EXECUTIVE SUMMARY

The Internet Organised Crime Threat Assessment (iOCTA) informs decision makers at strategic, policy and tactical levels about on-going developments and emerging threats of cybercrime affecting governments, businesses and citizens in the EU. It draws on highly valuable contributions from law enforcement authorities in the EU and from other countries. Partners in the private sector and academia also provided important input to the report.

Combating cybercrime requires a different approach from that which has been traditionally taken in respect of most crimes. In contrast to the off-line world where criminals normally need to be physically present at the crime scene and can typically only commit one offence at a time (i.e. rob one bank or burgle one house at a time), criminals in cyberspace do not need to be close to the crime scene, they might never even travel to the target country, and can attack a large number of victims globally with minimum effort and risk by hiding their identity.

In practice, the need for a different approach to tackle cybercrime confronts police forces with new challenges. This calls for much stronger cross-border cooperation and orientation. New partners need to be found and integrated into existing cooperation frameworks, as we have seen with the European Cybercrime Centre (EC3) at Europol. In many jurisdictions outside the EU there are, however, no adequate legal frameworks in place for judicial cooperation. In fact, the whole concept of a territorially-based investigative approach conflicts with the borderless nature of cybercrime.

Even within the EU the differences in legislation and legal instruments to detect, attribute and exchange information in relation to cybercrimes cause significant impediments. The latter applies not only to law enforcement, but also to its cooperation with the private sector. While there is an overflow of information available to millions of citizens and businesses, few effective measures are available to law enforcement to access that information in order to aid the apprehension of criminals that undermine public safety and economic interests. On top of that, economic austerity has hampered the ability of EU law enforcement (LE) to adapt swiftly and sufficiently to the new realities that cybercrime has introduced.

Meanwhile cybercrime itself is a growing problem. Trends suggest considerable increases in the scope, sophistication, number and types of attacks, number of victims and economic damage. There are two important factors worth highlighting in this context: *Crime-as-a-Service* and *anonymisation*.

The Crime-as-a-Service (CaaS) business model drives the digital underground economy by providing a wide range of commercial services that facilitate almost any type of cybercrime. Criminals are freely able to procure such services, such as the rental of botnets, denial-of-service attacks, malware development, data theft and password cracking, to commit crimes themselves. This has facilitated a move by traditional organised crime groups (OCGs) into cybercrime areas. The financial gain that cybercrime experts have from offering these services stimulates the commercialisation of cybercrime as well as its innovation and further sophistication.

Relationships between cybercriminals are often transient or transactional and although they may form more coherent, project-based groups, they lack the structure and hierarchy of a traditional organised crime group. The current definitions of organised crime therefore do not reflect the digital underground economy, although this behaviour may reflect how all serious crime will be organised in the future.

The anonymisation techniques used in parts of the Internet, known as Darknets, allow users to communicate freely without the risk of being traced. These are perfectly legitimate tools for citizens to protect their privacy. However, the features of these privacy networks are also of primary interest to criminals that abuse such anonymity on a massive scale for illicit online trade in drugs, weapons, stolen goods, forged IDs and child sexual exploitation.

Criminal marketplaces are complemented by anonymous payment mechanisms such as virtual currencies. While in principle legitimate, they are abused by criminals for criminal transactions and money laundering. Centralised schemes such as WebMoney are commonly exploited.

However crypto-currencies continue to evolve and it is likely that more niche currencies will develop, tailored towards illicit activity and providing greater security and true anonymity.

This report highlights important developments in several areas of online crime. The changes in the production of malware are increasing rapidly in scale and sophistication. These are producing cybercrime capabilities ranging from simple key logging and theft of sensitive data, to ransomware and sophisticated and complex banking Trojans. Malware is also essential in creating and controlling botnets. Recent developments in the use of peer-to-peer networks to host command and control infrastructure create additional difficulties for law enforcement to disrupt or takedown botnets.

In the area of payment fraud the size of financial losses due to online fraud has surpassed the damage due to payment fraud with physical cards. This causes huge losses, not only for the payment card issuers, but also for airlines, hotels and online retailers.

Child sexual exploitation online continues to be a major concern with offences ranging from sexual extortion and grooming, to self-produced child abuse material (CAM) and live streaming, which pose particular investigative challenges. Offenders are facilitated by many of the same services and products as typical cybercriminals including anonymisation tools, secure e-mail, bulletproof hosting and virtual currencies.

Current and future developments such as Big and Fast Data, the Internet of Everything, wearable devices, augmented reality, cloud computing, artificial intelligence and the transition to IPv6 will provide additional attack vectors and an increased attack surface for criminals. This will be exacerbated by how emerging and new technologies will be used and how they will influence people's online behaviour.

KEY FINDINGS

Global Trends

- Globally an estimated **2.8 billion people** and **over 10 billion Internet-enabled devices** access the Internet. The growing adoption of the Internet provides increasing opportunities to commit crime **facilitated, enabled or amplified by the Internet**.

- The advent of the **Internet of Everything (IoE)** combined with the ever increasing number of Internet users globally creates a **broader attack surface**, **new attack vectors and more points of entry,** including social engineering methods, for criminals to exploit, making **endpoint security** even more important.

- As the scale of Internet connectivity, including mobile access, continues to spread, **EU** citizens and organisations will be subjected to a larger volume of **attacks from previously under-connected areas** of the world.

- The **EU** will remain **a key target for cybercrime** activities because of its relative wealth, high degree of Internet penetration, its advanced Internet infrastructure and increasingly Internet-dependent economies and payment systems.

- Attacks predominantly originate from **jurisdictions outside of the EU**, particularly from countries where the proceeds of online crime notably outweigh income from legitimate activities.

- In general **cybercrime is increasing in scale and impact**; while there is a lack of reliable figures, trends suggest considerable increases in scope, sophistication, number and types of attacks, number of victims and economic damage.

- Cybercriminals need not be present in target countries and are able to **conduct crime against large numbers of victims** across different countries simultaneously with **minimum effort and risk**.

- The **trans-national nature of cybercrime** creates challenges for law enforcement to **secure and analyse electronic** evidence in countries from where the attacks originate, where there may be no or ineffective legal tools in place or insufficient capacity.

A Service-Based Criminal Industry

- A professional, continuously evolving, **service-based criminal industry** drives the innovation of tools and methods used by criminals and facilitates the **digital underground** through a multitude of complementary services, extending attack capacity to those otherwise lacking the skills or capabilities.

- **Traditional organised crime groups** (OCGs), including those with a mafia-style structure are beginning to use the service-based nature of the cybercrime market to carry out more sophisticated crimes, **buying access to the technical skills** they require. This trend towards adopting the cybercrime features of a more transient, transactional and less structured organisational model may reflect how all serious crime will be organised in the future.

- **Underground forums** provide cybercriminals with a **nexus** for the **trade of goods and services** and a hub for **networking**, creating an organised set of criminal relationships from an otherwise disparate population.

- A **number of legitimate features of the Internet** are being exploited by cybercriminals such as **anonymisation, encryption and virtual currencies**, creating challenges for law enforcement especially in regards to tracing the sources of criminal activity.

- **Malware** is becoming **increasingly sophisticated, intelligent, versatile, available**, and is affecting a broader range of targets and devices.

- **E-commerce related fraud has increased** in line with the growing number of online payments, affecting major industries such as airlines and hotels. Key factors fuelling the increase are **large-scale data breaches** supplying compromised card data to underground forums and a **low prevalence of preventive measures** implemented by merchants and the financial industry, such as 3D Secure.

- There is a **value chain of e-commerce fraud** which includes trading compromised credit card details on underground forums, using these to make online purchases and monetising the goods via money mules.

The Abuse of Anonymisation

- **Darknets** and other environments offering a high degree of anonymity are increasingly hosting hidden services and marketplaces devoted to traditional types of crime, such as the **drug trade, selling stolen goods, weapons, compromised credit card details, forged documents, fake IDs, and the trafficking of human beings**.

- **Child sex offenders and producers** make increasing use of the Darknet and other similar areas. The nature of child sexual exploitation forums on the Darknet promotes the abuse of new victims as the provision of new child abuse material is typically used as an entry token.

- New forms of child sexual exploitation online such as the **live streaming of on-demand abuse of children** present new challenges for law enforcement.

- Through the mainstream use of social media and availability of Internet-connected devices, the **creation and online dissemination of sexually explicit images,** sometimes **self-generated,** and the use of such images for **sexual extortion** is becoming increasingly common.

KEY RECOMMENDATIONS

Prevention - Awareness

- Law enforcement should **increase its visibility and presence online** to address the phenomenon of minimisation of authority in cyberspace in order to increase public confidence in the security of the internet and offer a credible deterrent to criminals.

- Law enforcement should co-operate with third parties, including industry, in running **awareness campaigns** about **cyber threats**. This should involve measures highlighting the importance of **'digital hygiene'** and endpoint security, the importance of **security by design**, and providing more online resources for **victims to report crime and seek help and support**.

- In this context, law enforcement should support the development of **communication programmes** to help the general public manage and maintain their privacy online and to establish the **norms of social conduct in cyberspace**. Particular focus should be given to children at a young age, stressing the need for **safe behaviour online**.

- Law enforcement should **establish a channel** through which details of **compromised financial data** discovered in the course of an investigation can be relayed to the financial sector in order to mitigate potential or further fraud.

Prevention - Capacity Building & Training

- Law enforcement needs to **invest in capacity building** with a view to acquiring the necessary skills, expertise, knowledge and tools to perform **cybercrime investigations, Big Data analysis and Internet of Everything (IoE) related digital forensics**. This should range from **first responder training** on the basic principles of cybercrime, to team leaders managing international cybercrime investigations and ideally be coordinated at an EU level to ensure harmonization. Synergies with the public and private sector and academia should be considered when developing new training courses.

- Law enforcement should urgently develop its understanding of **how virtual currencies operate**, and how to recognise the **wide variety of digital accounts** which may hold a suspect's digital assets as a key means to seize the proceeds of crime.

Partnerships

- As **cybercrime investigations and electronic evidence** often span **multiple jurisdictions**, it is essential that law enforcement efforts in combating cybercrime are sufficiently supported at the **legal and policy levels**. Together with Eurojust and other relevant stakeholders, this will require **developing more efficient and effective legal tools**, taking into account the current limitations of the Mutual Legal Assistance Treaty (MLAT) process, and further **harmonisation of legislation** across the EU where appropriate.

- The dynamic, evolving and trans-national nature of cybercrime demands an equally diverse and flexible response by law enforcement in close **international strategic and operational partnership** with all relevant stakeholders. Public-private partnerships and co-operation and co-ordination with all relevant stakeholders, including the academic community, will play an increasingly important role.

- As a number of **cyber threats emanate from non-EU states**, law enforcement needs to explore strategic and operational cooperation and capacity building possibilities with law enforcement in states that criminals operate from. This must be intelligence led and coordinated with relevant stakeholders to prevent overlaps and duplication of effort.

Protection

- In the context of the **proposed EU Directive on Network and Information Security**, there is a need for a **balanced and harmonised approach to information sharing and reporting from national and international stakeholder communities**. This should include reporting of certain suspicious activities to national cybercrime centres and the European Cybercrime Centre at Europol.

- Legislators in the EU need to provide law enforcement with the **legal instruments** it requires to allow it to **disrupt and investigate criminal activity**, and to **access the information** it needs in order to **apprehend criminals** that undermine public safety and economic interests.

- Law enforcement should prepare for the **transition period from IPv4 to IPv6** and the potential abuse of ICANN's new generic top-level domains. This should include **acquiring the necessary knowledge, skills and forensic tools**.

Investigation

- Law enforcement should concentrate on **pro-active, intelligence-led approaches to combating cybercrime** in a prioritised manner, focusing on high impact areas. This will require **leveraging existing platforms,** such as the **European Cybercrime Centre** and its respective Focal Points and **Interpol's Global Complex for Innovation**, to allow for the pooling of intelligence to better co-ordinate activity and make best use of limited resources.

- In order to measure the **scale and scope of cybercrime** in a consistent way, there is a need for **improved monitoring, reporting and sharing of cybercrime-related data** in a standardised EU-wide manner. Law enforcement should work with all relevant stakeholders on developing the necessary processes, protocols and trust relationships, considering the tools and services provided by the European Cybercrime Centre and the centre's potential role as an **information and intelligence sharing hub**.

- Common **digital forensics standards and procedures**, including tools and data formats, to facilitate **cross-border investigations and the exchange of electronic evidence** should be developed and implemented.

- Law enforcement should focus its activities on the **top identified criminal forums** and **marketplaces** and on **targeting individuals with the highest reputations** on these platforms. Given the present predominant use of the Russian language, many law enforcement services will need to increase or adapt their language capabilities.

- Law enforcement should focus with priority on **dismantling criminal infrastructure**, **disrupting the key services** that support or enable cybercrime and prosecuting those responsible for malware development, as the numbers of highly skilled cybercriminals are limited and their skills are hard to replace.

- Law enforcement should target for **apprehension and prosecution** the **developers of malware**. Many of the more pernicious variants are controlled by closed criminal circles, the disruption of which would have considerable impact.

- Following the successful operations against airline sector fraud other areas of Internet facilitated **payment card abuse should be identified and addressed** on a global, European or national level.

- The increase of both cyber-enabled and facilitated crime should be met with a proportionate **increase of relevant resources and skills** within law enforcement.

- In the context of relevant EU legal frameworks and regulations, law enforcement needs to be equipped with the tools and techniques necessary to **address the increase in and further sophistication of encryption and anonymisation**.