in the production, trafficking or distribution of various types of drugs across Member States, generating multi-billion euro profits for the groups involved in this activity. Technical innovation and the accessibility of sophisticated equipment has allowed criminal groups to maximise production output. Large-scale cannabis cultivation sites are often maintained using professional growing equipment such as climate control systems, CO2 and ozone generators. Similarly, laboratories manufacturing synthetic drugs feature advanced equipment and production lines capable of producing synthetic drugs on an industrial scale. The production, trafficking and distribution of illicit drugs remains a key threat to the EU that is only enhanced by the availability of advanced production equipment and the shift to online platforms used to trade these illicit drugs.

Other crimes that have benefited from advances in manufacturing technology are those that concern the production of other illicit commodities, such as counterfeit products, including counterfeit banknotes. Industrialisation, automating and miniaturisation have all contributed to faster and greater production of higher quality (in terms of apparent authenticity) counterfeit goods.

### 3D-printing

One particular manufacturing technology that has demonstrated its potential for criminal abuse is that of 3D printing. Already readily available, 3D printers can print in a wide variety of materials including ceramics, plastic and metals. Moreover, assuming that the appropriate files can be obtained, almost any object can be printed with those materials. It is already possible to print handguns, and magazines, and as bigger printers become available, it will be possible to print larger objects. Such technology is already used by ATM skimmers to produce skimming devices and equipment (such as ATM panels). Developments in 3D printing technology have seen many consumer 3D printers hit the markets making it easier for criminals to acquire the technology they need to make the custom components required for any illicit purpose.

### Drone technology

Advances in drone technology are expected to have an impact on a number of areas of criminality - essentially any crime that could exploit a low profile mechanism of transporting or delivering illicit goods. The trafficking and distribution of drugs or other contraband are obvious examples. As drones develop greater travel distance and the ability of carrying heavier loads, as well as becoming more affordable, criminal groups involved in drug trafficking will likely invest in drone technology in order to avoid checks at border crossing points, ports and airports.

The availability of drones will open up a number of opportunities for criminals and other malicious actors. Drones will allow for reconnaissance and counter surveillance, and it has already been demonstrated that civilian drones can be mounted with firearms, including automatic weapons, or potentially even explosives.

## 6. The law enforcement response

It is clear that that any developments in the use of technology by criminals must be matched and countered by an appropriate and effective law enforcement response. There is an obvious challenge here for law enforcement to not only keep pace with new technological developments, but with emerging crimes and a continually changing threat landscape.

Cybercrime, as a relatively new crime area, is a good example of this, and poses many challenges peculiar to that crime area. Attribution – determining who is behind an attack, and where they globally are located, is especially challenging, particularly in an environment where cybercriminals share tactics and tools with malicious actors with other motivations, such as hacktivist or nation state actors. Furthermore, many aspects of cybercrime are developing rapidly, requiring specific expert knowledge and the use of cutting-edge investigative techniques and advanced digital forensic tools.

In order for law enforcement to effectively fight technology-enabled crime, it must of course embrace technology itself. Technology can also be a significant aid to law enforcement authorities in the fight against serious and organised crime, often using the very same technology abused by criminals. For example, mapping and geo-location tools have proved to be invaluable for planning and co-ordination during large events such as public protests, especially if combined with other technologies such as drones and social media monitoring on the internet. Developments in artificial intelligence and machine learning could have significant benefits when considering predictive policing software, or the processing of the increasing volumes of (big) data that potentially arise from modern police investigations.

Naturally, the use of such technology by law enforcement has considerable resource implications, not just in gaining access to or ownership of the technology in question, but in ensuring that adequate training is available to capitalise on the technology. A harmonised and co-ordinated approach towards training and capacity building across the EU is therefore essential.

Many aspects of the criminal abuse of technology are out-with the implicit remit of law enforcement, and instead lie with regulators and policy makers. This applies to issues such as encryption, or the commercial availability and use of drones. Emerging technology fields such the Internet of Things (IoT) for example, have resulted in the creation of new legal, policy and regulatory challenges, and demand cooperation between different sectors as well as different stakeholders. In such discussions, it is essential for law enforcement to

have a voice, and to provide guidance and recommendations regarding the needs and requirements of law enforcement in order to be able to continue effectively combatting crime where these technologies are involved.

Combatting crime however is not something law enforcement can or should shoulder alone. A critical factor for success is therefore to develop working relationships with private industry and academia. Industry and academia often have access to data, resources, technology and expertise that is simply unavailable to law enforcement. Moreover, they are often willing partners, particularly when a threat affects their industry. An excellent example of this are Europol's Global Airport Action Days that target fraudsters travelling on tickets bought using compromised payment cards. Such events bring together law enforcement, airline companies, travel agents, banks, and payment card companies from over 60 countries round the world, and have had a significant impact on this threat area.

This level of joint working and engagement with the private sector represents a significant change in the mind-set for many law enforcement agencies, whereas previously they may only have 'engaged' with companies through court orders and warrants. This formation of successful and mutually beneficial collaborative partnerships with non-law enforcement bodies demonstrates how law enforcement has had to adapt to factors other than emerging technologies, and has changed the way it interacts with other facets of society.

Another such development is the growing involvement of law enforcement in prevention measures. While the *prevention and detection* of crime has long been the mission of law enforcement, the focus has typically been on the detection. However, prevention has proved to be a key non-investigative measure for many crime areas, and another with which law enforcement can work closely with the private sector. Prevention measures aim to address the lack of knowledge or information about potential threats from various technologies that often leaves potential victims vulnerable to more tech-savvy criminals, or attempts to dissuade would-be criminals from following the wrong path. Simply raising awareness of these threats, and educating potential victims, can have significant impact on the success of malicious actors. This is again, particularly pertinent in cyberspace where a little knowledge can protect victims from attacks such as phishing, malware or sexual extortion.

Technology will continue to adapt and develop, often at a pace greater than either law enforcement or potential victims can maintain their knowledge or perhaps even awareness of it. New and developing technology will also continue to create new attack vectors, and further expand existing ones. While criminals continue to abuse and exploit new and existing technologies - in order to enhance their criminal activities, or perhaps as a key component of their criminality - it is essential that law enforcement continues to use all the resources, tools, and opportunities at its disposal. Public-private partnerships, the development of innovative technical solutions, prevention measures, and training and capacity building are all required in order for law enforcement to remain an effective countermeasure to crime in the age of technology.

## References


- Europol (2015) Guidance and recommendations regarding logical attacks on ATMs.
  Retrieved from https://www.ncr.com/sites/default/files/brochures/EuroPol_Guidance-Recommendations-ATM-logical-attacks.pdf
- Europol (2017a) Serious and Organised Crime Threat Assessment.
  Retrieved from https://www.europol.europa.eu/socta/2017/resources/socta-2017.pdf
- Europol (2017b) 2017 Internet Organised Crime Threat Assessment.
  Retrieved from https://www.europol.europa.eu/sites/default/files/documents/iocta2017.pdf
- RAND Europe (2016) Internet-facilitated drugs trade – An analysis of the size, scope and the role of the Netherlands, p41.
  Retrieved from https://www.rand.org/pubs/research_reports/RR1607.html