



The Internet Organised Crime Threat Assessment (iOCTA)

2014



EUROPEAN CYBERCRIME CENTRE

EC³

EUROPOL

MAKING EUROPE SAFER

COPYRIGHT

© European Police Office, 2014

Reproduction is authorised provided the source is acknowledged.

This publication and more information on Europol are available on the Internet:

Website: www.europol.europa.eu

Facebook: www.facebook.com/Europol

Twitter: [@Europol_EU](https://twitter.com/Europol_EU)

YouTube: www.youtube.com/EUROPOLtube

<https://t.me/learningnets>



EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

The Internet Organised Crime Threat Assessment (iOCTA)

TABLE OF CONTENTS

▶	FOREWORD	5
▶	ABBREVIATIONS	7
▶	EXECUTIVE SUMMARY	9
▶	KEY FINDINGS	11
▶	KEY RECOMMENDATIONS	13
▶	CHAPTER 1 - INTRODUCTION	15
	Aim	15
	Scope	15
	Methodology and acknowledgements	16
▶	CHAPTER 2 - THE STATE OF THE INTERNET	17
▶	CHAPTER 3 - CRIME AREAS	19
	3.1 Crime-as-a-Service	19
	3.2 Malware	23
	3.3 Child sexual exploitation online	28
	3.4 Payment fraud	34
	3.5 Criminal finances online	41
	3.6 Crimes relating to social engineering	44
	3.7 Data breaches and network intrusions	48
	3.8 Vulnerabilities of critical infrastructure	50
▶	CHAPTER 4 - FACILITATORS AND RELEVANT FACTORS	53
	4.1 Social networking	53
	4.2 Anonymisation tools	55
	4.3 Internet governance	56
	4.4 The future is already here	59
▶	CHAPTER 5 - GEOGRAPHICAL DISTRIBUTION	65
▶	CHAPTER 6 - LAW ENFORCEMENT	69
▶	CHAPTER 7 - CONCLUSIONS	71
▶	APPENDICES	73
	A1. The criminal exploitation of the Internet: Views of the academic advisors	73
	A2. Cyber legislation	77
	A3. The cyberpsychology of Internet facilitated organised crime	81
	A4. The fight against cybercrime through the lens of a data protection believer – a commentary	89



EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

The Internet Organised Crime Threat Assessment (iOCTA)

FOREWORD

I am pleased to present the 2014 Internet Organised Crime Threat Assessment (iOCTA), the first of its kind prepared by the European Cybercrime Centre (EC3) at Europol.

This report is EC3's flagship strategic product, the delivery of which is one of the prioritised actions for 2014 within the EU's multi-annual policy cycle for serious organised crime. It informs decision makers at strategic, policy and tactical levels about on-going developments and emerging threats in the field of cybercrime affecting governments, businesses and citizens in the EU. Contributions by EU Member States and the expert input of Europol staff, combined with input from the private sector and academia, have been essential for the research and in-depth analysis leading to this report.

With more than 2.8 billion people using the Internet across the globe and over 10 billion Internet-facing devices in existence, the report highlights the increasing opportunities to commit crimes facilitated, enabled or amplified by the Internet. For many, being online is no longer the exception but the norm, often without the individual being aware. This provides a broader attack surface and multiple areas of peoples' lives for criminals to exploit. Because of Europe's high levels of Internet access and increasingly Internet-dependent economies, this poses a significant threat to the safety and prosperity of the EU in particular.

The 2014 iOCTA identifies the growing commercialisation of cybercrime as one of its principal trends. A service-based criminal business model drives innovation and provides access to a wide range of services facilitating cybercrime. As a consequence, traditional organised crime groups are now able to step into cybercrime by purchasing bespoke skills and tools to support their criminal business.

The transnational nature of cybercrime, combined with an increasing sophistication of attacks, the problem of attribution, the abuse of legitimate services, and inadequate legislation are among the other main challenges the report identifies for law enforcement.



Based on these findings, the 2014 iOCTA delivers a set of recommendations for law enforcement to successfully address cybercrime in a diverse and flexible manner.

As highlighted in the report, Europol's EC3 can play an important role in supporting EU law enforcement in the fight against cybercrime, for instance through the exchange of relevant cybercrime intelligence and the support of multi-national operations. These recommendations call for enhanced collaborative action by Member States and other stakeholders to ensure a more effective and integrated response overall.

I am confident that the 2014 iOCTA, and Europol's work in supporting the implementation of the proposed recommendations, will contribute to an effective international law enforcement response to cybercrime. I look forward to our continued engagement and cooperation with law enforcement agencies and other partners in the EU and beyond.

Rob Wainwright
Director of Europol



EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

The Internet Organised Crime Threat Assessment (iOCTA)

ABBREVIATIONS

AIS	Automatic Identification System	IoT	Internet of Things
ATM	automated teller machine	IP	Internet protocol
BYOD	bring-your-own-device	IPv	Internet Protocol version
BYOC	bring-your-own-cloud	ISP	Internet service provider
BYOX	bring-your-own-everything	J-CAT	Joint Cybercrime Action Taskforce
CaaS	Crime-as-a-Service	LE	law enforcement
CAM	child abuse material	M2M	machine to machine
C&C	command and control	MaaS	Malware-as-a-Service
CERT	computer emergency response team	MLAT	Mutual Legal Assistance Treaty
CNP	card-not-present	MS	Member State(s)
CSE	child sexual exploitation	NIST	National Institute of Standards and Technology
CSECO	commercial sexual exploitation of children online	OCG	organised crime group
CSEO	child sexual exploitation online	OSINT	open-source intelligence
DDoS	Distributed Denial of Service	P2M	people to machine
DHCP	Dynamic Host Configuration Protocol	P2P	peer to peer, or people to people
DNS	Domain Name System	PaaS	Platform-as-a-Service
DoS	Denial of Service	PCF	payment card fraud
EC3	European Cybercrime Centre	PGP	Pretty Good Privacy
ECI	European Critical Infrastructure	PIN	personal identification number
EMPACT	European Multidisciplinary Platform Against Criminal Threats	PoS	point-of-sale
EMV	Europay, MasterCard and Visa	RAT	Remote Access Tool
EU	European Union	SaaS	Software-as-a-Service
FP	Focal Point	SCADA	Supervisory Control and Data Acquisition
GPS	global positioning system	SEPA	Single Euro Payments Area
I2P	Invisible Internet Project	SMS	short message service
IaaS	Infrastructure-as-a-Service	SPOC	Single Points of Contact
ICS	Industrial Control System	TCP	Transmission Control Protocol
ICT	information and communications technology	TCSO	travelling child sex offender
iOCTA	Internet Organised Crime Threat Assessment	TOR	The Onion Router
IoE	Internet of Everything	URL	uniform resource locator
		USB	universal serial bus
		VoIP	Voice-over-Internet Protocol
		VPN	virtual private network



EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

The Internet Organised Crime Threat Assessment (iOCTA)

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 **broadier 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.



EUROPEAN CYBERCRIME CENTRE
EC³
EUROPOL

The Internet Organised Crime Threat Assessment (iOCTA)

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**.



EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

The Internet Organised Crime Threat Assessment (iOCTA)

CHAPTER 1 INTRODUCTION

The delivery of the Internet Organised Crime Threat Assessment (iOCTA) is one of the prioritised actions for 2014 agreed within the framework of the EMPACT policy cycle. EMPACT¹ is aimed at coordinating the efforts of Member States' law enforcement authorities in combating organised crime affecting the EU. Cybercrime is one of the priorities identified for the period 2014-2017, subdivided into three areas: cyber attacks, online child sexual exploitation and payment fraud.

The iOCTA was drafted by the European Cybercrime Centre (EC3) at Europol with strong support and input from Member States and cooperation partners.

Aim

The aim of the iOCTA is to inform decision-makers at strategic, policy and tactical levels to fight cybercrime more effectively and to better protect online society against cyber threats. In particular, this threat assessment is intended to inform priority setting for the EMPACT Operational Action Plan for 2015 in the three sub-areas of the cybercrime priority.

For this purpose the iOCTA provides a description and analysis of the latest trends and the current impact of cybercrime within the EU. It also includes a forward-looking assessment, presenting analyses of future risks and emerging threats and will provide recommendations and proposed lines of action with the aim of informing the strategic planning of EU law enforcement and policy makers.



*Troels Oerting, Head of Europol's
European Cybercrime Centre (EC3)*

Scope

The assessment focuses on the crime areas that fall under the mandate of Europol's EC3, i.e. those investigated by Focal Points Cyborg (*Internet-enabled crime*²), Twins (child sexual exploitation online) and Terminal (payment card fraud). It also addresses other areas of criminality where they directly impact or operate in parallel with the three Focal Points; areas such as money laundering and social engineering. Although many crimes are now *Internet-facilitated*³ (such as intellectual property crime), these are not directly addressed outside the main parameters of the report.

The assessment examines a number of dual-use technologies - systems which are used legitimately by society but which are exploited by cybercriminals to enhance or proliferate their criminality. Where relevant, the assessment provides an overview of concepts such as the Internet of Everything and Big Data that have or are likely to have an impact on the crime areas covered in this report.

¹ The European Multidisciplinary Platform Against Criminal Threats (EMPACT), is a structured multidisciplinary co-operation platform of the relevant Member States, EU Institutions and Agencies, as well as third countries and organisations (public and private) to address prioritised threats of serious international and organised crime.

² i.e. crimes which would not exist without the advent of the Internet.

³ i.e. crimes for which the scope and impact are enhanced by the Internet but do not require it to operate

Each chapter begins by providing a description of the crime or threat area. The assessment then considers factors that facilitate or enable each crime and how they are exploited by criminals.

The report also assesses how the threat is likely to evolve in the future and highlights key developments likely to impact law enforcements' ability to combat the threat. Lastly each chapter provides specific recommendations on steps law enforcement can take to effectively address the threat. Here a distinction is made between actions from an *investigative/disruptive approach*, from a *prevention* perspective, and actions aimed at strengthening *protection* against cybercrime.

Several issues and recommendations span multiple threats and crime areas; those are discussed at the end of the document as overarching topics.

Methodology and acknowledgements

The iOCTA was drafted by a team of strategic analysts within EC3 drawing on contributions from Member States, the EUCTF, the expert input of staff from Focal Points Cyborg, Terminal and Twins, as well as the Cyber Intelligence team, the Serious Organised Crime Strategic Analysis team and the Data Protection Office. This has been further enriched with input from the private sector, including EC3's advisory groups, and academia. Combined with open source research and analysis, these contributions have been essential to the production of the assessment.

Europol would like to extend special thanks to the EC3 Academic Advisory Board for their contributions. They are Prof. Marco Gercke, Prof. Michael Levi and Prof. Alan Woodward. A special thanks is also due to Dir. Mary Aiken for her input on cyberpsychology.



EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

The Internet Organised Crime Threat Assessment (iOCTA)

CHAPTER 2

THE STATE OF THE INTERNET

It is now no longer enough to simply state that more and more people are 'getting online' or that crime is becoming increasingly facilitated by the Internet. The Internet is now firmly *here* - for almost everyone - and is an established daily platform for communication, business, socialising, expression, commerce and crime. Few aspects of daily life are not, or cannot, be planned or accomplished online.

In 2013, the average Internet penetration⁴ in the EU was estimated to be 75%, compared to an average global penetration of 39%. This represents almost 380 million Internet-enabled Europeans. In some EU states - typically Nordic countries - penetration is in excess of 90%. Europe-wide this represents a growth of almost 400% in just over a decade⁵.

Despite its low Internet penetration (~27%), Asia's population of almost 4 billion still correlates to over 1 billion Internet users - 45% of the world's total users. Africa and the Middle East have less than 5 million Internet-enabled citizens each, but both have witnessed a meteoric growth in Internet penetration over the last decade - 3600% and 2600% respectively. Latin America

is also rapidly becoming a major component of the global Internet community with 43% penetration, growing by 1300% in 10 years⁶.

A large part of this growth can be attributed to the boom in the sale of smartphones and tablets. Less than a decade ago, Internet access was restricted to those with the luxury of a desktop PC. While globally the number of PCs with a home broadband connection sits at just below the 700 million mark, the number of active mobile broadband subscriptions is approximately three times that figure⁷. Cheap, affordable mobile devices are bringing the Internet to masses. It is estimated that global smartphone sales will reach 1.2 billion in 2014, a figure equal to the combined population of Europe and North America.

The Internet has heralded a change in the behaviour of society and how family, friends, colleagues, customers, suppliers, businesses big and small, governments and nations interact. Consumers publish their lives on the Internet, sharing their data with a multitude of entities; businesses - from small ventures to sprawling corporations - all have a presence on the Internet, and

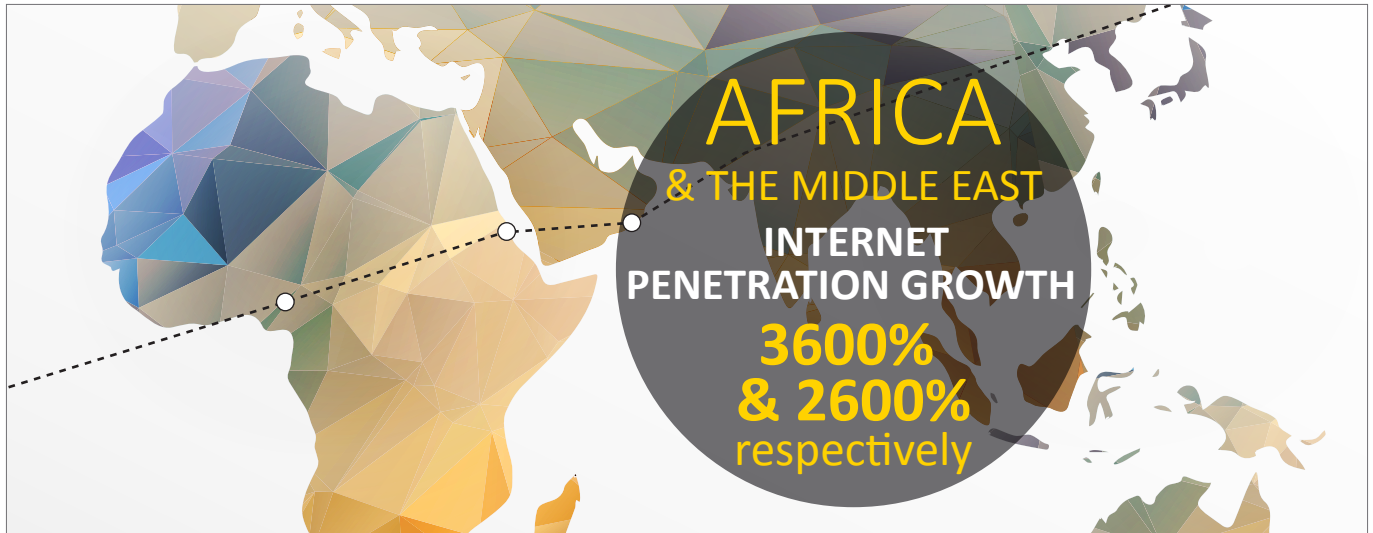


⁴ The percentage of the population that are Internet users

⁵ [Internet World Stats](#)

⁶ [Internet World Stats](#)

⁷ [International Communication Union - Statistics](#)



are increasingly shifting their data and resources to cyberspace; governments and public sector bodies are also moving services and resources online.

Across all of these interactions there is an intrinsic need for security. No security feature is impenetrable however, and where there are vulnerabilities - whether in hardware, software or in simple trust - there are opportunities for exploitation.

The Internet has created a unique ecosystem for the criminal exploitation of vulnerable online entities. It provides an environment where a perceived level of anonymity implies a lack of consequence and thereby a lack of responsibility. Out of the billions of individuals now accessing the Internet, literally with the world at their virtual fingertips, for those with sufficient curiosity and/or the inclination towards the illicit, all that is lacking is opportunity.

Enter the digital underground economy.





EUROPEAN CYBERCRIME CENTRE
ECC
EUROPOL

The Internet Organised Crime Threat Assessment (iOCTA)

CHAPTER 3 CRIME AREAS

3.1 Crime-as-a-Service

Overview

Over the past few decades the digital underground has evolved and matured from a few small groups hacking and phreaking for fun and prestige, to a thriving criminal industry that costs global economies an estimated USD 300+ billion per year⁸.

The digital underground is not only complex and highly dynamic but also highly fragmented. Each actor, from sophisticated criminal groups to the fledgling cybercriminals, has their own particular skill-set and area of expertise. It is this division of labour and adoption of niche functionalities that drives the criminal economy, and has created a booming *as-a-service* industry, as skills can be monetised and create broader – even mass – access to crime capacities that would have formerly required exceptional abilities.

Underground forums

The underground economy relies extensively on websites and forums - market places and hubs where supply and demand meet; places to advertise, buy and sell products and services, network and share experience and expertise. Here the pooling of knowledge and the constant need for innovation also stimulates research and development.

These forums can be devoted to a particular topic (a product or specialised service such as hacking or carding) or be more generalised, covering a huge range of topics and products, servicing the entire spectrum of cybercrime and supplying all logistical aspects required to perpetrate cybercrime offences.

One Russian language carding forum with over 13 000 members and almost 4000 daily visitors had more than 20 subforums covering topics including online security, tutorials, carding, botnets, web design and money laundering. Across the forum there were in excess of 75 000 individual discussion topics.

Since their first appearance in the early 2000s⁹, these forums have matured in sophistication, in the expertise and range of products available, and the level of professionalism and operational security exhibited.

Traditionally these forums have resided within the open or Deep Web¹⁰, however the Darknet¹¹ is increasingly becoming host to such communities. The same mechanism which provides anonymity to users likewise allows content to be hosted anonymously on the network, ostensibly being untraceable whilst remaining accessible from within the network. This capability has given rise to what have become known as *hidden services*.

These services generally take one of two forms - *underground forums* and *criminal marketplaces*. Underground forums on Darknets typically mirror their open Internet or Deep Web counterparts, serving as meeting places and message boards for many different communities. Forums dedicated to drugs, hacking, carding and child abuse material can all be found on the Darknet.

Although trade in illicit commodities does occur on these forums, Darknets have risen in infamy due to the specialised criminal marketplaces - epitomised by the *Silk Road*. These markets offer browsers a place to acquire almost any illicit commodity or service including

8 [McAfee July 2013 - The Economic Impact of Cybercrime and Cyber Espionage](#)

9 [Rand Corporation 2014 - Markets for Cybercrime Tools and Stolen Data](#)

10 The portion of the Internet not indexed by search engines

11 Peer-to-peer networks within the Deep Web operating using technologies such as TOR and I2P



narcotics, weapons, pharmaceuticals and steroids, forged documents, credit cards, hacking tools and even contract killings. *Silk Road* spawned a number of alternate sites such as the *Agora* and *Outlaw* markets and, following its takedown in October 2013, *Silk Road 2.0*. As of August 2014 there were at least 39 such markets¹². The majority of these sites are in the English language, however a number of them cater to specific languages including Finnish, French, Italian, Polish and Russian¹³.

Despite the increased protection and anonymity the Darknet affords, the more sophisticated, high threat *cybercrime* forums still operate in the open or Deep Web. It is possible that this is due to a perceived greater degree of control over internal security than that afforded by a Darknet infrastructure in addition to superior connection speeds.

In either environment, access to these platforms is not always straightforward. Entry requirements escalate with the sophistication of the forum. The more security-conscious forums for example, often require new members to be 'vouched' for by existing members.

Within forums a rigid and unique (for *cybercrime*) hierarchy often exists. This structure, with designated roles and responsibilities, allows forums to effectively police themselves, controlling population levels, and rooting out unwanted or troublesome members. Forums are run by *Administrators* who manage its hosting, determine the general purpose and direction of the forum and set rules for recruitment and behaviour. Each subforum is generally overseen by one or more *Moderators*. These are trusted individuals who are often subject matter experts for their particular subforum topic and who manage content and disputes within their area. Each forum will also have a multitude of *Vendors* with services and products to trade with the forum membership. Vendor status typically requires providing samples to the *Moderators* for review.

Furthermore their products will continuously be reviewed and rated by customers. The concept of reputation and ratings is analogous to that of legitimate commercial websites with the exception that access to cybercriminals with a high reputation is not easy.

A user's reputation and consequently their online nickname¹⁴ on these underground forums is one of the most important factors in creating trust and for deciding to engage in a business relationship.

To the remainder of the community, these markets give organisation to previously disparate individuals, permitting them to escalate the scale of their operations. The current definitions of organised crime do not reflect the digital underground economy. Often, relationships between cybercriminals are transient or simply transactional, with cybercriminals rarely knowing each other offline. Instead these markets create an organised set of criminal relationships¹⁵. Increasingly however individuals are forming more coherent groups focused around a particular project or attack campaign, although these groups still lack the structure and hierarchy of a traditional organised crime group.

The most persistent *cybercrime* forums are populated by Russian speaking communities, and although English is also commonly used in communication, many jurisdictions host forums in their native language. Underground forums have various nationalities and these communities are growing.

Criminal services

In a simplified business model, a cybercriminal's toolkit may include malicious software, supporting infrastructure, stolen personal and financial data and the means to monetise their criminal gains. With every aspect

¹² [Deep Dot Web](#)

¹³ [Deep dot Web](#)

¹⁴ [Industry of Anonymity](#)

¹⁵ [The European Parliament, The Economic, Financial and Social Impacts of Organised Crime in the EU](#)



of this toolkit available to purchase or hire as a service, it is relatively easy for cybercrime initiators - lacking experience and technical skills - to launch cyber attacks not only of a scale highly disproportionate to their ability but for a price similarly disproportionate to the potential damage¹⁶. The possibility to outsource significant parts of their work also allows experienced cybercriminals to focus on their core activities, becoming more efficient and specialised.

The following is an outline of some of the key services offered:

Infrastructure-as-a-Service - To launch their attacks cybercriminals require infrastructure which provides security, anonymity, resilience and resistance to law enforcement intervention. Protected infrastructure for delivering attacks is not only used by profit-motivated cybercriminals, but can be used in other types of offending such as hacktivism or online child sexual exploitation.

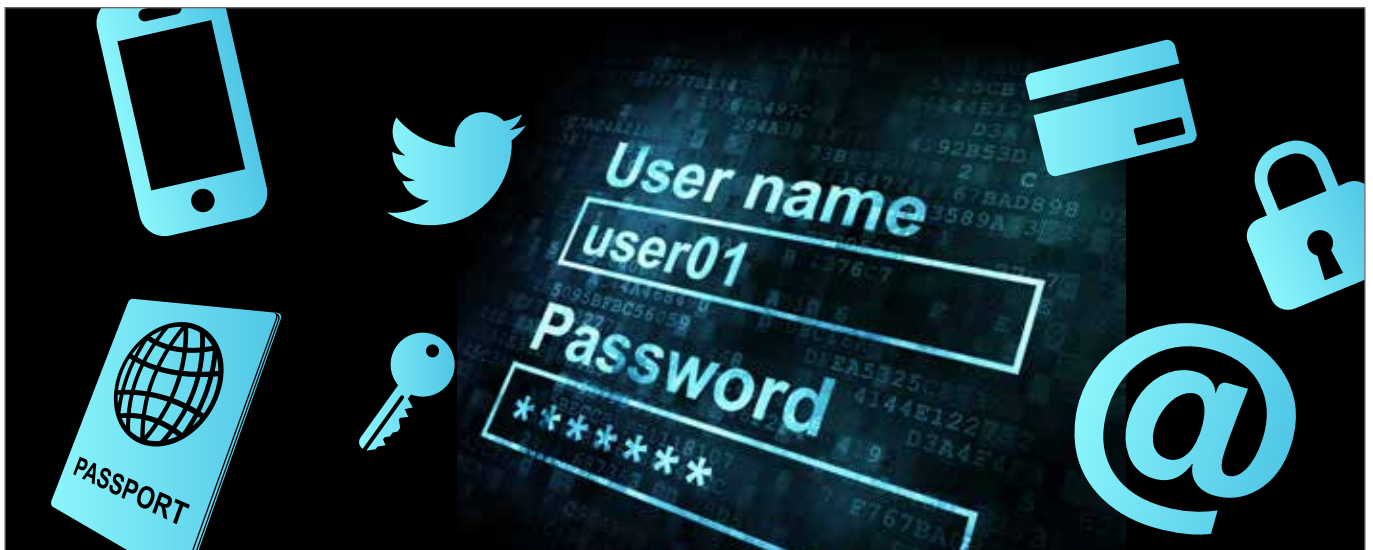
Hosting providers have a critical role in the underground economy, providing secure storage for attack tools, such as malware and exploit kits, illicit material and stolen data. Bullet-proof hosting services are highly sought after in online marketplaces¹⁷, providing customers with the necessary resilience to evade law enforcement. VPN and proxy services play an important role providing anonymity to cybercriminals and their activities.

Distributed Denial of Service (DDoS) attacks have become accessible to anyone willing to pay for such services. Those offering this service typically have a botnet at their disposal, renting out its capacity in order to launch attacks. With today's methods a large botnet is not always required to launch a large scale attack. A number of methods such as *NTP amplification* or *DNS reflection* can magnify the efficacy of any botnet. Such methods were used in the Spamhaus DDoS attack in 2013 - one of the largest recorded attacks in history - which spiked at nearly 300Gbps of traffic.

Although we can only expect the magnitude of DDoS attacks to increase, networks will become better at mitigating such attacks as they have with spam.

Attackers do not restrict themselves to botnets comprised of infected home computers. They have also begun identifying, compromising and exploiting vulnerable website and content management system (online publishing) servers which have greater bandwidth, are optimised for heavy traffic¹⁸ and are therefore well suited to launching large attacks.

Data-as-a-Service - Data is a key commodity for cybercriminals. Large volumes of compromised personal and financial data are retailed in the digital underground economy. This includes not only data such as credit card, and bank account details, but also data such as physical



¹⁶ [Cyber Infrastructure Protection, pg. 15](#)

¹⁷ [Trend Micro: Russian Underground 101, 2012](#)

¹⁸ [Verizon 2014 DBIR](#)

addresses, phone numbers, email addresses, names and dates of birth, e-wallets, social network accounts and other web logins (particularly those with a financial aspect). Underground market places can also supply counterfeit or fraudulently obtained physical documents such as ID cards, passports, driver's licences, and utility bills to facilitate both online and offline fraud¹⁹.

Pay-per-install Services - A popular method of distributing malware. The providers of these services distribute the malicious files supplied by their customers and get paid according to the number of downloads. These services can provide country specific traffic.

Hacking-as-a-Service - At a basic level this may include hacking of email and social networking accounts but may include more sophisticated attacks such as economic espionage, or gathering private data on a target.

Translation Services - Many campaigns target victims in specific countries, for which the attacker may not be a native speaker of the target language. The use of translators to provide grammatically correct scripts maximises the impact of a campaign as poor language is often a giveaway that a particular message is part of a scam.

Money Laundering-as-a-Service - In order to financially benefit from their activities cybercriminals employ services to 'cash out' from digital or real world financial systems. These services involve a combination of online and offline solutions, with money mule networks often having a central role.

Law enforcement considerations

The dispersed nature of cybercriminals, even those in a temporary coalition for the purposes of a project or campaign, creates challenges for law enforcement (LE) intervention; there is no organised criminal group (in the traditional sense) to target and dismantle. Cybercriminals will typically only interact online and behind a wall of anonymisation, therefore targeting one individual will not always lead to identifying their associates. Associates that might be identified are likely to be distributed globally, which complicates those investigations further.

This arrangement also has advantages for law enforcement. Although targeting the cybercriminal 'elite' may be particularly challenging due to their operational security and/or jurisdiction, there are many secondary targets that provide skilled and essential services whose removal would cause considerable disruption to the market.

Where LE has the lawful possibility and capacity to conduct infiltration, specific identified forums used by



notorious cybercriminals can be a valuable source of criminal intelligence on new and future threats as well as for obtaining evidence of current cybercrime.

It is important to remember that content hosted on a Darknet is still physically hosted somewhere and can be subject to LE intervention. The success of LE in taking down hidden services on the Darknet demonstrates how achievable this is as an operational goal:

- August 2013 - US and Irish authorities take down *Freedom Hosting*, thought to be one of the largest operators within TOR, offering services such as TorMail and hosting for websites distributing child abuse material;
- October 2013 - *Silk Road* taken down by US authorities;
- February 2014 - Dutch authorities take down *Utopia*, a marketplace similar to Silk Road, after only being live for seven days.

Future threats and developments

The use of the Internet to facilitate traditional organised crime is already a common phenomenon. The Internet provides secure communications, is a tool for research and a platform to buy and sell goods. However, as traditional criminals become more confident and comfortable

19 [Trend Micro: Russian Underground 101, 2012](#)

with cyberspace we can expect to see the recruitment of specialists to carry out increasingly sophisticated cyber attacks to complement their established criminal activity.

In June 2013, police in Belgium and the Netherlands dismantled a Netherlands-based drug smuggling ring. The gang had hired hackers to infiltrate the systems controlling the movement and location of shipping containers at the Belgian port of Antwerp. This allowed the gang to manipulate the data to allow their own drivers to remove drug-laden shipping containers before the legitimate haulier could collect them.

The volume of illicit services finding their way onto the Darknet will only increase over time as criminals involved in traditional crime become more familiar with the technology. Cybercriminals will also increase their presence within the Darknet as anonymisation technologies continue to develop.

The cybercrime community can be divided into two distinct populations. The larger demographic consists of inexperienced individuals with little technical skill who dabble with cybercrime, buying the skills and tools they lack. This group remains a high volume but low impact threat, content to carry out relatively minor offences such as small frauds, defacements, etc. Only a few of these individuals will graduate to the smaller demographic of highly skilled individuals who not only carry out the most damaging cyber attacks but sell their services to the larger, less capable population. This cycle both perpetuates and proliferates cybercrime. As cybercrime tools and services become more available and easy to access, the former group will grow which in turn leads to the development of more highly skilled individuals.

Recommendations

- A co-ordinated EU-wide undertaking is required to disrupt or dismantle the top identified criminal forums and marketplaces. This should be an intelligence-led endeavour combining the efforts of law enforcement, judicial authorities, Europol and Eurojust, and utilising initiatives such as the Joint Cybercrime Action Taskforce (J-CAT) under EC3.
- Law enforcement should target individuals with high reputations on the underground forums. Successful prosecution of top tier cybercriminals would not only have considerable impact on the cyber community but may provide many other investigative leads and sends a strong message to the criminal community that nobody is untouchable.

- Where it is not possible to target top tier cybercriminals due to lack of attribution or jurisdictional issues, law enforcement should focus on targeting those providing key support services. There are often only limited numbers of skilled and experienced individuals providing the more technical services, who may not be quickly or easily replaced should they be removed.
- Where possible law enforcement should similarly focus on targeting criminal infrastructure such as the servers where cybercriminals host their content or communications.
- Where national legislation allows lawful, targeted surveillance possibilities, these options should be utilised where appropriate to identify high threat underground forums used by cybercriminals and to gather intelligence and evidence. This may require law enforcement to increase or adapt its language capacity.
- Law enforcement should take full advantage of successful operations to increase their visibility and presence online. Attributing themselves to successful website takedowns and domain seizures with the likes of branded splash pages increases the impact of the activities. Following this, further prevention activities such as LE-badged emails to forum members, will act as further deterrents.

3.2 Malware

Overview

One of the fundamental services provided by cybercriminals is the design, development and distribution of malware – arguably the key primer for the majority of downstream cybercrime. *Malware-as-a-Service (MaaS)* is becoming increasingly professional, mirroring legitimate commercial software development companies by providing functionality such as 24/7 customer support and frequent patches and updates to continually refine their product and increase its capability and competitiveness in the malware marketplace. As such, MaaS is becoming an essential component of the underground economy.

Attack vectors

Exploit kits represent one of the most common methods of infection with more than 80% of online threats detected in 2012 associated with infected websites²⁰. Current popular kits include the *Pony*, (Sweet) *Orange*, *Magnitude* and *Nutrino* exploit kits. Java and Adobe products remain

20 [Sophos 2013 Security Threat Report](#)

primary targets to exploit, with up to 90% of exploits working through vulnerabilities in Java²¹.

The Blackhole Exploit Kit (BEK) was a very successful implementation of Malware-as-a-Service. The BEK was available for rent to deliver everything from fake antivirus and ransomware to Zeus and the infamous TDSS and ZeroAccess rootkits, attacking Windows, OS X, and Linux. The BEK's authors offered free updates for the life of the subscription and customers who wanted to run their own Blackhole servers could purchase longer licences.

Watering Hole attacks are an increasingly popular social engineering attack method for criminals targeting specific industries or organisations. This methodology was used to breach several prominent Internet companies in 2013 including Facebook, Twitter, Apple and Microsoft²².

Spam, although on a general downward trend, is still a major threat representing approximately 70% of all inbound email traffic²³. A blunt tool in a cybercriminal's hi-tech toolkit, spam relies on sheer numbers, despite low success rates, to distribute malicious URLs and attachments to infect unwitting victims. That is not to say that spam is not the weapon of choice for the malware developers at the forefront of contemporary malware; a massive spam operation was used to launch the *Cryptolocker* campaign of late 2013.

Most mobile devices are permanently on - giving attackers much larger windows of opportunity to attack or exploit a particular device. Mobile devices share a number of infection methods, though many are unique to the platform:

- *SMS spam* - luring potential victims to click on malicious links which will download malware to their device.
- *Spoofed/Trojanised apps* - victims install free, discounted or cracked versions of popular apps, however in reality the apps are malicious and download malware to their device.
- *Adware* - Victims will download an innocuous app APK in which the criminals control the in-app advertising. Once enough potential victims have downloaded their app, criminals will change the advertising to direct victims to infected websites.

- *Infected Updates* - Victims download a non-malicious, free app to which attackers push an update which carries the malware payload.

Infected mobiles have the potential to act as an infection vector for other platforms and devices. Some emerging malware variants are capable of propagating themselves (along with other malware) to other devices via Bluetooth. Other malware is designed to spread to desktops via infected smartphones and tablets once connected via USB²⁴.

Malware functionality

Malware serves a multitude of malign purposes. This ranges from logging keystrokes to steal sensitive user data, to sophisticated and professional malware which can intercept and alter data or hijack the victim's user session. 'Ransomware' typically disables a victim's device until a fee is paid to release it. Other malware simply provides a 'backdoor' for attackers to access the infected device. Compromised devices can also be used as malicious web servers to host illegal content or child abuse material.

Although cryptoware originated in 1989²⁵, 2013 witnessed a resurgence of this threat with a spam campaign spreading the *Cryptolocker* malware. Cryptolocker identifies files likely to be of value to the victim (photos, videos, text documents, etc) and encrypts them, rendering them effectively irretrievable without the decryption key. Payment of the ransom results in the provision of the decryption key, although the malware will remain on the victim's device unless removed by the victim. As ransomware potentially renders the victim's device unusable it is often used as a 'final stage' attack, deployed only once other exploitation opportunities have been exhausted²⁶.

Ransomware remains a lucrative venture for cybercriminals. Once deployed, each successful extortion represents a direct payment to the attacker. Furthermore, a relatively unskilled cybercriminal can initiate a campaign by taking advantage of the pay-per-install services or crimeware kits readily available as products or services in the digital underground economy²⁷.

The majority of mobile malware takes advantage of a mobile's *direct* access to funds in the form of the victim's account credit. Approximately half of mobile malware are *premium service abusers* or *chargeware*. These send SMSs or subscribe their victim to premium services without the victim's knowledge.

21 [Panda Labs 2013 Q1 Report](#)

22 [E-Secure 2013 H1 Threat Report](#)

23 [Trustwave Spam Statistics, 2014](#)

24 [Panda Labs 2013 Q1 Quarterly Report](#)

25 [SecurityFocus: PC CYBORG \(AIDS\) trojan horse, 1989](#)

26 [Cisco 2014 Annual Security Report](#)

27 [McAfee 2013 Q1 Threat Report](#)



Some malicious apps either work in conjunction with malware already present on the victim's PC or spoof legitimate mobile banking apps in order to steal login credentials but with the added function of being able to intercept the mobile transaction authentication number (mTAN) required for two-factor authentication and transmit it to the attacker²⁸.

Approximately a quarter of mobile malware harvests the second most valuable commodity to cybercriminals after cash – *data*. SMS content, call logs, IMEI numbers, WiFi network details and lists of contacts and installed apps are harvested from infected devices, transmitted to the attacker and traded to facilitate further fraud. SMS related information databases are some of the best-selling data sets in the underground²⁹.

Mobile malware is increasingly mirroring the functionality of its desktop counterpart - unsurprising as smartphones are now comparable in processing power to desktop computers from 2010³⁰. There are already examples of mobile malware being used to (inefficiently) mine cryptocurrencies³¹. Smartphones are also ripe targets for ransomware. 2013 saw the first examples of mobile

ransomware, and variants of mobile cryptoware (*SIMPLOCKER*) began appearing in June 2014³² - only six months after the emergence of *Cryptolocker*.

Criminal botnets

In addition to what can be obtained from an individual machine, once infected, a victim's device may become part of a *botnet*. Comprised of thousands if not millions³³ of infected machines or 'bots', botnets can be used for a variety of functions including spam campaigns, adware, spyware, ClickFraud or DDoS attacks on other networks and systems. An infected mobile device can also become part of a botnet. Mobile botnets can similarly be used to send SMS spam in order to reach new victims.

A recent development in botnets, as seen with *GameOver Zeus*, is the use of peer-to-peer (P2P) networks such as TOR to communicate with the command and control (C&C) architecture in an encrypted and anonymised way. This makes it difficult for law enforcement to locate C&C servers, thereby making the botnet more resistant to any take-down attempts.

There are two prominent categories of malware reflected in the cases encountered by law enforcement in Europe - *ransomware* and *banking Trojans*. Both attacks are profit making engines for attackers and are therefore likely to represent the majority of malware campaigns.

Ransomware

Roughly 65% of European law enforcement has encountered some form of ransomware, and mainly police ransomware. This bias in reporting is most likely due to the police-orientated composition of the attack, increasing the likelihood that it would be referred to law enforcement. Although the majority of these attacks follow the typical attack modus operandi of blocking access to and the functionality of a victim's device, examples of police ransomware using encryption are starting to emerge.

Despite heavy reporting in the media, cryptoware did not feature as a significant current threat for EU law enforcement in comparison to other malware attacks. Still, several Member States were subject to cryptoware campaigns from attackers deploying either *CryptoLocker* or *CryptoBit*.

Banking Trojans

Banking malware remains the cyber workhorse of the digital underground, harvesting victims' credentials and logins, and providing attackers with access to their accounts. Over half of EU Member States reported cases relating to banking Trojans. Of these the *Zeus* (including

28 [McAfee 2013 Q2 Threat Report](#)

29 [TrendLabs Q2 2013 Security Roundup](#)

30 [Softpedia: iPhone 5s Equals 2010 Mac mini in Processing Power, 2013](#)

31 [G Data: Android Malware goes "To The Moon!", 2014](#)

32 [ESET: Simplelocker, 2014](#)

33 [Symantec 2013 ZeroAccess In Depth](#)



more sophisticated P2P variants) and *Citadel* campaigns were the most common. To a lesser degree *SpyEye*, *Dexter*, *Qadars* and *Torpig* were also encountered.

Member States were additionally plagued by a mixed bag of other malware attacks with Remote Access Tools (RATs), such as the *Blackshades* malware also commonly reported.

Today the ability to launch a successful malware campaign is enhanced and propagated by the *Crime-as-a-Service* business model of cybercrime. Crimeware packs and kits for launching malware campaigns are readily available on the illicit forums that cybercriminals frequent. Malware is often supplied by resellers rather than the original developers indicating further niche roles in the marketplace.

Many attacks are customised to target specific jurisdictions. With ransomware for example, ransoms are demanded in national currencies or languages. Poor translation suggests that campaigns often originate from outside the victim's jurisdiction.

Facilitators and relevant factors

A major enabler for malware is a lack of awareness and education on the part of the victim. The weakest link in cyber security is often the user, meaning that even the most effective and sophisticated security solutions rely on the user's understanding of how to stay safe online. Users leave themselves additionally vulnerable by running unpatched and outdated software.

The digital underground supplies a number of services which support and complement the successful development and deployment of a malware product. Coders are required to write the various injects and plugins which can give malware-specific or unique functionality (such as targeting a specific URL or grabbing credit card

details). Encryption services are essential to obfuscate the source code of malware to allow it to bypass detection by antivirus software. Others sell *traffic* - directing potential victims to compromised URLs - or offer *pay-per-install* services, receiving payment for each new victim they are able to infect for your customer.

Counter-antivirus services are another key support service. These allow malware developers to anonymously upload files to scan them against a range of commercial antivirus products in order to determine their resistance to antivirus products.

Law enforcement considerations

Often law enforcement services direct their resources to different priorities than those identified by the Internet security industry. This is due in part to the high level strategic view of the security industry compared to the more granular, ground level viewpoint of law enforcement. Many police forces often do not have the capacity, capability or the resources to tackle a global cybercrime threat, and are limited to simply dealing with the cases presented to them by victims.

There is also a natural time-lag between the Internet security industry identifying a threat within the broader user community and it subsequently registering on law enforcement's cybercrime radar. For example, from the viewpoint of the security industry, mobile malware is very much a current problem, whereas much of law enforcement still considers this a future threat.

Future threats and developments

On 8 April 2014, Microsoft ceased support for its Windows XP operating system. Windows XP is still widely used, running on up to 25% of PCs worldwide³⁴ as well as embedded systems such as ATM machines. 2014/2015 will undoubtedly see an increase in infections of systems running XP as new vulnerabilities are discovered and left unaddressed. It is likely that exploit writers have been stockpiling new exploits for Windows XP, simply waiting for support to be withdrawn in order to release them onto the market at a premium rate³⁵. We will inevitably see more targeted attacks on private and public sector entities still running XP. These attacks will gradually decline as it ceases to become profitable for malware developers to target an operating system used by an ever-dwindling victim-base.

We will see not only further development and refinement of cryptoware but also encryption built into many other

³⁴ [Net Market Share, 2014](#)

³⁵ [Security in 2014: What are the experts predicting?](#)



malware variants to increase their functionality and the range of attack options available to cybercriminals with a single product. Malware developers will increasingly target other Internet enabled devices, particularly as they may not enjoy the same level of technical support or built-in security as other digital devices³⁶.

However, as public awareness of ransomware increases, the success rate of the malware, at least with domestic victims, will be eroded by every attacker too malicious or lazy to release the encryption key once the ransom is paid³⁷. Once victims begin to believe their files will not be returned nor computers unlocked despite paying the ransom, then they may well accept their losses and pay nothing. Law enforcement should highlight this as part of any awareness campaign.

Malware is becoming increasingly 'intelligent'. Some malware includes code to prevent it either being deployed or run in a sandbox environment, as used by malware researchers for analysis. In this way malware developers can avoid automated analysis of their product, thereby remaining undetected for longer³⁸. Malware developers will continue to refine their products to make them stealthier and harder to detect and analyse.

Internet companies are increasingly employing a more liberal approach to identifying new vulnerabilities in the form of 'bug bounties'. Many companies offer such rewards, paying security researchers up to USD 100 000 for finding flaws and vulnerabilities in their products. Such schemes will no doubt develop if ad-hoc payments to independent researchers become a more cost efficient preventative method for improving the security of a company's products. However, just as malware development is mirroring commercial software development, exploit kit developers are also offering bounties for zero day exploits

for inclusion in their kits; in October 2013, exploit writer *J.P.Morgan* announced a budget of USD 450 000 for the purchase of vulnerabilities³⁹.

Research has demonstrated a technical possibility to propagate malware via open WiFi networks⁴⁰. Should this become a reality and be developed for criminal purposes it has the potential to have catastrophic consequences and will likely usher in a new wave of Internet and mobile security.

By 2012, mobile malware had reached a level of magnitude which PC malware had taken more than a decade to reach⁴¹. It is expected that, as malware developers refine their skills and become more intimately familiar with this platform, their products will become increasingly sophisticated and professional, and produced *as-a-service*. Mobile *cryptoware* is already a reality, although currently in limited circulation, however it is inevitable that more widespread variants will appear in the near future.

Internet security companies are reporting hundreds of thousands of new malware samples every single day⁴². It is likely that the current signature based methods of malware detection will be unable to cope with future malware production. We will therefore see further development of antivirus which detects malware based on abnormal activity.

Recommendations

- A top priority for law enforcement should be the apprehension and prosecution of malware developers. As many of the more malicious variants such as *Gozi*, *Torpig*, *Shylock* and *GameOver Zeus* are controlled within closed criminal circles, successful

36 [BBC News: Internet of Things: The 'ghosts' that haunt the machine, 2014](#)

37 [Microsoft Protection Centre – Ransomware](#)

38 [Malwarebytes: Sandbox Sensitivity, 2013](#)

39 [Krebs on Security, 2013](#)

40 [Edgis Security: WiFi Malware Spreads like Common Cold, 2014](#)

41 [TrendLabs Q2 2013 Security Roundup](#)

42 [Panda Labs Quarterly Report January-March 2014](#)

law enforcement action on such groups would have considerable impact, not only removing the threat caused by their product but also preventing future product development or refinement by some of the more talented malware developers.

- Better co-ordination is required in operations to dismantle criminal infrastructure. Botnet takedowns are an area in which law enforcement has displayed considerable success. Such ventures require co-operation between multiple jurisdictions and Europol as well as with partners in private industry and CERTs. Many stakeholders have vested interests and resources linked to the criminal infrastructure therefore the *timely* involvement of all interested and involved parties is important to ensure the operation is executed at the most opportune time.

In May 2014 law enforcement dismantled a GameOver Zeus botnet and Cryptolocker infrastructure. Co-ordinated at EC3, this FBI-led operation also involved investigators from Canada, France, Germany, Italy, Japan, Luxembourg, Netherlands, New Zealand, Ukraine and United Kingdom, along with multiple partners from the Internet security industry.

- It is essential that law enforcement continues to build and maintain partnerships with the Internet security industry. The industry holds

an accurate and contemporary picture of the cybercrime landscape at a broad, strategic level which law enforcement often lacks. The Internet security industry also holds a wealth of data which could assist in identifying and prioritising targets. MS should, based on national legislation and data protection rules, identify the possibility to establish procedures to benefit from this fact by initiating a dedicated outreach program for public-private partnerships. Furthermore, the industry can provide insight into new and emerging threats to allow LE to better prepare and take preventative action.

3.3 Child sexual exploitation online

Overview

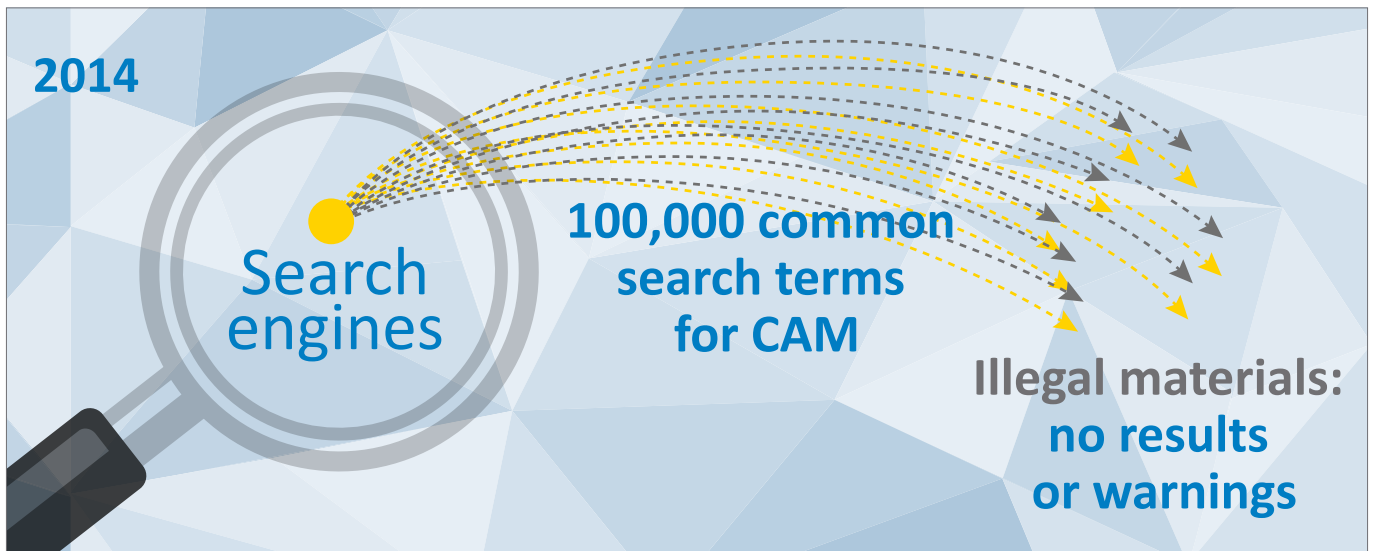
Child sex offenders commit criminal offences with an element of sexual activity or sexual contact with a minor, thereby violating established legal and moral codes with respect to sexual behaviour.

Most child sex offenders are not part of any criminal network and usually operate alone, driven solely by their sexual interest in children.

However, this does not mean that offenders act in isolation from each other. They communicate among themselves within like-minded groups in cyberspace, using a variety of online tools, from IRC, ICQ, Yahoo newsgroups/forums



"Aiken, M.; Moran, M. and Berry, M. (2011). Child abuse material and the Internet: Cyberpsychology of online child related sex offending"



to social networks, peer-to-peer file sharing networks, secure email and TOR. Even though it is commonly accepted that child sexual exploitation (CSE) offenders do not form typical organised crime groups, they still organize themselves in an analogous hierarchy on such platforms. This is usually the case on platforms where offenders exchange child abuse material (CAM), either in video, pictures or even text format. Here, those who provide material that is considered to be of 'high quality' (typically novel material), show higher levels of technical expertise and share best practise, can achieve the highest ranks and be recognised amongst their peers. Furthermore, some offenders affiliate themselves with each other in order to share physical access to children, therefore facilitating the production of new material, as well as its customisation.

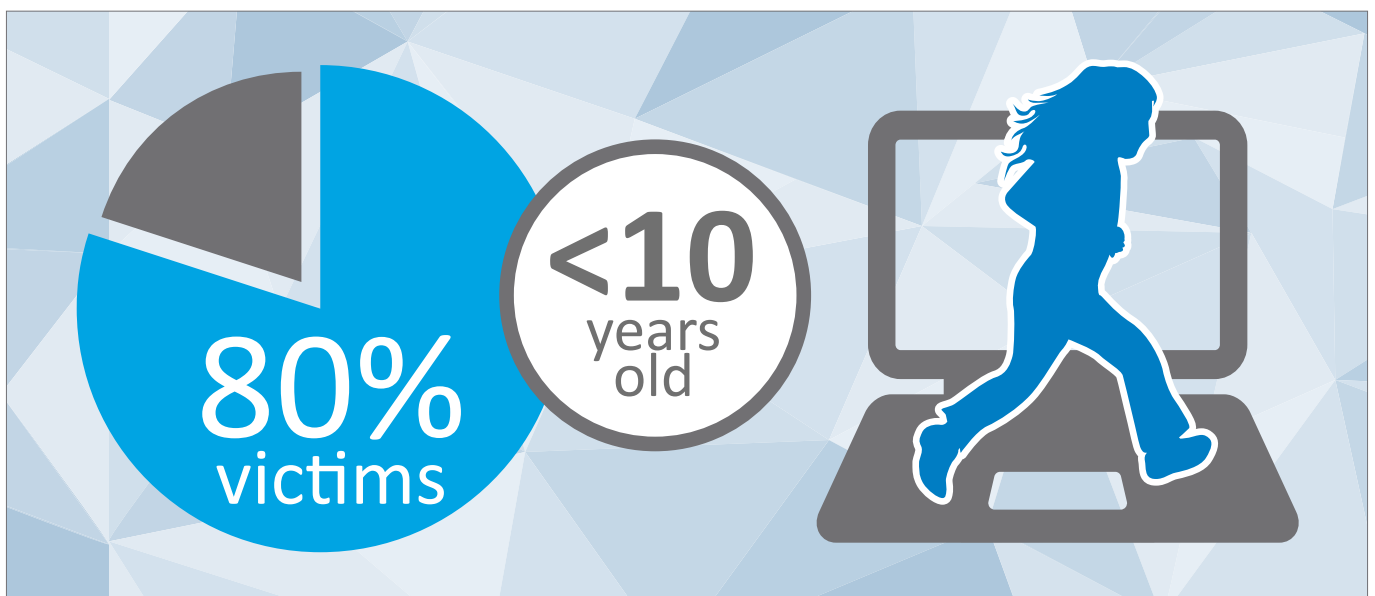
The forensic awareness of CSE offenders can vary considerably, but evidence indicates that overall forensic skills are on the rise, which may be in response to improved detection and forensic policing. This increase

in expertise is propagated in closed communities where it is common to find a section dedicated to technical and forensic guidance. The level of technical expertise is in some cases very advanced, indicating professional ICT and information security expertise.

Exploitation of children online

Child sex offenders use the Internet to meet like-minded individuals, to have access to a wider pool of children, to share resources and knowledge and to disseminate CAM.

According to the threat assessment from the UK Child Exploitation and Online Protection Centre (CEOP), when taking into account the overall demographics of child sexual exploitation online (CSEO) - including sexual extortion and grooming - girls, of white ethnicity, aged between 11 and 14, are the main victims⁴³. Nevertheless, information from the Internet Watch Foundation (IWF) reveals that when considering web pages containing child



43 [CEOP: Threat Assessment of Child Exploitation and Abuse, 2013](#)

abuse material, a different demographic emerges: girls of white ethnicity are still the main victims but the age of the victims is considerably lower, with more than 80% of the victims younger than 10⁴⁴. Data from the International Association of Internet Hotlines (INHOPE) also shows an increase in infant victims of sexual abuse⁴⁵ and in abuse of an extreme and sadistic nature.

Sexual extortion and grooming

A major growing trend in CSE is sexual extortion, also known as *sextortion*, which, for the purpose of this document will be defined as coercion to extort sexual favours or images from a victim, usually by threatening to disseminate existing images of the victim if demands are not met. By exposing their personal details online without proper precautions, either via social media platforms or by sharing sexualised self-produced images, children and adolescents create the possibility of being targeted as potential victims by online predators.

An offender's *modus operandi* typically involves initiating contact with youngsters on social media platforms. Offenders exploit the contact opportunities provided by social networking platforms and other types of computer mediated communication, creating groups of sometimes hundreds of online friends that they consider potential victims. With such a large pool of children to choose from, offenders can scan their profiles in search of vulnerabilities, while engaging in virtual interactions to see which ones are more prone to falling for their lures. Offenders usually focus on the children that respond favourably or remain engaged⁴⁶.

In one notable case, a child sex offender coerced children to engage in sexual acts in front of webcams. The offender would meet children on social media platforms and convince them to send him indecent images of themselves. Once the children complied with the request, the offender would coerce them to undertake more serious abuse with the threat of disseminating the pictures to the childrens' friends and family if his demands were not met.

The offender used TOR and proxies to disguise his identity, but made a number of mistakes that led to his identification and arrest in the Netherlands.

The operation was led by the United Kingdom with the participation of EC3, US ICE, the Netherlands and Canada.

While most cases of sexual extortion seem to be initiated through an initial grooming process there is evidence of cases where the offenders have hacked into a victims' personal computer or instigated them to download malicious software, compromising their computer and then scouring their social networks⁴⁷. There are cases of offenders making use of images acquired in this manner to force the minors to engage in off-line contacts and proceed with physical abuse.

Many cases of sexual extortion are a consequence of 'sexting'. Sexting can be defined as the 'exchange of sexual messages or images'⁴⁸, typically self-generated, sent via mobile phone or the Internet. This exchange frequently occurs between peers - young people consciously exchanging naked or sexualised images of themselves with one another. Technology can facilitate the further unwanted dissemination of the images, affecting the well-being of the originator, leading to harassment and bullying, online and off-line, self-harming or even suicide. The subject of self-generated images brings added challenges. In some jurisdictions it is sometimes considered that the minor who generated the picture and distributed it is guilty of producing and disseminating child abuse material⁴⁹.

It is worth highlighting that the scope of criminal activity is defined by the offender's language skills. An offender speaking widely known languages is able to reach more potential targets, whereas an offender speaking a language which is not widespread will not extend beyond the national level.

Child sexual exploitation online on the Darknet

The use of the Darknet is increasingly popular among Europeans⁵⁰. A large number of offenders, in particular the ones with greater security awareness and technical knowledge, have established communities using hidden services on platforms such as TOR. Within these hidden services there is a proliferation of social networking platforms and storage providers dedicated to child abuse material (CAM) where offenders can post and view CAM securely.

Platforms like TOR and the hidden services therein facilitate practically untraceable sexual exploitation of children by allowing the exchange of images anonymously through websites, private messages and email. They promote the request of on-demand abuse, allow offenders

44 IWF: Annual Report 2013

45 INHOPE 2013, Facts, Figures & Trends

46 UNODC: Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children, 2014

47 FBI Cyber Alerts for Parents & Kids – Sextortion, 2012

48 Ringrose, J.; Gill, R.; Livingstone, S. and Harvey, L., (2012). "Children Young People and sexting: Data analysis – A report prepared for the NSPCC"

49 Crofts, Thomas and Lee, Murray, (2013). "'Sexting', Children and Child Pornography", Sidney Law Review

50 Information Geographies: "The Anonymous Internet", 2013



to anonymously create social network accounts to contact children and promote discussion among offenders on how to better groom and abuse children, where good destinations are for travelling child sex offenders (TCSOs) and how to obtain children there. These platforms encourage the normalisation of child abuse by the sharing of experience and justifications.

Having an awareness of many of the techniques employed by LE, offenders share guidance on how to sanitize material or mislead investigators, advising on removing EXIF⁵¹ data from pictures and how to include misleading background details in the images. Best practices on how to rape, kidnap, murder and dispose of children's bodies are also shared openly on Darknet forums⁵² and the rape of children openly discussed⁵³. CAM of a sadistic and violent nature is more readily available and there is also some evidence of a decrease in the age of the victims.

The existence of VIP or restricted sections is a common feature of most message boards, with access usually involving a vetting procedure frequently requiring production of new CAM, bringing added challenges to LE who, according to most jurisdictions, cannot usually provide this type of material within the law.

Services like 'TORchat', designed to be untraceable, facilitate engagement among offenders. Recent developments on TOR include the possibility of downloading Apps onto mobile Android devices, as well as 'safepug' hardware to anonymise web browsing by linking to wireless routers and streaming data onto TOR.

There are instances of CAM being exchanged via 'TOR mail' in exchange for Bitcoins. Even though most offenders do not exchange CAM for commercial reasons, the valuable significance of the material associated to the anonymity of

TOR and Bitcoin creates the ideal setting to add a financial benefit to a traditional exchange.

Nevertheless some offenders on TOR claim that services with paid memberships do not fit into the TOR environment as it brings more insecurity to the process of sharing CAM online. According to CEOP's research a good level of trust needs to be achieved in order to purchase CAM, with offenders arguing that if the material is not new it should be freely available while producers might charge for new material⁵⁴.

Overall there is a trend of child sex offenders moving into secure environments such as the Darknet, making use of its anonymity to facilitate the exchange of customised material, and therefore encouraging hands-on abuse.

Commercial sexual exploitation of children online (CSECO)

The traditional commercial exploitation of children online has seen a downward trend in recent years. The amount of commercially available CAM is estimated to be very low. The few investigators that were able to provide a percentage estimate mention an average of only 8.5% of commercial CAM.

In some cases of CSECO 'hackers-for-hire' are employed to hack servers of websites - typically those of small businesses hosted globally - in order to abuse their hosting. URLs directing individuals to commercial child abuse material hosted on the compromised server are distributed via spam. Typically these CSECO websites demand payment in Bitcoins⁵⁵. However, most of these websites are fraudulent and only aimed at obtaining money from individuals seeking online CAM, without actually providing any material.

51 Exchangeable image file format (EXIF)

52 CEOP - The Hidden Internet: Enabling Child Sexual Exploitation and Abuse

53 CEOP - The Hidden Internet: Enabling Child Sexual Exploitation and Abuse

54 CEOP - The Hidden Internet: Enabling Child Sexual Exploitation and Abuse

55 [IWF: Preliminary Analysis of New Commercial CSAM Website Accepting Payment by Bitcoin, 2014](#)

The once common use of credit cards for CSECO has seen a downward trend as a result of the proactive measures put in place by payment processors⁵⁶ and further availability of other, more anonymous, payment methods. Currently one of the upward trends for CSECO is the live streaming of abuse for which money transfer services seem to be the preferred payment method.

Live streaming of child abuse

The popularisation of webcams and chat platforms that enable the streaming of live images and video has led to their exploitation by child sexual abusers. Some applications allow users to upgrade their accounts by paying a fee, guaranteeing access to extended features such as broadcasts protected by passwords and extra layers of anonymity.

While live streaming is also common in sexual extortion cases, a trend has been detected concerning the abuse of children overseas, live in front of a camera at the request of Westerners. Payments per session can vary from USD 30 to USD 3000. A session allows the perpetrator the chance to orchestrate and view the abuse of a child in real time.

The abused children are from countries with deprived economies, typically in Eastern Asia. In the cases that have been investigated the financial profit is used to support the basic needs of the family or group involved. In these cases there has been a certain level of organisation, at a familial or community level.

The potential to earn money makes the crime of abuse via live streaming an attractive proposition. Payment for these services is made through international money transfer and, less frequently, via local money transfers.

The live streaming of child abuse is likely to be a growth area. It is a crime that is hard to detect and investigate since the offenders do not usually store a copy of the streamed material, therefore emphasis should be put on investigating the ordering and delivery of streamed CAM. In addition, the real-time monitoring of this type of transmission is legally and technically challenging.

The potential connection of live streaming to TCSOs should be taken seriously into consideration. The pay-per-view abuse of a child may lead to or be a consequence of the hands-on abuse of the same child. Those responsible for organising the online abuse may also be facilitating children's physical abuse by offenders.

Facilitators and relevant factors

The most common method for offenders to exchange CAM is still Peer-to-Peer (P2P) platforms. This is facilitated by

the ease of access to this type of platform and by the large amounts of CAM available for free within this medium. It is important to note that the offenders might start their online CSE criminal career by exchanging material in P2P, forums, emails, and other easily accessible platforms and move on to more sophisticated methods of accessing and distributing CAM, such as the Darknet.

The Darknet represents a significant threat in this area. The anonymity granted by these platforms is a strong enabling factor.

The use of encryption is also increasing and includes measures such as compressed files through to full disk and server encryption. Until recently *Truecrypt* was the most commonly used tool for encryption, together with *BitLocker* for full disk encryption. For server encryption *Luks* is frequently used.

Many offenders take their security very seriously, investing not only in encryption but taking other defensive measures such as using VPNs (Virtual Private Networks), secure email, disposable emails, proxies, prepaid Internet access, bullet-proof hosting services⁵⁷, free WiFi connections and disk wiping tools.

The usage of cloud services within CSEO is not yet common but is an emerging trend. These services allow offenders to store CAM remotely, enabling removal of materials from a distance.

Another facilitating factor for this crime is the increase in mobile devices and apps, which enable constant connection to the online world by both potential victims and offenders.

Law enforcement considerations

The lack of harmonised investigation capabilities among Member States (MS) creates additional strain on investigations.

Furthermore, the increased use of the Darknet, coupled with many Member States' lack of investigative powers to perform undercover activities, and lack of technical capabilities to access these environments, brings added difficulties to investigations.

Law enforcement does not usually have enough capabilities or resources to challenge these crimes in a significant way. Lack of cooperation agreements with some countries means that some investigations cannot be pursued, as does the limited or non-existent possibility to perform undercover investigations, for example, on the Darknet.

56 [European Financial Coalition: Strategic Assessment of Commercial Sexual Exploitation of Children Online, 2013](#)

57 Hosting services that by their nature or geographical location are largely immune to takedown requests by LE and which will knowingly host dubious content.



Also, the large quantity of data collected during operations, and its subsequent analysis, takes a great amount of resources and has implications both on the initiation of new operations as well as on the completeness of the different steps of an investigation such as thorough victim identification.

In addition, a shortage of human resources limits attempts to identify victims. Child sexual exploitation online, and the large amount of CAM available, requires dedicated capacity not only to be employed in investigations per se but also in victim identification (ID) which is sometimes not performed in MS. Victim ID is one of the most relevant aspects of the investigations as each time a victim is identified a child can be taken out of the exploitation environment, starting the recovery process.

In order to support this with effective victim ID platforms are necessary which, by augmenting the cross-matching possibilities, enhance the probability of identifying both victims and offenders.

Decisions concerning privacy and data protection, such as the EU Court of Justice ruling on Data Protection and the Initiatives such as the 'right to be forgotten', may bring added challenges to transnational investigations or hamper open source research on suspects.

An increased usage of encryption and anonymity devices bring additional complexity to investigations. A stronger focus on traditional LE work and increased liaison with intelligence services – infiltration, human intelligence (HUMINT), etc – might be of added value in overcoming some of the challenges LE faces in cyberspace.

Also the use of Big Data – pro-active/predictive approach to identify potential perpetrators⁵⁸ – needs to be well balanced with existing legislation and respect the basic principles of justice.

Cyberspace presents many difficulties for investigations but it is also true that CSE in which images are shared online is easier to trace. As long as adequate jurisdiction and investigative capacity is in place, offenders and victims are more likely to be identified in cyberspace than in the offline world.

The Internet can provide an inflated sense of anonymity and security to offenders that can work to law enforcement's benefit.

Future threats and developments

Darknet platforms will grow in number and availability. The technical skills quickly adopted by most child sexual offenders, together with a conscious understanding of risks, will direct more offenders to environments where levels of privacy and anonymity are high.

The impact of increasing Internet adoption rates in developing countries has already been felt by some Member States and third parties. It is expected that offences such as live streaming of CAM for a fee, which is currently happening mainly from Eastern Asia, will become increasingly popular in other East Asian countries, as well as in African and South American countries, since it generates high revenues for the criminal groups exploiting

58 [Laorden, C.; Galán-García, P.; Santos, I.; Sanz, B.; Hidalgo, J. and Bringas, P.\(2013\). "Negobot: A Controversial Agent Based on Game Theory for Detection of Paedophile Behaviour". Springer – Verlag, Berlin Heidelberg](#)

the children and presents low risks. An increase in CAM featuring varied ethnic groups can also be expected.

Live streaming may become a preliminary step for travelling sex offences: offenders who engage, via technical means, in the on-demand abuse of a child in a foreign country could travel to the same country for hands-on abuse.

There will be an increase in the use of virtual currencies for CAM. Producers of CAM may realise that new virtual currencies such as *Darkcoin* offer further anonymity possibilities and that there is an additional opportunity for financial gain in the exchange of CAM.

There is an increasing trend in providing access to mobile devices to very young children. As children handle mobile devices that can both take pictures, produce videos and access social networks with little supervision, sexualised self-generated material, and thus opportunities for sexual extortion, could continue to increase. The already existing geo-location capabilities supported by the devices, and consequent geo-referencing of pictures and videos, also offer extended opportunities for offenders to physically locate children of their interest.

The expansion of the Internet of Everything and the interconnectivity of electronic devices will create new opportunities for child abusers, further expanding offenders' access to images of children. There will be increased opportunities to hack into devices such as baby monitors and CCTV in schools and other facilities frequented by children. The increase in the availability of personal data will also enhance the possibility to forecast the personality traits, behaviour and location of people in general, offering more possibilities for paedophiles to research and engage with children.

There will be an increased use of technologies that facilitate the unnoticed recording and dissemination of images – the use of augmented reality wearable devices might facilitate the collection of children's images and other personal details.

The Crime-as-a-Service (CaaS) business model of the digital underground will open up greater opportunities for offenders to access expertise and tools which can be used to gain access to victims, their data and devices.

Affordable access to remote storage, especially when associated with encryption, will provide extended security for offenders, as they can remove CAM remotely, whilst limiting law enforcement with regards to evidential capture and forensic analysis.

Recommendations

- Most self-generated sexualised images observed in sexual extortion and sexting seem to be produced

through mobile phones and tablets. Cyber education should be implemented at schools from a very young age and adequate monitoring of children's use of mobile devices and the Internet should be considered by parents. Minors need to be educated on the impact of online exposure. Nevertheless the recourse to control children's access to the Internet should not be taken without consideration, as fear of being prevented access to the Internet might restrain children from confiding in their parents/adult supervisors.

- The implementation of reporting mechanisms such as 'panic button' apps in mobile devices or websites could be instrumental in increasing children's reporting of abuse.
- Law enforcement should invest in capacity building to improve Live Data Forensic expertise and capabilities, namely to take into consideration factors such as the use of remote storage and the existence of encrypted containers in the offenders' devices.
- Use of non-law enforcement mechanisms to report child abuse is of added value to increase the reporting of child sexual exploitation online and should be implemented or enhanced whenever possible.
- Law enforcement should dedicate resources to victim identification and investment in the broader adoption of best practices such as victim ID databases, taking into account the efforts undertaken by EC3 and Interpol in this field.

3.4 Payment fraud

Overview

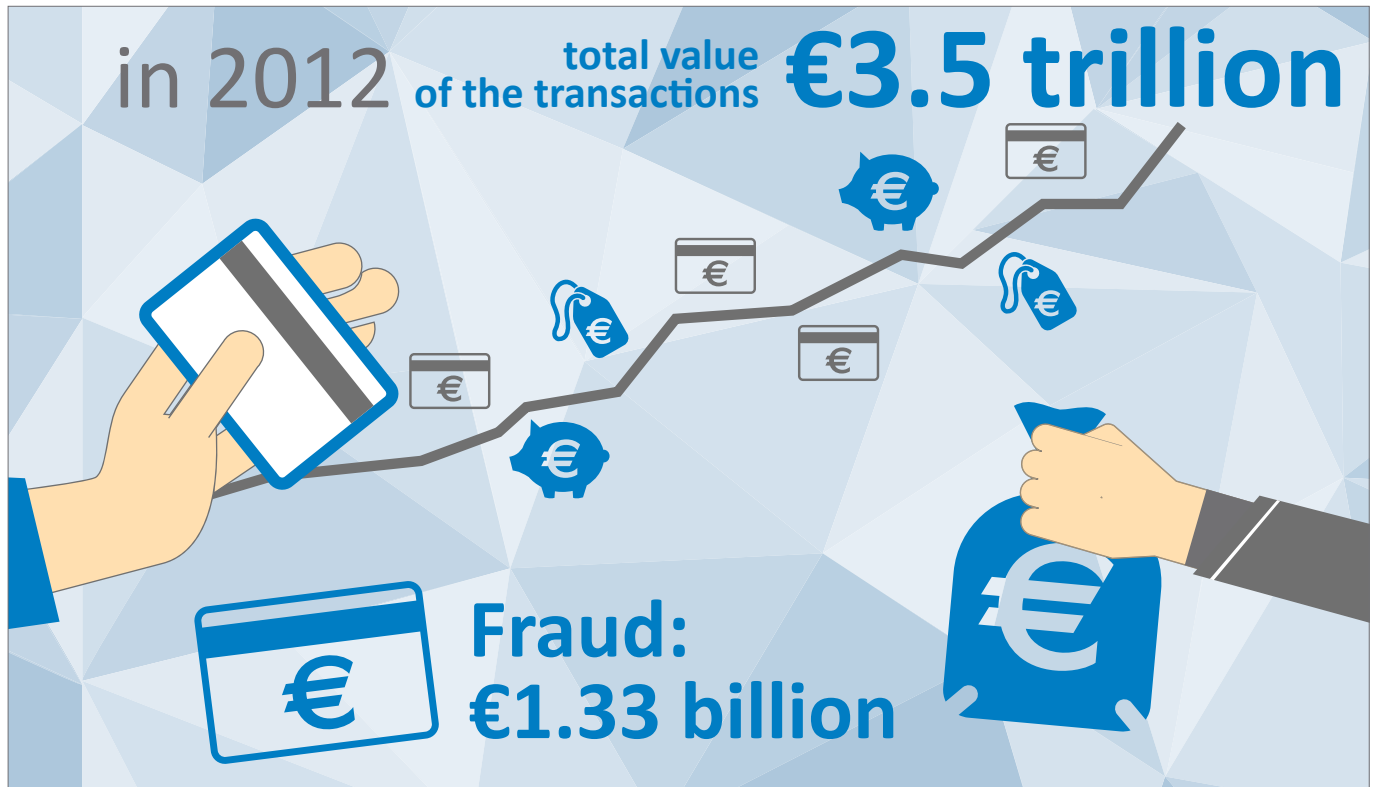
Payment card transactions are the most widespread non-cash payment method used in the EU⁵⁹. In 2012, the total value of transactions made by debit and credit cards issued within the Single Euro Payments Area (SEPA)⁶⁰ amounted to EUR 3.5 trillion⁶¹. In the same period, criminals acquired EUR 1.33 billion⁶² from payment card fraud (PCF). This represents 38 cents lost to fraud for every EUR 1000 worth of transactions.

59 [ECB: Press Release on September 10, 2013](#)

60 SEPA is an EU initiative to harmonise payments in euros, the objective of which is to increase the security and speed of financial transfers. As of April 2014, SEPA consists of all 28 EU Member States and 6 other countries: Iceland, Liechtenstein, Monaco, Norway, San Marino and Switzerland

61 [ECB: Press Release on February 25, 2014](#)

62 [ECB: Third Report on Card Fraud, 2014](#)



The real impact of payment card fraud is far more substantial due to the other costs associated with the crime. Merchants are paying an average EUR 2.79 for each EUR 1 of fraud losses incurred⁶³. Furthermore, expenses can be expected in terms of insurance, fraud management and crime prevention costs.

The financial impact of fraudulent payment card activity is not limited to increased costs. A 2013 European Commission survey found that 35% of EU citizens interviewed had concerns about the security of online payments, which translates into a reluctance to use online transactions⁶⁴.

In 2012, 60% of the total payment card fraud value occurred when the card was not present (CNP) at the transaction⁶⁵, which occurs predominantly online. Point-of-Sale (PoS) and ATM transactions accounted for another 23% and 17%, respectively. All categories of fraud experienced growth throughout 2012⁶⁶.

In 2014, the number of online transactions is estimated to reach 34.8 billion worldwide, almost twice the number from 2010⁶⁷. CNP fraud is likely to grow proportionately with the increasing number and volume of online transactions.

PCF has developed into a true hybrid crime that can occur in both online and offline environments. Regardless of where it occurs, the fraud inevitably includes two phases: obtaining the credit card details and monetising them. These are facilitated by online forums that bring together buyers and sellers of compromised cards.

Skimming (the extraction of card data from the magnetic strip of a payment card) continues to have a strong presence particularly across Member States in the Southern and Eastern part of the EU as well as in candidate and potential candidate countries.

However, most European countries have already observed an increasing shift from skimming towards CNP and this trend is being replicated across the continent. This migration has been fuelled by rising numbers of data breaches as well as implementation of effective counter-measures against skimming by the financial industry forcing the organised groups to refocus their criminal activities.

The Internet has changed the way traditional crimes such as skimming work. Skimming components can now be purchased online and the price of a skimming set is so affordable that even a single cashed out card may cover the cost of the investment. Many components are manufactured and dispatched from China, which offers the ideal mix of legal, environmental and economic conditions for the production of such items. The devices are then assembled in the EU, particularly in Bulgaria and Romania, before they are deployed to be used by organised crime groups (OCGs) abroad.

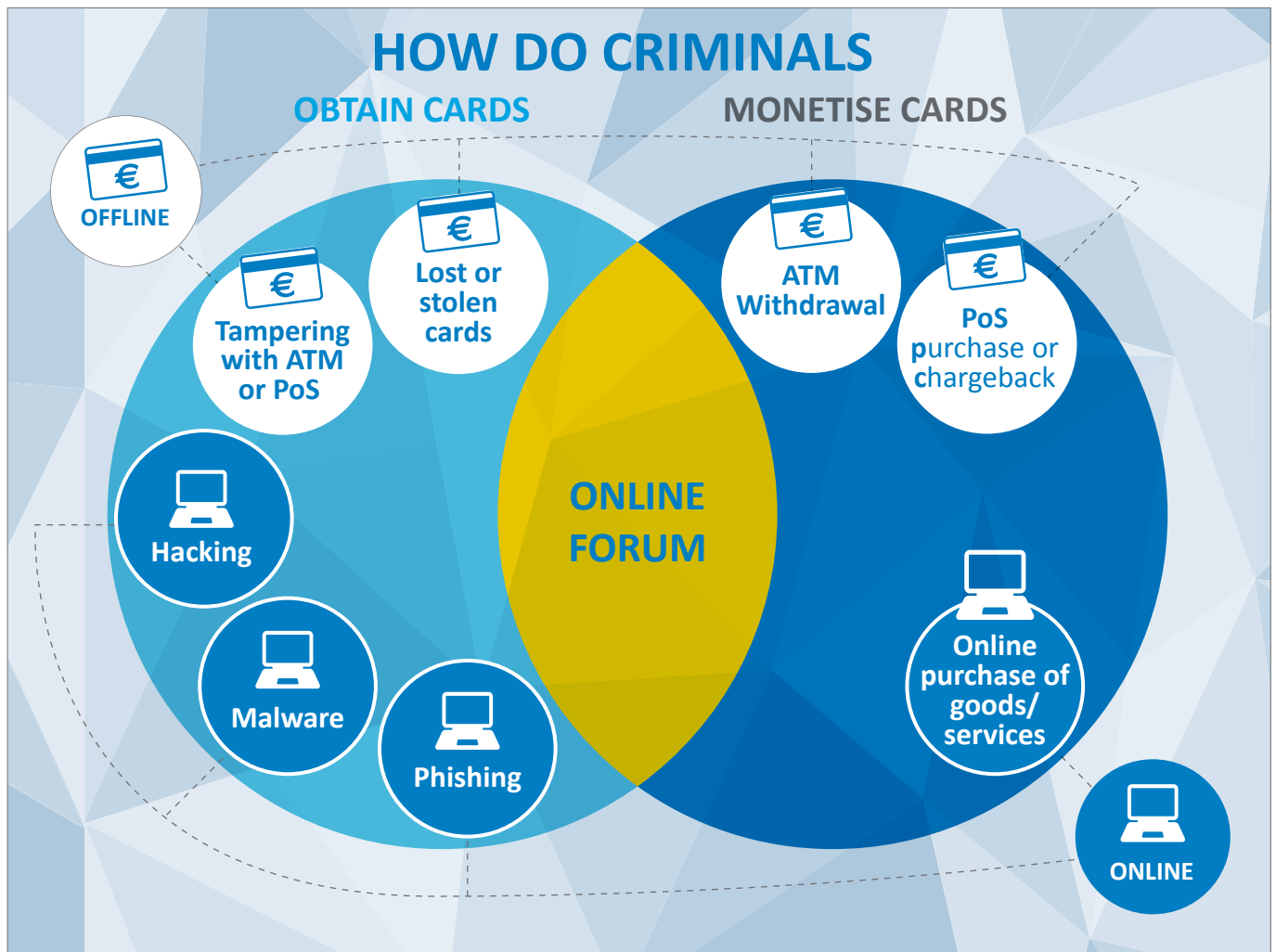
63 [LexisNexis – True Cost of Fraud, 2013](#)

64 [Special Eurobarometer 404 on Cybersecurity, 2013](#)

65 [ECB: Third Report on Card Fraud, 2014](#)

66 [ECB: Third Report on Card Fraud, 2014](#)

67 [World Payments Report, 2013](#)



Point-of-Sale (PoS) fraud is a threat to all merchants accepting payment cards. Traditionally, the criminals would obtain a terminal to study its operations in an effort to identify techniques of defeating its security mechanism. Compromising and returning the terminal to the merchant's location remains an effective method of obtaining the data⁶⁸. Another PoS threat is collusion of the merchant, where a staff member or owner of the business collaborates with the fraudsters.

However, a PoS breach no longer requires physical access to the device. The card data might also be obtained through a network intrusion. The starting point for the criminals may be network scanning to identify vulnerable PoS devices. Once discovered, attackers try a series of default passwords or conduct a brute force attack to access the network. When successful, the attackers proceed with installation of a malware that scrapes card data from the terminal's random-access memory (RAM) while it is being stored in an unencrypted state⁶⁹.

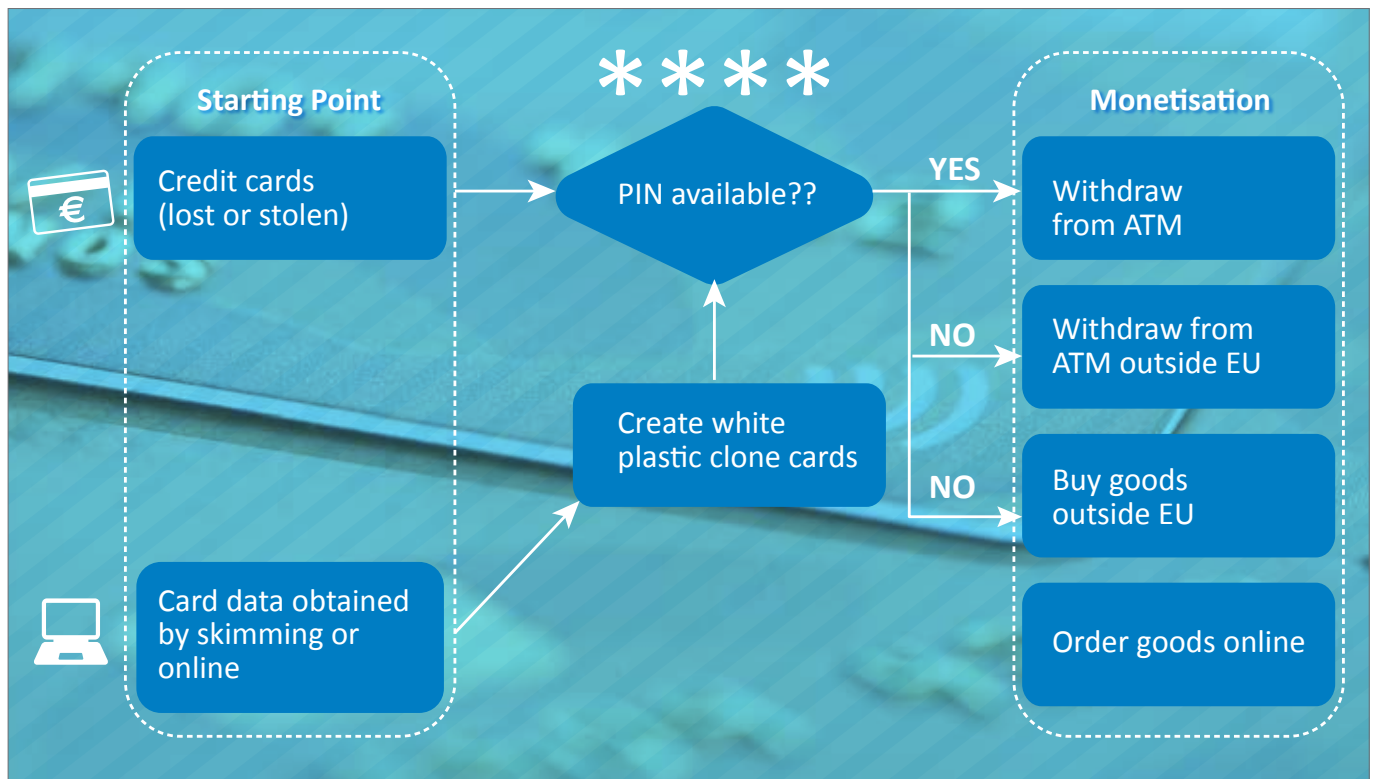
Online carding forums are a key enabler of payment card fraud, facilitating communication and trade between sellers and buyers of compromised data. These forums have lowered the entry barrier to PCF, increasing its volume. Although some of these forums have moved into the Darknet, many remain in the open web. A search query for the term 'cvv shop' generates hundreds of relevant results.

The sale of compromised data is becoming increasingly automated and industrialised. Automated Vending Carts (AVCs) are online services for selling bulk compromised payment card data. Customers can shop for data using a click-and-buy interface, tailoring their purchase by filtering variables such as country, postcode and issuer and thus circumvent Geoblocking protection.

Tools sold on the forums include credit card validity checkers, out-of-the-box skimming tools or items used to create the fake IDs required to open bank accounts. Adopting the one-stop-shop approach, the forums offer full packages including cashing-out, money laundering and after-sales care, mirroring professional commercial services provided by legitimate businesses.

⁶⁸ [MasterCard Academy of Risk Management: Understanding Terminal Manipulation at the PoS](#)

⁶⁹ [VISA Data Security Alert, August 2013](#)



Monetisation of the Card Data

Offenders have several options when converting stolen cards or card data into money:

Offenders possessing a card and its personal identification number (PIN) can withdraw the money from an ATM. Criminals who obtained the magnetic strip data need to upload these onto *white plastic* cards that can be purchased cheaply in bulk online.

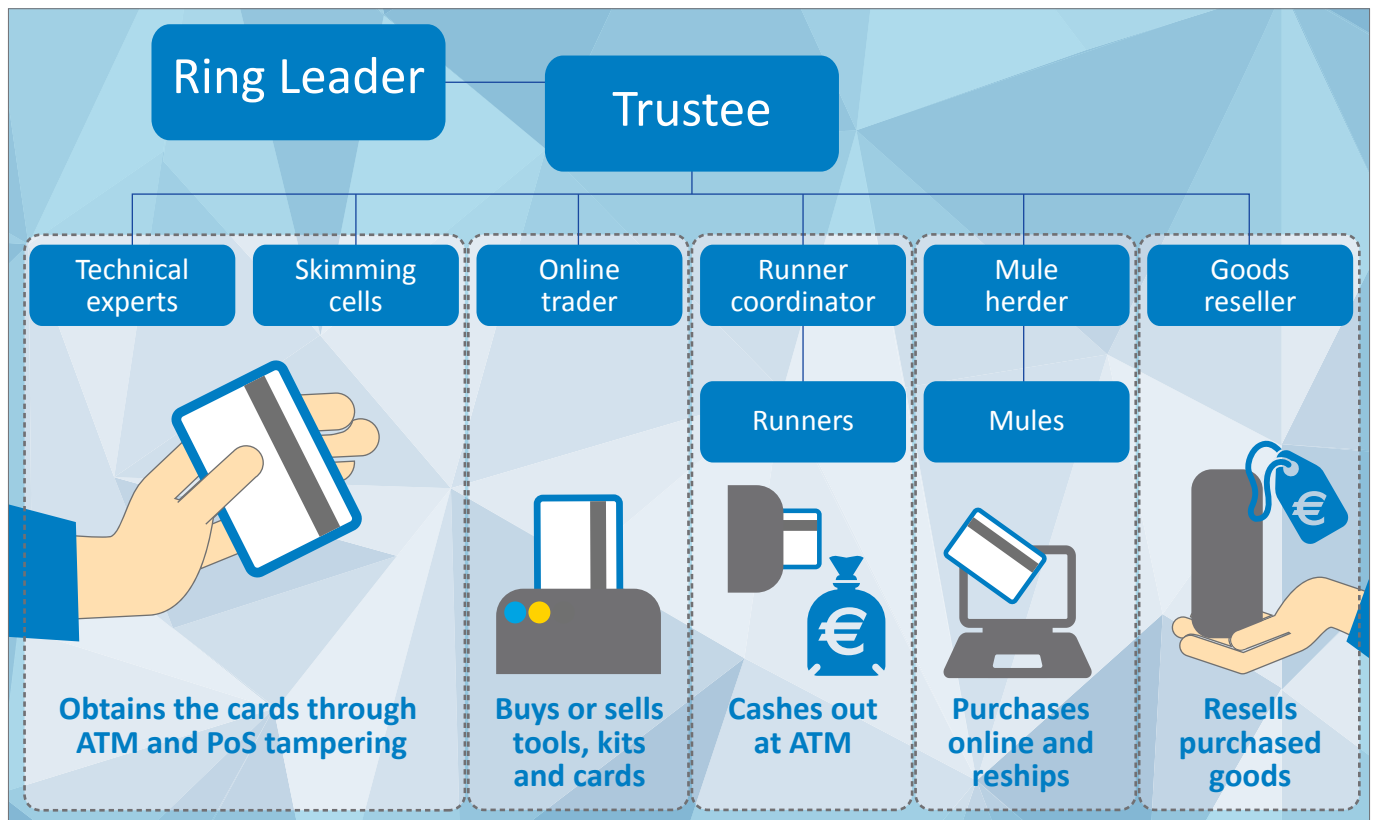
Payment cards without PINs are used to commit fraud in a country where chip and pin protection has not been fully implemented such as in the USA, South America and Asia. Another popular way to monetise card data without the accompanying PIN is to order goods or services online and have them delivered through a network of intermediaries to obfuscate the true recipient of the shipment. At the end of the shipping chain the goods are delivered to warehouses in Scandinavia or Baltic countries that are geographically located next to Russia – frequently the final destination, where the goods are sold through local websites.

Fraudsters use compromised cards to commit airline fraud - the purchase of airline tickets using compromised cards - often with the intention of travelling to and offending in multiple jurisdictions⁷⁰. EC3 initiated a joint multi-agency response to this threat involving law enforcement from a number of Member States, the US Secret Service, Colombia and Interpol as well as industry partners including card schemes, airlines, airports, travel agencies and the International Air Transport Association (IATA). Over a two-day period in April 2014, 113 individuals were detained at airports after purchasing tickets with compromised cards. The operation also resulted in a number of enquiries into further criminal activity, such as drug trafficking, smuggling and illegal immigration, further blurring the line between the online and 'real world' crime.

The airline fraud operation was suitable for transnational multi-stakeholder cooperation due to a number of factors: high levels of payment fraud affecting the industry⁷¹, few key market players, a centralised database to interrogate and, last but not least, the physical presence of suspects to arrest. Other areas suffering with high levels of payment fraud, such as purchase of luxury goods, accommodation booking or car rental, should be assessed for their suitability for similarly co-ordinated efforts in close cooperation with relevant stakeholders.

70 EC3 Cyberbits – Airline Action Day, 2013

71 [Visa Airline Fraud Guide, 2014](#)



Industry Prevention Measures

With nearly 40 billion card payments in SEPA in 2012⁷², robust prevention measures have been put in place to mitigate the levels of fraud. Efficient implementation of Europay, MasterCard and Visa (EMV) technology across EU countries⁷³ pushed fraudulent transactions overseas, particularly to Asia, South America and the USA. While the compliance rate across Asia and South America is gradually improving⁷⁴, the industry in the USA has been reluctant to adopt EMV mainly due to cost implications, although rising fraud levels may soon shift the cost-benefit ratio.

Despite the adoption of EMV technology throughout the EU, payment cards remain vulnerable to skimming as a result of the magnetic strip still present on cards for use in parts of the world where chip and PIN cannot be processed. To prevent its abuse, PoS and ATMs were equipped with 'low dip' card slots, which preclude full insertion of the card, preventing skimming of the strip.

3D Secure is an industry response to CNP fraud, familiar through 'Verified by Visa' or 'MasterCard SecureCode'. When adopted and implemented properly, this approach has led to a reduction in fraudulent online transactions. However major disparities in the adoption of 3D Secure across the EU countries exist⁷⁵, giving fraudsters the

possibility to circumvent the protection by targeting merchants that have not yet adopted it⁷⁶.

93% of transactions conducted using cards took place in the same country in which the card was issued. Although only 7% of all transactions occurred abroad, these contributed to 50% of the fraud⁷⁷. A large portion of this fraud could have been prevented by *Geoblocking*, working on the basis of rejecting all transactions that occur outside a permitted area. This has significantly reduced fraud in countries where it was implemented.

Criminals

The majority of attackers behind online card data thefts hail from Eastern Europe, particularly from Russian-speaking countries. The offenders tend to be males aged between 20 and 35 years with advanced but often self-taught computer skills and little connection to 'traditional' crime. This contrasts with the traditional skimming gangs frequently involved in other serious organised crime including human and drug trafficking, extortion and prostitution.

The majority of the offenders involved in skimming migrate from Bulgaria or Romania. These groups are highly mobile and avoid detection by employing hit and run tactics – being active in one jurisdiction for a few days before moving on to commit crime in another.

⁷² [ECB: Press Release on April 29, 2014](#)

⁷³ [EMVCo: worldwide EMV deployment statistics as of Q4 2013](#)

⁷⁴ [EMVCo: worldwide EMV deployment statistics as of Q4 2013](#)

⁷⁵ [Ogone: 3D Secure Landscape in Europe](#)

⁷⁶ [TSYS: EMV is Not Enough: Considerations for Implementing 3D Secure, 2013](#)

⁷⁷ [ECB: Third Report on Card Fraud, 2014](#)



Offenders who attempt to monetise card data obtained from online forums can be both individuals as well as OCGs. Even organised groups can have a very simple structure with a single person acting as the buyer from online forums and monetising these through a network of associates.

Criminals known to be involved in skimming often tend to form OCGs. These groups are either structured hierarchically or operate as a network of separate cells. The leaders are very skilled at distancing themselves from the crime and only communicate with the gang through trustees in charge of different cells. One cell organises the production of the skimming devices, another recruits *runners* who tamper with the ATMs and a third cell is in charge of withdrawals and transfers. Recent investigations have indicated that OCGs may be involved in both online and offline payment card fraud operations using the uppon structure:

Traditionally, OCGs used to predominantly operate in silos within the confines of ethnic or national diasporas. However, the dynamics of the OCGs are shifting with the industrialisation of crime driven by *Crime-as-a-Service*, and the composition of the crime groups is increasingly based on skill and value for money ratio rather than social factors.

Law enforcement considerations

Limited resources is one of the main challenges faced by EU law enforcement when investigating payment card fraud. This is a consequence of several factors, one of which is under reporting. The resulting incomplete intelligence picture prevents the linking of associated incidents resulting in insufficient allocation of resources for the investigation. Limited resources then have a negative effect on crime detection, which in turn leads to further under reporting as victims may get the impression the police cannot effectively deal with the online fraud cases.

For the financial industry, fraud losses are a sensitive topic, as disclosure of this information in an attributable way

could cause reputational damage. Similarly, companies that experience data breaches are concerned with PR issues instead of reporting the attack for LE investigation. These factors lead to under reporting of crime and an artificially low perception of the risk of the crime by society. To address the issue, some Member States have created confidential reporting mechanisms for businesses - the financial industry in particular.

The limited number of resources is also affected by the lack of ability to link related incidents to a single case. While the total damage of an attack might be significant, the reported crimes may end up fragmented among many incidents that are never associated as a single case. This contributes to a lack of justification for the resources needed to run an investigation.

Companies looking to implement cost cutting measures may be increasingly tempted to outsource payment processing operations to third world countries. However, the savings may come at the price of more relaxed security measures, possibly resulting in large scale data thefts. An increasing level of outsourcing will result in further obstacles for law enforcement authorities requesting data for evidential purposes.

While EMV technology has managed to decrease skimming within the EU, this has pushed the cashing out of cards overseas, making it more difficult for LE to obtain evidence.

GPS receivers are getting smaller, discreet and manage to operate longer. This provides law enforcement with an interesting possibility to arrange controlled deliveries of goods ordered by the fraudsters.

Future threats and developments

The USA is one of the most popular locations to cash-out compromised cards due to low prevalence of EMV protection. In 2015, the situation may improve due to a *liability shift* that may result in a strong push towards the



adoption of EMV. The shift means that the issuers and merchants still using non-EMV compliant devices will become liable for all fraudulent transactions⁷⁸. Should this initiative succeed, it would significantly hamper the abuse of European cards in the US.

Similar to EMV protection, which displaced crime to non-compliant jurisdictions, implementation of Geoblocking is likely to have a negative effect on fraud in countries where it was not yet implemented. For example, a rise in skimming in Sweden was likely driven by Geoblocking adopted in nearby countries.

3D printing may become a driving force behind payment card fraud, facilitating convenient customisation of skimming devices for different models of ATMs. This follows the trend of the industrialisation of cybercrime, allowing for mass production of skimming units. The schematics for the devices can be shared on P2P networks and traded on online marketplaces.

Although they currently attract too much attention to be practical for criminals, wearable technologies may soon prove their value for shoulder surfing criminals.

The proliferation of smart phones has given rise to a number of different mobile and contactless payment technologies, such as Near Field Communication, QR codes, mobile wallets or Bluetooth Low Energy. While it remains hard to predict the outcome of this competition, it can be assumed that mobile and contactless phone payments will continue to grow in popularity for reasons of convenience and availability. This will inevitably make them an attractive target for criminals looking for exploitable vulnerabilities in these technologies. On the

other hand, once widespread, mobile and contactless payment technologies may lead to a decrease in traditional forms of attacks such as skimming or shoulder surfing.

Recommendations

- Law enforcement should set up confidential platforms for businesses to report the theft of sensitive data and other compromises.
- Law enforcement should establish Single Points of Contact (SPOC) to liaise with the financial sector and direct all incoming and outgoing information flow through this channel.
- Law enforcement should establish procedures for notifying financial partners in case compromised data is discovered in order to mitigate potential or further fraud.
- Law enforcement should engage fully with Europol's EC3 and Focal Point (FP) Terminal. Exchange of operational data with other Member States (MS) and EC3 may lead to identification of common links between the cases and prevent duplication of investigative efforts. Law enforcement agencies should share lists of forums and AVCs.
- Law enforcement should strengthen cooperation and information sharing with other MS as well as with countries where the compromised cards are cashed out.
- Law enforcement should cooperate with search engine operators to prevent carding forums featuring among the search results.
- For skimming cases close cooperation with banks is essential to swiftly identify common point of compromise and to link crimes to the relevant case. Time is of the essence as these crimes are often committed by migrating criminals.
- If not possible to take down identified forums, law enforcement should consider infiltrating these with an undercover presence where national legislation permits.
- Following the successful operations against airline fraud, other areas of payment card abuse should be identified and addressed on a European or national level.
- The financial sector and merchants should implement the existing anti-fraud measures such as Geoblocking and 3D Secure to protect their customers from abuse of their payment card credentials.

⁷⁸ [VISA, US Merchant EMV Acceptance Readiness Guide, Mastercard EMV for US Acquirers: Seven Guiding Principles for EMV Readiness, 2012](#)

3.5 Criminal finances online

Overview

The final phase in most cybercrimes is to successfully launder the proceeds of crimes into the legal economy, often entailing their movement across jurisdictions. Smuggling large amounts of cash around the world remains a popular option for criminals despite the risk of seizure of undeclared cash exceeding EUR 10000 by customs agents⁷⁹. Alternative methods include a variety of offline and online payment methods such as bank transfers to accounts opened with fake IDs, prepaid cards, wire transfers through Western Union and Moneygram, Ukash, Paysafecard, Paypal, Paymer, trust-based Hawala transfers or virtual currencies. The plethora of payment mechanisms used by cybercriminals to cash out virtual proceeds demonstrates that criminals exploit any system where they believe there is little risk. More sophisticated offenders also exploit legal business structures to obscure the link between proceeds and underlying criminal activities. The industrialization of crime has also led to the emergence of specialist entities that manage money laundering for multiple illegal enterprises.

Another method is the use of online gambling services; in 2013, the total value of this sector was approximately EUR 26.1 billion and is continuously growing⁸⁰. Unregulated or inadequately regulated online gambling has been exploited for money laundering purposes for years. Such services manage huge volumes of transactions and cash flows - making it easier to hide comparatively small amounts of illicit activity - and are tax free in many jurisdictions. This provides criminals with the ability to conceal and transfer assets while avoiding detection by law enforcement agencies.

Money Mules

Money mules provide a key service in the laundering of criminal proceeds from cybercrimes. They are the most visible link between the online and offline worlds. Acting as middlemen they receive goods or funds and forward them to the offender in exchange for a commission, typically 3-5% of the transferred amount or, in some cases, a monthly salary. To avoid laborious duties connected with recruitment and micromanaging mules and to distance themselves from the physical crime, elite criminals use the services provided by a *mule herder*.

The mules can be either professional criminals or naïve individuals recruited online through email campaigns or classified adverts. Gradually the mules who were initially unwitting, slowly come to understand the true nature of



their 'job', yet often continue to engage in the illegal activity for their own financial gain⁸¹. Money mules are often in acute need of money, such as unemployed individuals, students and housewives. Money mules can also be absent immigrants who have sold their bank account details to an OCG.

Virtual Currencies

Virtual currencies offer a particular set of features that make them attractive to online criminals: anonymity or 'pseudonymity', and the rapid and irreversible transfers of funds for minimal transaction fees compared to conventional banking. Virtual currencies offer a level of anonymity similar to cash in the online environment and have arguably become a major facilitator for all financially-driven cybercrime.

Virtual currencies fall into two categories - *centralised* (or scheme-based) and *decentralised*. Centralised currencies such as *WebMoney* and *Perfect Money* are run and administrated by a single entity which manages the scheme in a role analogous to a central bank (although they are not banks and therefore need not adhere to the same rules and regulations).

Decentralised currencies such as *Bitcoin* and *Darkcoin* have no such entity administering them, operating instead across a distributed peer-to-peer network of user nodes. Each transaction on what is known as the *blockchain* is open to public scrutiny, only the particulars of the remitter and benefactor are obscured.

The conversion between fiat currencies and virtual ones, or from one virtual currency to another generally takes place via online *exchangers*. Although most of these

⁷⁹ [EC Regulation No 1889/2005 on Controls of Cash Entering or Leaving the Community](#)

⁸⁰ www.bvwinparty.com: The Online Gaming Market

⁸¹ Input from Advisory Group on Financial Services, 2014

services are legitimate, they exist as a service within the digital underground economy, offering additional security to their customers.

Although generally designed for legitimate use, virtual currencies are heavily abused by cybercriminals. Cybercriminals often favour centralised schemes which, being tied to tangible assets, are inherently more stable compared to cryptocurrencies whose price is often highly volatile due to high levels of speculation. Of the centralised schemes favoured by the criminal community *WebMoney* is still very popular, particularly for criminal-to-criminal payments, as is *Perfect Money* to a lesser extent.

Another type of centralised scheme popular with cybercriminals is those that use a voucher system such as Ukash and Paysafecard. Voucher systems allow customers to purchase a coded voucher to which the scheme allocates the purchase value. The code is then redeemable at participating outlets, or easily and anonymously transferrable to a third party.

While historically decentralised virtual currencies or cryptocurrencies have not been popular with cybercriminals, they have become the currency of choice for internet-enabled traditional crime on the Darknet. Hidden marketplaces such as *Silk Road* typically use Bitcoins as a method of payment.

The takedown of first *E-Gold* in 2009, and subsequently *Liberty Reserve* in 2013, has resulted in a growing level of distrust in centralised schemes as cybercriminals are increasingly adopting cryptocurrencies. Bitcoin is beginning to feature heavily in police investigations, particularly in cases of ransomware and extortion.

A feature of cryptocurrencies that makes them an attractive alternative to cybercriminals is their distributed nature which makes them resistant to law enforcement disruption and government control - a premise at the heart of the cryptocurrency philosophy. So why then have cybercriminals not shifted their operations over to these systems?

The transparency of such systems is a likely deterrent, potentially providing law enforcement with a financial trail to follow. The market is also volatile with currency prices fluctuating significantly and often. Furthermore a number of exchange services were hacked in 2014 with many users losing their online e-wallets with no recourse for compensation.

Money Laundering Using Virtual Currencies

Virtual currencies have the potential to become an ideal instrument for money laundering. Entry to and exit from the system is typically via an exchanger. Exchange services are another niche service offered in the digital underground economy. However, legitimate exchangers

are also exploited, particularly those which carry out little Know Your Customer (KYC)⁸² processes and offer multiple methods to 'cash out' including payments via pre-paid or virtual credit cards and Money Service Bureaus.

Once in control of the digital funds, the ease of creating new e-wallets means a launderer can easily discard 'dirty' wallets. In addition to traditional layering methods, cryptocurrencies use specialised laundering services known as 'tumblers' or 'mixers'.

'Tumblers' are services, often operating on Tor⁸³, which allow users to transfer their cryptocurrencies into a pool of funds and then receive them back (minus a small commission) into newly generated 'clean' addresses, thereby breaking the financial trail.

When considering money laundering through online gambling, the introduction of the possibility to pay, play and cash out using virtual currencies has added a new level of anonymity. Indeed a new generation of online casinos has emerged specifically for cryptocurrencies⁸⁴, some of which promote themselves on the level of anonymity they provide, advocating the use of TOR⁸⁵, if not *only* being accessible via TOR.

Law enforcement considerations

Within the constraints of national legislation law enforcement should pursue the possibility to obtain evidence from virtual scheme operators as they would do from any other financial institution. Investigators should also have the possibility to have accounts and funds frozen for the purposes of confiscation.

Decentralised schemes offer significant challenges to law enforcement. It may be possible to obtain addresses that the suspect uses through other investigative means, but with no central body to approach for additional information this is of limited value. Potentially an investigator could follow the flow of funds to and from that address on the blockchain to identify transactions with a real world entity such as an exchanger, online casino or other merchant. Should that outlet be approachable by law enforcement it may be possible to obtain a link to the address holder. Another barrier for law enforcement is that, other than by physically seizing the device on which a suspect holds his e-wallet, there is no way to confiscate, freeze or otherwise block access to the funds held by the suspect. Moreover, the variety of payment mechanisms used by cybercriminals presents an additional challenge.

82 Process used by businesses to verify the identity of their clients

83 e.g. [Bitcoin Fog](#)

84 e.g. [SatoshiDice](#)

85 [McAfee 2014, Jackpot! Money Laundering Through Online Gambling](#)



Virtual currencies represent an example of technology overtaking legislation. Few jurisdictions recognise virtual currencies as a currency or have managed to adopt adequate regulatory controls. As such the law enforcement response between jurisdictions varies significantly. Some jurisdictions consider virtual currencies to be goods or property; some consider them to be taxable assets. Some jurisdictions regulate only centralised services, some only regulate the services surrounding them such as exchangers. Such disparity across Europe creates additional challenges for law enforcement and opportunities for criminal exploitation. The freezing and subsequent confiscation of criminal assets is an integral part of many investigations, but the combination of unseizable cryptocurrencies and inadequate legislation clearly causes issues. For cybercriminals, cryptocurrencies may become the offshore accounts of the future.

The activity of mule herders may be detected through monitoring ads relating to home-based, part-time positions such as ‘*payment processor*’ or ‘*regional agent*’. Another position advertised is that of ‘*mystery shopper*’⁸⁶, where mules are asked to purchase goods from high street shops and send them over to the fraudster along with completed satisfaction questionnaires.

Wire transfers remain a popular method for onward transfer of funds for criminals and frequently feature in both traditional as well as cybercrime investigations. This is likely due to a perceived diminished risk of detection due to less stringent customer identification and verification procedures as well as availability of these services worldwide.

⁸⁶ ABA Bank Compliance, 2014

Future threats and developments

It is unlikely that any centralised scheme will seek to take on the mantle of *Liberty Reserve* due to risks associated with attracting high law enforcement attention. Even without a successor, the digital underground will continue to use and abuse legitimate schemes as long as it proves safe and profitable for them to do so.

As cryptocurrencies continue to evolve, it is likely that more niche currencies will develop, tailored towards illicit activity and providing greater security and true anonymity. Several Russian language underground forums have created their own private currencies. Schemes such as *MUSD*, the *United Payment System* and *UAPS* have been developed to cater specifically for these markets⁸⁷. Proliferation of these schemes will permit an entire criminal economy to flourish with little possibility of law enforcement intervention.

Cryptocurrencies operate using asymmetric encryption. Should sufficient processing power come under criminal control, it is conceivable that it could be turned to brute forcing the private keys of some of the wealthiest Bitcoin addresses. 20% of all Bitcoins, representing over USD 1.4 billion, are currently held in only 100 Bitcoin addresses⁸⁸. With today’s current processing power however this is not possible, but with developments in powerful quantum computers it may become more than hypothetical.

A number of malware variants on both PCs and mobiles include e-wallets in the data they harvest from infected devices. Other variants turn their hosts into cryptocurrency miners, using the devices’ processing power to generate freshly mined coins for the attackers. We expect this to become more commonplace.

Recommendations

- Countries should ensure that policy-makers, financial intelligence units, law enforcement authorities and other relevant competent authorities have mechanisms in place to facilitate cooperation and coordination concerning the development and implementation of money laundering policies⁸⁹.
- Legislative changes at EU level, or the uniform application of existing anti-money laundering regulations are required to address the criminal use of virtual currencies.

⁸⁷ [The RSA Blog and Podcast - Mo Money Mo Problems, 2014](#)

⁸⁸ [Bitcoin rich list](#)

⁸⁹ [The FATF Recommendations, 2013](#)

- Law enforcement should strengthen relationships with money transfer businesses to promote lawful assistance in the identification of suspicious transactions and suspects.
- Virtual currency scheme operators and exchangers should fall under the same regulatory framework as their non-virtual counterparts, providing protection for consumers and accountability on the part of the scheme provider. The absence of the central authority makes the enforcement more problematic for the decentralised cryptocurrencies while for certain schemes such as the private forum currencies, regulation will have no impact at all.
- Law enforcement should develop a working relationship with the financial sector including banks, money transfer agents, virtual currency scheme operators and exchangers in order to promote the lawful exchange of information and intelligence.
- Digital investigators need to be familiar with how virtual currencies operate and how to recognise the wide variety of digital accounts which may hold a suspect's digital assets.
- Forensic teams must be aware of the nomenclature and file formats for digital currency wallets and accounts so that these can be identified and retrieved during analysis of a suspect's device.
- Law enforcement should establish relationships with the major cryptocurrency exchanges and websites offering cryptocurrencies for sale, with a view to facilitating the exchange of relevant information and intelligence in a lawful manner.
- Law enforcement should work in conjunction with relevant public sector actors to initiate awareness campaigns targeting prospective money mules.
- Law enforcement should not cease investigative efforts after detecting the low level mules. It is important to follow the flow of money or goods upstream to other jurisdictions to map the criminal network.
- Law enforcement should proactively monitor job classified job advertisements for those that are suspicious. Increased activity of mule herders may indicate upcoming fraud operation.

3.6 Crimes relating to social engineering

Overview

Social engineering refers to a set of offline and online methods and techniques that aim to manipulate a victim into voluntarily releasing sensitive information or into transferring money. Social engineering is used because *people* are often the weakest link in system security and the associated costs of such an attack are often significantly smaller compared to attacks on computers and networks⁹⁰.

Online social engineering often uses spam and phishing techniques. Since there are almost no costs attached to attempts, the majority of these attacks are distributed en masse to get as many responses as possible. Some attacks are targeted, however *Spear Phishing* or *Whaling* targets high-profile individuals or members of a certain group such as employees of financial institutions.

Spam

Spam uses a variety of communication vectors such as e-mail, social networks, messengers, blogs, forums, comments, autodiallers or SMS messages. Scammers use a number of schemes to get access to the victim's data and wallet, with most of these falling into the following categories:

While the core mechanic of these scams remains consistent, the *modus operandi* follows the latest technological trends, such as cryptocurrency transactions.

In 2013, cybercriminals distributed spam leading to a fake Mt. Gox⁹¹ website where they captured login credentials and requested transfers to their Bitcoin wallet⁹².

The total daily volume of spam in 2014 is approximately 80 billion messages⁹³. However, not all spam reaches its destination. Throughout 2013, roughly 70% of the spam was automatically filtered out⁹⁴ utilising methods such as *machine learning* and *crowdsourcing* - using feedback from users to flag spam. The share of blocked emails decreased from almost 90% in 2010⁹⁵ mainly due to spam moving to different platforms and botnet takedowns.

⁹⁰ Mitnick, K: "CSEPS Course Workbook", 2004

⁹¹ Mt. Gox was a Bitcoin exchange based in Tokyo, Japan

⁹² [F-Secure: Threat Report, 2013](#)

⁹³ [Trend Micro Global Spam Map, 2014](#)

⁹⁴ [Microsoft Security Intelligence Report, volume 16, 2014](#)

⁹⁵ [Messaging Anti-Abuse Working Group, 2011](#)

Motivation	Scam Type	Modus Operandi
Money	Advance fee	Pay money to get money e.g. Nigerian letters, lottery, inheritance...
	Advertisement	Buy fake-/non-existent goods, often medication
	Dating	Send money to cover medical care, flights or visa
	Investment	Invest into non-existent/fraudulently valued companies and pump and dump schemes
	Employment	Pay upfront administration fees for a falsely promised service and/or become a money mule
	Friend in need	Send money to a friend in need whose email, twitter or social network account has been hacked
	Charity	Contribution to an unregistered charity
Sensitive Information	Phishing	Disclose exploitable information, such as credentials e.g. banking scam, tax scam, raffles
Malware	Malicious website or application	Click the malicious link. A friend's message, adult content, fake virus alerts and breaking news are particularly effective to attract victims' attention

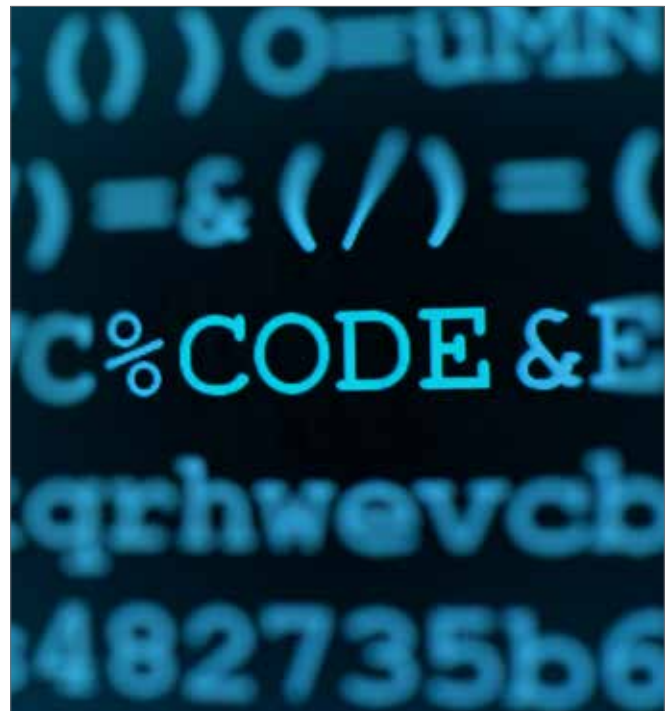
Phishing

The majority of phishing incidents start with potential victims receiving spam, luring them to websites attempting to elicit login credentials and other sensitive data from them, or hosting exploits designed to compromise the visitor's computer system.

A victim's account details were obtained by phishing emails and sold to a UK suspect for GBP 3,200. Subsequently, over GBP 1 million was stolen from the account in a case that stretched from South Africa to the UK and involved Egyptian and Nigerian nationals.

A number of phishing variants have developed to exploit different communication technologies. These target victims through automated redirects to a bogus website (pharming), SMS (smishing) or phone or VoIP (vishing). Vishing was used to contact victims in the so-called *tech support* scam, where scammers pretend to be engineers from a software company. A survey of 7000 computer users in the UK, Ireland, US and Canada revealed that 15% of respondents were contacted by the scammers. Of these, 22% handed over credentials needed for a remote connection⁹⁶. In 2013, the scammers replicated the fraud on the Mac platform and at the beginning of 2014, they began targeting Android users⁹⁷.

Many cyber attacks cannot be easily categorised as pure malware compromises, hacking, man-in-the middle



attacks or social engineering, as typical incidents may involve a combination of these methods. When criminals are able to exploit a victim's identity and data in both the physical and online world, they can maximise both the effectiveness of the crime and the impact on the victim.

Facilitators and Relevant Factors

Entry into phishing is facilitated by the Crime-as-a-Service model. On online forums, offenders can get everything they need to carry out attacks – tutorials, support, tools, templates and even large, sorted datasets of prospective

⁹⁶ [Microsoft Survey, 2011](#)

⁹⁷ [Malwarebytes research: Tech Support Scammers Target Smartphone and Tablet Users, 2014](#)



victims. Offenders conducting the more sophisticated attacks often use tools purchased from more technically skilled offenders and may return to the forums to sell harvested data to other offenders for exploitation.

Offenders go to great lengths to make their scam appear legitimate and many scams occur as a result of scanning social networks and other open source data.

In Switzerland, scammers used publicly available data provided by a commercial registry to establish bogus websites for companies with no website of their own. They chose domain names similar to that of the company and made their website appear legitimate and trustworthy for unsuspecting visitors.

Many spam and phishing attacks use URL shorteners, allowing attackers to hide malicious links behind them⁹⁸. This technique emerged over five years ago and has since been used for both genuine as well as nefarious purposes.

In 2013, approximately 76% of spam was sent from botnets⁹⁹. These provide criminals with monetisation opportunities as well as spreading the malware, fuelling the future growth of the botnet. Attackers may also use the infected bots as SMTP servers and channel spam through these. The main benefit is bandwidth and the large number of different network identities which prevents the spam messages from being easily filtered and/or traced.

Spam and phishing are dependent on the availability of contact details and other personal data. The supply of these is bound to increase due to the number of large scale data breaches in companies holding huge volumes of consumer data.

The growth of the internet gave rise to *data brokers*, companies competing in a multi-billion euro industry hidden from the view of those whose data is traded. They collect personally identifiable information including online searches, shopping patterns and health statuses, building up a database of consumer demographics which is later sold, often for marketing purposes. Hence it is possible to foresee abuse of this data for spam or phishing¹⁰⁰.

Victims

Despite the publicity generated by certain scams and prevention campaigns, the number of victims falling for phishing has increased across Europe. Particularly affected are elderly people who lack internet skills and who are generally more trusting and respectful of official-looking material¹⁰¹ than younger generations.

Although there is no hard evidence relating to the prevalence of repeat victimisation for cybercrime, many victims falling for scams are likely to be targeted by the criminals again - a concept known as a double-dip scam. For example, the victim may get an offer to recover the lost money in exchange for a fee.

Some organisations will be a target regardless of what they do, but most become a target because of what they do¹⁰². Major national or international financial institutions and payment services are frequently singled out and accounted for 78.2% of phishing attacks at the end of 2013¹⁰³.

99 [Symantec: Internet Security Threat Report, Volume 19, 2014](#)

100 [US Senate, Committee on Commerce, Science and Transportation: A Review of the Data Broker Industry: Collection, Use and Sale of Consumer Data for Marketing Purposes, 2013](#)

101 [Arfi, N., Agarwal, S., Knowledge of Cybercrime among Elderly, 2013](#)

102 [Verizon Data Breach Investigations Report, 2013](#)

103 [APWG, Phishing Activity Trends Report 4th Quarter 2013, 2014](#)

98 [Symantec: Internet Security Threat Report, Volume 19, 2014](#)

Law enforcement considerations

In 2013 around 3% of internet users in the UK experienced financial losses from phishing attacks in the previous 12 months¹⁰⁴. While this figure is likely to underestimate the scale of the losses, given that it is challenging for victims to accurately attribute the source of their financial loss to a phishing attack, it is still significantly higher than the number reported to law enforcement.

The detection rates for this type of crime are low and sentences have historically been modest relative to the criminal gain. Since fraudsters engage in a rational calculation, making an assessment of the benefits and costs, lenient sentences do little to diminish their inclination to offend¹⁰⁵.

Phishing incidents, particularly those occurring across multiple jurisdictions, require many investigative resources and often lead to with an uncertain result as the attackers adopt multiple levels of obfuscation, such as registering phishing domain names via privacy or proxy services¹⁰⁶.

Some joint law enforcement and private sector efforts have successfully targeted and disrupted phishing websites. The uptime of phishing websites declined in the second half of 2013, with the majority of the websites being active on average for less than eight hours¹⁰⁷.

Future threats and developments

As global technological knowledge continues to mature, new and more complex methods of social engineering is expected. The development of artificial intelligence may soon have a practical impact on offenders harvesting information through automated spam and phishing campaigns¹⁰⁸.

High speed broadband has become available in developing countries. This will increase the number of attacks from West Africa which traditionally ranks high for incidents involving spam and social engineering, and will likely further develop with a gradual shift to more sophisticated crime¹⁰⁹.

Social networks are likely to be increasingly targeted, particularly if they implement payment mechanisms through fiat or virtual currencies.

Customisation of phishing attacks is increasing. Replica sites with SSL encryption will become more widespread, targeting users in their local languages¹¹⁰.

The Internet of Everything (IoE) offers new attack vectors for criminals. Spam campaigns disseminated via IoE devices will pose new challenges for forensic examinations.

Recommendations

- Law enforcement should focus on targeting botnets spreading spam, taking them down where possible in close cooperation with the private sector. Take-downs result in disrupting core infrastructure used to conduct a variety of cybercrimes, denying sources of income and further growth for the whole cybercrime community.
- Law enforcement should develop working relationships with both global and national webmail providers and social media with a view to exchanging relevant information, considering using EC3's relationships with these entities to the full extent.
- Law enforcement should decide whether and how to record high volume yet extremely under reported crimes such as spam or phishing. The Anti-Phishing Working Group (APWG) could be consulted in relation to technical aspects of the reporting model for these types of crimes.
- As law enforcement cannot cope with the volume of internet scams¹¹¹, it is advisable to prioritise the use of scarce resources in conjunction with EC3 to tackle high impact criminal campaigns.
- Law enforcement should establish relationships and two-way communication with the national organisation(s) running national anti-scam or anti-phishing campaigns or create such initiatives if no such organisation exists.
- Law enforcement should use available communication platforms including social media to highlight the latest threats and scams to the general public. This will not only enable the quick dissemination of information but also interaction with the public, and has the potential to strengthen community relations.

104 [Ipsos MORI, A survey of public attitudes to internet security, 2013](#)

105 Smith, Russel G., Grabosky, Peter, Urbas, Gregor, Cyber criminals on trial, 2014

106 [Clayton, R., Mansfield, T., A study of Whois Privacy and Proxy Service Abuse, 2014](#)

107 [APWG, Global Phishing Survey: Trends and Domain Name Use in 2H2013, 2014](#)

108 [University of Reading: Turing Test success marks milestone in computing history, 2014](#)

109 [Trend Micro: Africa – A new Safe Harbor for Criminals?, 2013](#)

110 [Symantec: Internet Security Threat Report, 2013](#)

111 [Levi, M. and Williams, M., eCrime Reduction Partnership Mapping Study, 2012](#)

3.7 Data breaches and network intrusions

Overview

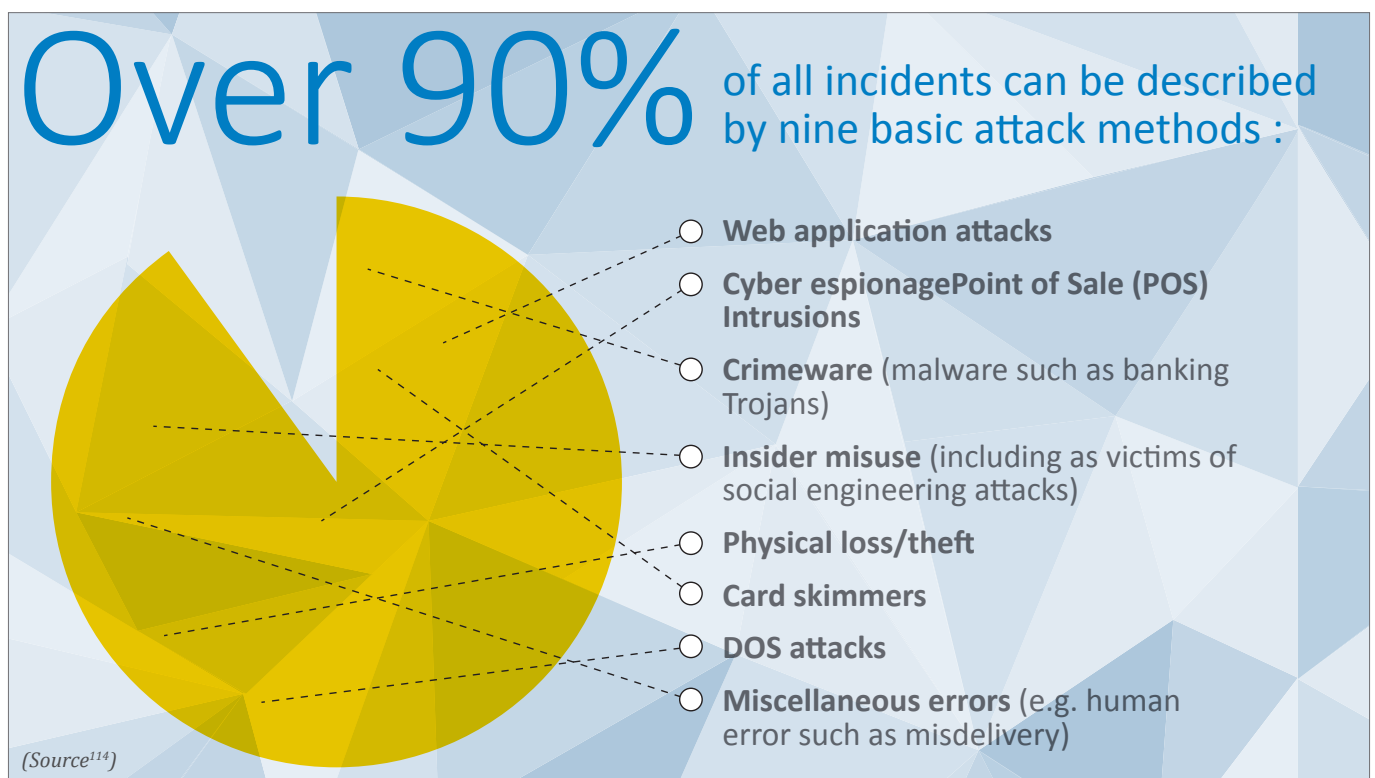
Any sector will hold data of value or interest to another entity, whether that entity is a financially or politically motivated cybercriminal, a competitor or foreign state. Furthermore almost any type data has worth, from card data to medical records to intellectual property. As a consequence all sectors are affected by data breaches and network intrusions¹¹². Although the motivation for most data thefts is largely financial gain, the proportion of attacks for the purpose of espionage is steadily increasing¹¹³. Not every attack revolves around data theft however; attacks can also be for the purpose of extortion, protest (hacktivism) or sabotage.

In 2013 web application attacks, cyber espionage and POS intrusions accounted for over 70% of all breaches - a breach being defined as an incident where data either was, or was potentially, lost. The costs of a breach are estimated to be up to USD 200 per record, with malicious attacks being the most costly¹¹⁵.

Of all the sectors seeing victims of data breaches, the financial sector was most heavily hit, followed by the public sector, retail, the accommodation sector and utilities. Those sectors which are heavily regulated (healthcare, education, financial, etc) also have the highest costs per capita from a breach¹¹⁶.

The scale of these breaches can be immense. In December 2013, an attack on US retail company Target resulted in the exfiltration of details of up to 70 million customers and 40 million credit cards. In February 2014 a breach at eBay resulted in the disclosure of 145 million customer details as a result of a hacking attack¹¹⁶. The data lost included customer names, email addresses, physical addresses and phone numbers. The breach represented one of the largest breaches to date.

Many intrusions are executed as what is termed an *Advanced Persistent Threat (APT)*. These are multi-stage attacks which take place over an extended period. In 2013 the average period of time an attacker remained undetected on a compromise network was 229 days¹¹⁸. Such attacks typically begin with the attacker attempting



112 [Verizon 2014 Data Breach Investigations Report](#)

113 [Verizon 2014 Data Breach Investigations Report](#)

114 [Verizon 2014 Data Breach Investigations Report](#)

115 [Ponemon Institute, 2014 Cost of Data Breach Study: Global Analysis](#)

116 [Ponemon Institute, 2014 Cost of Data Breach Study: Global Analysis](#)

117 [Reuters: eBay asks 145 million users to change passwords after cyber attack](#)

118 [Trends: Beyond the Breach, Mandiant 2014 Threat Report](#)



to identify vulnerable entry points. The actual incursion will generally use one or a combination of methods from social engineering, malware attacks and hacking. Once 'inside' the attackers will map the compromised network, deploy additional malware to facilitate further access and capture information and valuable data. The final stage is to exfiltrate the captured data to be used for whichever criminal purposes it can be exploited.

Once exfiltration occurs the likelihood of discovery significantly increases although as little as one third of compromises are discovered by the target company themselves¹¹⁹ with many disclosures being discovered by LE or third party threat researchers¹²⁰.

The increasing proportion of these attacks which relate to some form of hacking or malware can be attributed to the increasing availability of crimeware kits and hacking services available on the digital underground¹²¹ and the extent to which attacks can now be automated. Social engineering techniques typically consist of *spear phishing* or *watering hole* attacks^{122, 123}.

In 2013 over 50% of attacks targeted the USA. Almost half of these attacks nominally originate from Eastern Asia, with a further fifth originating from Eastern Europe. State-affiliated attacks are believed to account for almost 90% of all attacks, while organised crime is believed to be responsible for just over 10%¹²⁴.

EU Member States investigated a number of data breaches and network intrusions. Notably there were a number of attacks on critical infrastructure - with telecommunications companies being a common target. Other instances involved breaches into private industry and government sectors and were primarily motivated by financial gain, although cases of hacktivism and intellectual property theft are also occurring.

Facilitators and relevant factors

Many industries outsource parts of their business to third parties which may not match their security standards. Attackers will always target the weakest link and therefore corporate entities may be vulnerable via their third party suppliers.

The digital underground provides a variety of products and services which can facilitate network intrusion ranging from crimeware kits and customised malware to hacker-for-hire services. The proliferation of these services opens up the possibility to carry out attacks of this nature to any customers who otherwise lack the expertise or knowledge to initiate an attack unaided.

In March 2014, the European Parliament approved an amended version of the Network and Information Security (NIS) Directive. The directive originally included a requirement for a variety of Internet facing entities including e-commerce platforms, social networks and search engines to report to competent authorities any incident with impact on their core services - such as a data breach. However the amendment excluded these entities and limited the scope to companies providing critical infrastructure and supporting industries.

119 [Trends: Beyond the Breach, Mandiant 2014 Threat Report](#)

120 [Verizon 2014 Data Breach Investigations Report](#)

121 [Verizon 2014 Data Breach Investigations Report](#)

122 [Verizon 2014 Data Breach Investigations Report](#)

123 [Symantec Targeted Attacks against the Energy Sector](#)

124 [Verizon 2014 Data Breach Investigations Report](#)



Law enforcement considerations

Compounding the issues of attribution and jurisdiction, data breaches are often simply not reported or referred to LE. The exception to this is likely to be cases where there has been a significant and publicised disclosure of public information.

In cases where only company data or intellectual property has been disclosed, companies will often either manage the situation in-house, or use the services of an Internet security company specialising in investigating data breaches - expertise that LE often lacks. The reluctance to report to LE is likely to be as a result of a perceived lack of confidence in LE's ability to investigate discreetly, increasing the risk of a reputation-damaging leak to the media.

Future threats and developments

As high value targets begin to improve their IT security measures, we can expect more targeted attacks on third party suppliers. Not only is their own data vulnerable but they can be compromised as a stepping stone to an ulterior attack on a larger corporation to whom they are a trusted source - a method known as 'Island Hopping'¹²⁵. Moreover, with the widespread adoption of *Big Data*, more companies will act as data brokers by amassing large amounts of data. Given the potential value and multi-purpose use of this data, we can also expect to see more targeted attacks on data brokers, mainly for economic reasons but also for politically motivated attacks¹²⁶.

With the expanding availability of criminal services on the digital underground we can expect a proliferation of untargeted and unsophisticated security incidents. At the opposite end of the scale we can also expect more hackers-

for-hire such as *Hidden Lynx* and the *Comment Crew* to emerge as the professionalism and business model of the digital underground continues to evolve - contracted by clients to steal or sabotage as required.

In addition to the number of attacks rising, as companies become more aware of the threats and become better at detecting or identifying indicators of an intrusion we can expect the number of reported incidents to increase.

Recommendations

- If law enforcement is to successfully investigate these attacks, it must invest in the appropriate training, particularly forensic expertise, and capability to do so. Developing a more professional capability to act in this area will also increase the confidence of industry partners.
- To redress the lack of reporting in this area law enforcement should seek to build trusting relationships with industry to encourage reporting of sensitive crimes with the confidence that they will be investigated tactfully and discretely. This should include information on failed attacks which will still add to the intelligence picture.
- Industry standards already exist for the storage and transmission of payment card data (PCI DSS). For other data however there is no such industry standard. The implementation of such standards within and across industry would act to protect consumer, client and customer data. Companies offering greater levels of security may also gain a competitive edge.

3.8 Vulnerabilities of critical infrastructure

Overview

As EC3 is not directly mandated to assess the vulnerabilities of critical infrastructure, it is not a core competency of Europol. However, since it is an area that can directly impact upon the work of EC3's three Focal Points, it is considered important to provide an overview of these vulnerabilities as well as relevant developments and potential new attack vectors for cybercrime.

¹²⁵ [Trend Micro: FBI Details Major Trends in Cyber Attacks against SMB's](#)

¹²⁶ [FTC: Data Brokers – A Call for Transparency and Accountability. 2014.](#)



Critical infrastructure refers to physical and virtual assets or systems, which if disrupted or destroyed would have a significant impact on safety, security, public health, the economy or social well-being of people¹²⁷. European Critical Infrastructures (ECI) are defined as critical infrastructures located in Member States (MS), the disruption or destruction of which would have a significant impact on at least two Member States, or a single MS if the critical infrastructure is located in another Member State¹²⁸.

Some important additional aspects of critical infrastructure are cross-sector dependencies and cascade effects which means that an outage in one critical infrastructure sector may have an impact on other sectors. This is particularly true for the energy sector as it supports other critical infrastructures such as transport, health and ICT.

A large part of critical infrastructure, including energy, water treatment or transport, is controlled, monitored and operated by Industrial Control Systems (ICS)/Supervisory Control and Data Acquisition (SCADA) systems as well as Automatic Identification System (AIS) tracking systems.

These systems, which used to only be accessible internally, have gradually become more accessible remotely via the Internet. While increased interconnection, integration, remote-control and the use of open software standards and protocols¹²⁹ make critical infrastructure easier to operate, they also make them more vulnerable to cyber-attacks, for instance by compromising wireless access points or by distributing infected USB keys around facilities. Consequently, cyber threats are becoming a core challenge for the operators of critical infrastructure because, especially with cascade effects, a well co-ordinated cyber-attack could cause far more damage than

a physical attack. The challenge is further compounded by the fact that a number of these monitoring and control systems are poorly protected as most of these systems were designed at a time when Internet connection was not envisaged^{130, 131} or they run on software that has reached end-of-life such as Windows XP¹³². Moreover, the use of open standards may provide additional risks as it is easier for criminals to identify potential vulnerabilities. However, this must be counter-balanced against the time it may take to detect and patch vulnerabilities in proprietary software. The risk of a remote, malicious attack became apparent when Stuxnet¹³³ was used to target control systems for nuclear centrifuges. The possibility of such cyber-attacks poses an increasing threat to EU critical infrastructure¹³⁴. According to a recent study among critical infrastructure operators, specialists and vendors, the overwhelming majority of respondents believe it is not a matter of if – but when – there will be a cyber-attack of major significance and impact on critical operational infrastructure¹³⁵.

With the Internet of Everything we see new forms of critical infrastructure emerging, for instance in the form of smart grids, smart cars, smart homes or smart cities. An area of concern, for example, is the growing use of smart metering and smart grids that enable utility companies to measure energy consumption more accurately. These smart meters can be manipulated to send false information or report incorrect billing identities, resulting in substantial economic damage¹³⁶. The necessary tools are readily available on the Internet. They may also be used as an attack vector on the

¹²⁷ [Directive on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection \(2008/114/EC\)](#)

¹²⁸ [Communication from the Commission on a Programme for Critical Infrastructure Protection, 2006](#)

¹²⁹ Journal of Energy Security - Critical Energy Infrastructure Protection: The Case of the Trans-ASEAN Energy Network

¹³⁰ [Trend Micro – Blurring Boundaries, Trend Micro Security Predictions for 2014 and beyond](#)

¹³¹ [Reuters - All at sea: global shipping fleet exposed to hacking threat, April 2014](#)

¹³² Threat update – cyber-crime – Jan-May 2014

¹³³ [Trend Micro – Threat Encyclopedia: Stuxnet Malware targeting SCADA Systems](#)

¹³⁴ [Trend Micro – Cybercrime hits the unexpected. Bitcoin – and PoS-System-Related Attacks Trouble Users, 2014](#)

¹³⁵ [Tripwire – the state of security - Attacks Shift from Data Breaches to Targeting of Critical Infrastructure, 2014](#)

¹³⁶ [Krebs on Security: FBI - Updates Over Public 'Net Access = Bad Idea, 2012](#)

operator of the critical infrastructure since these devices are connected with the utility company in some ways. Moreover, the cycle to update or change smart devices can be costly and time-consuming.

The potential impact of organised crime as well as state-sponsored or cyber-attack by terrorist or extremist groups in this area is significant. Any cybercrime approach can be used by other actors as well. The key message is that while the motivations among the various actors in cyberspace differ, the methods employed are, to a large degree, very similar and often they are the same^{137, 138}.

Law enforcement considerations

Threats against critical infrastructures are often investigated by agencies that may not be pooling data with law enforcement. While there are recommendations and guidelines for Member States on how to protect critical infrastructure¹³⁹, little has been developed about the role of cybercrime or with LE in mind. While LE may be involved in the post-incident investigation of attacks against critical infrastructure, they are typically not involved in the sharing of information or intelligence that could be relevant in mitigating or preventing such an attack. However, as LE may have a more complete overview of the cyber threat landscape and the tools and methods used by cyber criminals, they can play an important role in the protection of critical infrastructure, for instance through sharing best practices and raising (public) awareness¹⁴⁰. In fact, LE involvement is seen as essential as a significant number of major cyber incidents in this area are caused by criminal activity¹⁴¹.

Another reason for LE to engage in public-private partnerships is the fact that most of the critical infrastructure is owned by the private sector.

Future threats and developments

Given the increasing trend of interconnecting, integrating and remote-controlling critical infrastructures, we expect cyber-attacks on these systems to remain a serious challenge for operators. The dual use aspect and availability of cybercrime facilitators, including zero-day

exploits for ICS/SCADA systems^{142, 143} combined with the relative ease to locate critical infrastructure devices¹⁴⁴, will continue to attract actors with different motives.

With the Internet of Everything expanding and becoming more widely adopted, new forms of critical infrastructure will appear and dependencies on existing ones will become more critical. As public and private sector organisations are outsourcing data, applications, platforms and entire infrastructures to large cloud service providers, cloud computing itself will become a critical infrastructure¹⁴⁵.

Also, some countries have started to open the energy market for smaller private contributors which allows mini power plants like water, wind or photovoltaic sites to feed energy back into the power grid. This may lead to more vulnerabilities as these smaller operators often do not have the resources to implement adequate security measures.

All this provides for new attack vectors and an increased attack surface and, consequently, we are likely to see more targeted attacks on these emerging infrastructures as well. As mentioned before, this will be exacerbated by smart devices that are no longer supported or are not being updated, or that are so small that they do not have security built into them or were simply not designed with security in mind.

We can expect to see an increase in DDoS attacks with the aim of disrupting critical infrastructure and/or for extortion purposes. Moreover, cybercriminals will continue to use malware and ransomware to mainly target user-facing devices of critical infrastructure.

Recommendations

- 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.
- Law enforcement should explore a more active role in public-private partnerships aiming at the protection of critical infrastructure and incident reporting¹⁴⁶, in partnership with Europol and the EC3.

137 [Ars Technica: Attackers poison legitimate apps to infect sensitive industrial control systems, 2014](#)

138 [F-Secure: Havex Hunts for ICS/SCADA Systems, 2014](#)

139 [ENISA - Protecting Industrial Control Systems - Recommendations for Europe and Member, 2011](#)

140 [INTERPOL: FBI-INTERPOL symposium to enhance global preparedness in securing critical infrastructure, 2014](#)

141 EUCTF letter to the Council of the European Union, dated 24 April 2014

142 [Threat Post: SCADA, ICS Bug, 2013](#)

143 [Dark Reading: SCADA Researcher Drops Zero-Day, ICS-CERT Issues Advisory, 2014](#)

144 [Threat Post: Shodan Search Engine Project, 2013](#)

145 [ENISA: Critical Cloud Computing, 2013](#)

146 [ENISA: Public Private Partnerships](#)



EUROPEAN CYBERCRIME CENTRE
ECC
EUROPOL

The Internet Organised Crime Threat Assessment (iOCTA)

CHAPTER 4 FACILITATORS AND RELEVANT FACTORS

4.1 Social networking

The proliferation of the Internet has brought about an unprecedented level of global social connectivity. The average Internet user spends 16 hours per month¹⁴⁷ online and 27% of that time is spent on social networking¹⁴⁸. 2014 marks the 10 year anniversary of Facebook, the world's largest social networking site. Following its success the last decade has seen an explosive growth in social media platforms. Facebook alone has grown in size from 1 million users in its first year to over 1.15 *billion* today; 71% of online adults have Facebook accounts¹⁴⁹. Globally there are currently estimated to be almost 2 billion social network users, with over 310 million users within the EU¹⁵⁰.

Not only is the Internet becoming part of our daily lives, but our private and professional lives are increasingly becoming part of the open and accessible content of the Internet. Every *Tweet*, *Like*, *Status Update*, *Tag*, *Pin*, *Comment*, *+Friend* or *Share* increases our ever-expanding Internet footprint.

Attackers exploit the prolific sharing and posting of media on these websites. The combination of the viral nature of media sharing and the huge target audience makes social networking platforms a perfect resource for cyber criminals for the distribution and propagation of malicious content.

Criminal exploitation

Attacks via social media sites can take many forms. Despite the efforts of the providers, social networking sites are becoming an increasingly popular mechanism for distributing malware. Most attacks rely on victims clicking

on malicious links or performing some other action which subsequently infects their device. These attacks typically also 'Like' or 'Share' the malicious content from the victim's profile, resulting in the victims' contacts further infecting themselves after viewing content they believed to be from a trusted source. In such a way the attacks propagate virally through the social media network¹⁵¹. Effectively, social networking sites are taking over from traditional spam.

Social media is also a perfect environment for attackers to employ social engineering tactics. By design, social platforms encourage users to share and disclose information. Attackers need only provide suitable incentives to potential victims for them to disclose private information or lure them to a malicious URL.

Social networking accounts also provide criminals with the materials they need for identity theft. Attackers can create accounts duplicating their victim, likely replicating media and data the victims have published themselves on their genuine accounts. These doppelganger accounts can then be used for further social engineering attacks on the victim's contacts, exploiting their trusted relationships. Alternatively, compromised social networking accounts are a valuable commodity in the underground digital economy. In early 2012, the number of phishing sites targeting social networking sites briefly surpassed those targeting financial institutions¹⁵². Stolen and hacked accounts are a commonly reported problem for many law enforcement agencies. Consumer data is a valuable commodity. The mining of personal data by private companies is a growing trend in addition to its exploitation by criminals.

¹⁴⁷ [Media Bistro: All Twitter](#)

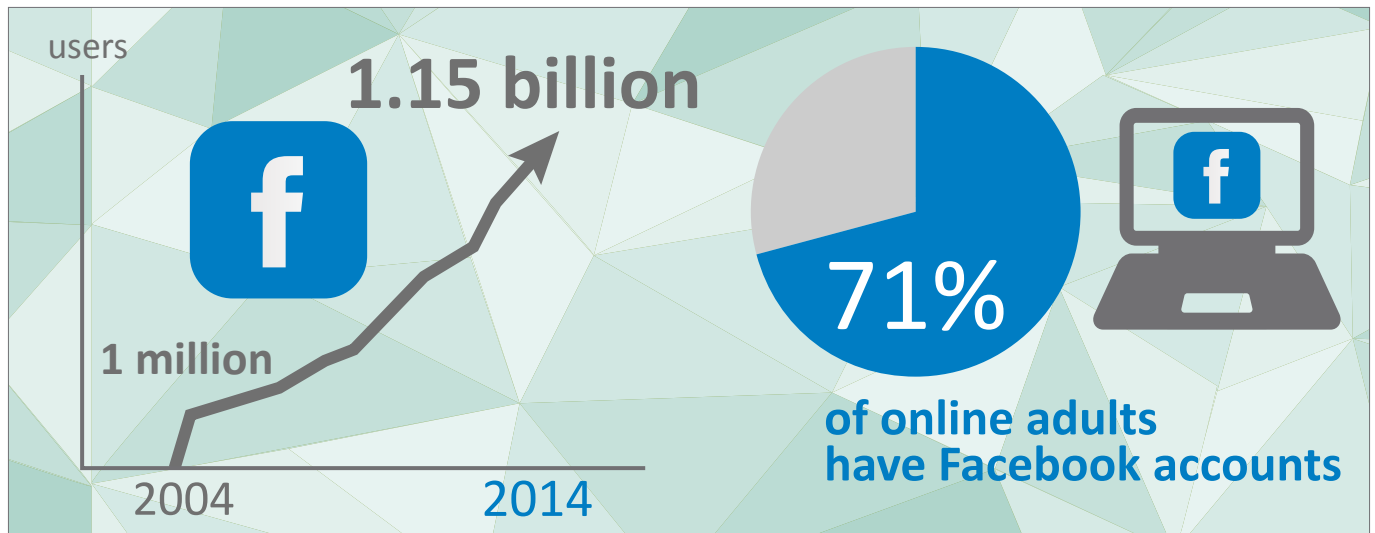
¹⁴⁸ [Media Bistro: All Twitter](#)

¹⁴⁹ [Media Bistro: All Twitter](#)

¹⁵⁰ [eMarketer: Social Networking Reaches Nearly One in Four Around the World, 2013](#)

¹⁵¹ [Sophos: Social Networking Security Threats](#)

¹⁵² [Microsoft Security Intelligence Report Vol 13, H1 2012](#)



2013 saw data breaches in many of the major providers including Facebook, Twitter, LinkedIn, Last.fm, eHarmony and Living Social, collectively representing the compromise of almost 65 million users' credentials.

Predictably, criminals also use social networking platforms to communicate with associates and recruit new members, although this is more common with criminals involved in more traditional crime.

Facilitators and relevant factors

The notion of privacy in cyberspace is somehow different to that in the off-line world. Users will disclose their private lives and personal details online without a comprehensive awareness of exactly who they are sharing their information with, whether it is the platform owner, a private company or the general public.

This leaves consumers extremely vulnerable to compromise from targeted attacks from social engineering and spear phishing and subsequently further fraud. This threat is exacerbated by the current trend in Single Sign On (SSO), whereby users can log into other services using their social media accounts. The compromise of a single account can therefore lead to the compromise of multiple linked accounts.

Law enforcement considerations

Social media is a valuable tool for law enforcement to identify, locate and gather intelligence on suspects¹⁵³. Many social media providers proactively share data,

particularly in cases of child abuse, and in many instances work closely with law enforcement.

In the wake of Edward Snowden's revelations regarding private companies sharing data with law enforcement and security agencies, industry has increasingly distanced itself from government to win back the trust of their customers. In May 2014, Apple Inc. announced that it would disclose to its customers when they had been the subject of a data request from law enforcement. This poses considerable problems for law enforcement as it may potentially compromise investigations, put victims and witnesses in danger and result in suspects destroying evidence or absconding. It is expected that other major Internet players such as Facebook, Google and Microsoft will follow suit¹⁵⁴ triggering a cascade of similar policies throughout the industry. In the future, interaction with such entities will have to be carefully risk assessed.



153 [Lexis Nexis: Social Media Use in Law Enforcement Investigations, 2012.](#)

154 [The Register: Apple - We'll tell users when the Feds come looking for their data, 2014](#)



Future threats and developments

As Internet adoption rates increase and social media access expands as a result, we will see more attacks targeting social networks and their inhabitants. As more consumers progressively favour social media as a means of communication over email, we can expect to see social media increasingly being used to deploy and propagate malware and scams instead of traditional spam¹⁵⁵.

Still, consumers will likely continue to share increasing amounts of personal data either privately with industry or openly on social networking platforms, making themselves increasingly at risk of compromise. The Internet of Everything and wearable technologies can only expand the opportunities for consumers to broadcast their lives virtually.

Recommendations

- Law enforcement should be keenly aware of the disclosure policies of any company they maintain a relationship with. Should such a company adopt a full disclosure policy with regards to data requests in relation to their customers, then law enforcement should fully risk assess the impact of any subsequent approach to that company. It may be that such information can only be obtained post-arrest without jeopardising the investigation.
- All sectors use the Internet and social media to build their reputation and Internet profile. Law enforcement should likewise take full advantage of social media platforms to enhance its Internet presence, spread crime prevention messages and engage with the Internet community.

4.2 Anonymisation tools

Overview

Anonymisation tools are widely used by many Internet users for a range of purposes; some have a simple desire for privacy, others require anonymity to avoid detection, persecution or prosecution.

There are many methods to hide or obscure one's origin or identity on the Internet. In terms of tools and technologies specifically designed for anonymity, although diverse in how they may ultimately function, these tools can be roughly grouped into three classes: (simple) proxies, virtual private networks (VPNs) and *Darknets*.

Darknets are networks which operate within the *Deep Web*¹⁵⁶. The first Darknet - The Onion Router (more commonly referred to as TOR) - was invented in 1995 by the US Navy for the purpose of protecting US government communication. Now publicly available, today TOR is one of the most widely used and well known anonymisation tools. These services also offer additional functionality using the same architecture such as secure messenger software (e.g. Torchat).

Although the most heavily adopted, TOR is only one of several Darknet services. Freenet and the Invisible Internet Project (I2P) are also popular and offer similar anonymisation opportunities, although they operate using alternative protocols.

In addition to the anonymisation of communications, Darknets also offer the possibility to anonymise content, such as the *Hidden Services* discussed in chapter 3.1. Darknets are also increasingly being used to host botnet

155 [Symantec Internet Security Threat Report 2013](#)

156 The portion of the Internet not indexed by traditional search engines.

Command and Control infrastructure¹⁵⁷. The use of Darknet in such a way makes it difficult for LE to locate and seize the servers.

The use of anonymisation tools is ubiquitous amongst the cyber underground. VPNs followed by TOR are the most commonly encountered form of anonymisation used by cybercriminals. The use of simple (one layer) proxies would appear to be in decline, with only a handful of jurisdictions reporting their use. In some cases suspects will stack several levels of anonymisation using multiple VPNs, proxies *and* TOR for maximum security at the expense of performance.

The use of encryption is also becoming increasingly commonplace. Encryption is commonly used in secure communications including applications such as PGP, VOIP, TOR and VPNs and is becoming a standard protection feature in many products, such as e-wallets for virtual currencies. Both the public and industry are also increasingly using encryption to protect their digital assets in the event of a cyber attack. However, in addition to weaponising encryption in the form of cryptoware, cybercriminals are increasingly using encryption to protect their data, thereby frustrating forensic analysis and evidence gathering from seized media by law enforcement.

Law enforcement considerations

The use of Darknets poses additional challenges for law enforcement. However, users and services on these networks are *not* untraceable and can still be identified via technical investigation or traditional investigative techniques (target profiling).

Blocking access to TOR on a national level is already a reality in China but has also been proposed in the Russian Federation. It is unlikely however that such restrictive censorship measures would ever be implemented within the EU, but it is possible that some other countries with strict censorship may follow suit.

Future threats and developments

Media attention and the resulting increased perception of the threat from hidden services has prompted a law enforcement response which has resulted in several high profile operational successes.

The current Darknets are popular and growing; they have communities which continue to support and develop them. These platforms will only continue to improve upon the security and anonymity they can provide to users. It is

also inevitable that new anonymisation technologies will develop on their foundations, such as the developing peer-to-peer (P2P) anonymisation services, which offer greater security and pose further challenges to law enforcement.

Recommendations

- Issues with attribution due to anonymisation may be partly mitigated by the sharing of operational intelligence between Member States and Europol (EC3). This should be an essential step in target profiling in all cases as a matter of routine.
- Law enforcement should share best practice in investigations involving Darknet and other anonymisation services including investigative and forensic techniques.
- Law enforcement should build technical capabilities in order to support technical investigations into subjects using Darknets, in accordance with relevant legislation.

4.3 Internet governance

Overview

Internet governance, defined as the development and regulation of the Internet through shared principles, norms and programs, is a continuous and complex process. The Internet is governed in what is called a 'bottom up multi-stakeholder model' rather than a purely intergovernmental approach. This multi-stakeholder approach has allowed the Internet to flourish, helping innovation and making the Internet as we know it today. However this approach has brought with it very real challenges for law enforcement.

IPv4 to IPv6

The number of available IPv4 addresses is rapidly diminishing. Migration to the IPv6 protocol – which offers a virtually unlimited number of IP addresses – is in progress but likely to take a considerable amount of time to implement. This means that, during this transition period – which may last several years or more – alternative ways to assign IP addresses are deployed by operators in order to ensure the continuity of Internet traffic in a growing market. The intermediate solution known as a 'Carrier Grade Network Address Translation Gateway' (CGNAT), is now being used by Internet service operators in the EU.

The ability to link users to an IP address is crucial in the context of a criminal investigation. Where the CGNAT is used, multiple devices are connected on a local network with only one single IP address. Potentially, this technology

157 [G Data: Botnet Command Server Hidden in Tor, 2012](#)



enables providers to link thousands of users per IPv4 address and the ability to identify individual users is therefore significantly impaired. The identification of users would require the retention of this data and its provision to LE by Internet operators.

Criminal exploitation

The role of the Domain Name System (DNS) in translating domain names into IP addresses can be exploited by criminals in various ways:

- DNS hijacking – used by hackers to redirect or 'hijack' the DNS addresses to bogus DNS servers for the purpose of injecting malware into a user's PC, promoting phishing scams, advertising on high traffic websites, and any other related form of criminal activity.
- Fast flux – a DNS technique used by botnets to hide phishing and malware delivery sites behind an ever-changing network of compromised hosts acting as proxies. In this scheme the DNS records change frequently, often every few minutes, to point to new bots, giving the botnet a robust hosting infrastructure.
- Cybersquatting – the crime of exploiting famous trademarks by registering similar domain names. The increase of the range of generic Top-Level Domains (gTLDs) and of the Domain Name Tasting¹⁵⁸ facilitates criminals who have more chances to create bad-faith domain names infringing copyright laws, and then reselling them to the legitimate trademark owner.

Transmission Control Protocol/Internet Protocol (TCP/IP) is the protocol ruling Internet traffic and can also be abused by cybercriminals in attacks such as Denial of

Service (DoS) attacks via SYN flooding, TCP sequence number prediction to generate counterfeit packets in a TCP connection and access the target host using a normal TCP/IP connection, or TCP session hijacking - the exploitation of a valid computer session to gain unauthorised access to information or services in a computer system.

IP addresses, Internet Protocols (IPs)

IP protocols present similar vulnerabilities, even though the IPv6 was conceived to replace the fourth version in a safer way by using Internet Protocol Security (IPsec) technology. Both IPs can be affected by four additional threats¹⁵⁹, briefly summarised below:

- Sniffing of sensitive information, where criminals are capturing network traffic between e.g. a user and a website by exploiting technical weaknesses of how IPv4 and IPv6 communicate with each other.
- An application layer attack is a form of Denial-of-Service attack, in which the attacker disables specific functions or features as opposed to an entire network. It is often used against financial institutions for specific targeted purposes. This type of attack can be used to disrupt transactions and access to databases by looking like legitimate traffic on the network.
- Rogue devices such as routers, which use IPv6 auto-configuration to assign IPv6 addresses to all the other devices on the network without the user's awareness. Traffic can be diverted to the rogue router which can then copy the detailed information, delete it or be used in man-in-the-middle attacks.
- Man-in-the-middle attacks, in which the criminal makes two parties believe they are talking to each

158 The practice of temporarily registering a domain under ICANN.

159 S. Convey and D. Miller (2004), *IPv6 and IPv4 Threat Comparison and Best-Practice Evaluation (v1.0)*, Cisco

other over a private connection while all traffic is actually controlled by the criminal, are enabled by IP and DHCP-spoofing. DHCP uses a broadcast message from the client when it initially boots up, allowing a rogue DHCP server to attempt to respond to the host before the valid DHCP server is able to. This allows the rogue server to set critical connectivity settings, including default gateway and DNS server, thus enabling man-in-the-middle attacks.

The Domain Name System WHOIS lookup allows users to lookup any generic domain, such as .com .org to find out the registered domain owner. Criminals can misuse/abuse WHOIS data in a number of ways:

- Improper use of others' WHOIS data: use of publicly accessible personal data to spam, to harm (malware delivery) or to harass individuals;
- Giving false WHOIS credentials to Registrars to avoid identification, in order to conduct illegal or harmful Internet activities (hosting child abuse sexual images, advanced fee fraud, online sale of counterfeit pharmaceuticals);
- Using of the private domain registration (domain names registered via privacy or proxy services or offshore) to obscure the perpetrator's identity.

Law enforcement considerations

EC3 has a thematic project aimed at researching these governance arrangements and architecture of the Internet, which identifies significant vulnerabilities exploited by organised crime groups (OCG) and identifies opportunities to affect and influence current and future developments of the Internet. EC3 works closely with the Internet Corporation for Assigned Names and Numbers (ICANN), Réseaux IP Européens Network Coordination Centre (RIPE NCC) and other Internet stakeholders who can influence and advise on Internet governance. The project aims to achieve real impact on the significant Internet governance bodies through ongoing law enforcement representation in this multi-stakeholder process.

The abundance of IPv6 addresses has both benefits and disadvantages for law enforcement. The re-use of IPv4 addresses resulted in attribution problems for law enforcement. This will not be an issue under IPv6 as there are enough IPv6 addresses for every person on the planet to be assigned trillions of addresses each. However, this will also give rise to occurrences of criminals using addresses for a single session or communication and then discarding them for a fresh one, which may complicate investigations considerably.

Future threats and developments

The current WHOIS system may be replaced by a new enhanced WHOIS called – Web Extensible Internet Registration Data Service (WEIRDS). It produces a simple, easy-to-implement protocol, supporting internationalised registration data and, specifically for name registries, capturing the needs of internationalised domain names in the data model. It has also been conceived to provide security services that do not exist in the current WHOIS protocol, including authentication, authorisation, availability, data confidentiality, and data integrity.

Recommendations

- International law enforcement needs to align its engagement with ISPs to provide the collective overview required to effect policies, particularly regarding access to IP addresses, domain names, registration of data and removal of registered ISPs involved in criminal activity.
- This overview will allow law enforcement to be involved in a bottom-up multi-stakeholder model, which will:
 - Enhance and further develop strategic relationships with the Internet community and all necessary stakeholders involved in Internet governance;
 - Raise the issues and concerns of law enforcement within the Internet governance process to respective governments;
 - Improve law enforcement knowledge and skills through collaborative training and operational exposure to common problems;
 - Result in an agreed set of requirements which all agencies will work towards;
 - Maximise the number of governance forums, in which the law enforcement perspective can be promoted.
- 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.
- Law enforcement needs to increase its knowledge of the architecture and governance structure of the Internet, and engage with the Internet governance community and other influential governance and commercial bodies to better understand the Internet governance landscape.



4.4 The future is already here

4.4.1 Big Data

Overview

The umbrella term Big Data has been used to describe very large data sets that are difficult to filter, analyse and interpret using standard database management tools or traditional data processing applications.

The driving factors behind Big Data¹⁶⁰ are not just technology and the wide-spread adoption of the Internet but also large-scale projects to digitise information that was previously not available in electronic format¹⁶¹ as well as *datafication*, i.e. the gathering of data about everything, including people, objects and locations. The concept of datafication is closely linked to the *Internet of Everything*, which is characterised by a steadily growing number of devices, sensors and actuators connected to the Internet. An example of datafication is the *Quantified Self* movement, which is a growing group of individuals who use wearable technology to constantly measure and share online data about their lives¹⁶².

Big Data is often collected as a by-product of people's actions, movements, contacts and social interactions. The term used to describe this is 'data exhaust'. From a cybercrime perspective these are electronic trails that criminals create as part of their online activities and interactions using electronic devices. These trails may often not be immediately visible but may be 'hidden' in the data in the form of relationships and correlations. For example, credit card companies use Big Data analysis to

identify potential credit card fraud. While in the past these companies could only monitor a small number of aspects of a transaction at once, they can now analyse several hundreds of aspects of a transaction at once and do so for a much larger set of data, which also means that credit card companies can now see patterns or anomalies that were not visible with smaller data sets¹⁶³. And since these credit card transactions happen in real time, the analysis needs to happen in real time too. A simpler example of interest to LE would be geolocation data that is often automatically included when taking a picture.

Big Data supports a different approach to gathering intelligence; one that is not necessarily targeted and hypothesis-based but focuses on gathering as much data from as many sources as possible. While an organisation may not be able to process all data yet, it can immediately investigate a case or criminal rather than having to start gathering the information from scratch.

Big Data supports a data-driven approach to identifying and exploiting patterns and correlations among the data collected, an approach known as *predictive analytics*. Predictive analytics reveals correlations – the *what* – but is usually not suitable to explain causality – the *why*. While there are many examples where correlation is good enough it is sometimes important to look for causal relationships, particularly when it comes to the investigation of crimes.

Criminal exploitation

Criminals already use basic Big Data analytical approaches to increase the value of stolen data. This is done, for instance, by splitting the stolen data into better-quality sets before selling them underground. Big Data analysis will be increasingly used by cybercriminals to maximise the monetary value of stolen data, which will lead to a more competitive cybercriminal market¹⁶⁴.

160 Mayer-Schönberger, V. and Cukier, K., (2013), "Big Data: A Revolution That Will Transform How We Live, Work, and Think", John Murray

161 [Google Books](#)

162 [Quantified Self: Self Knowledge through Numbers](#)

163 [Wall Street Journal: Visa uses Big Data to Combat Cybercrime, 2013](#)

164 [The Globe And Mail: As Hackers Feast on Stolen Data, Profiting from Fraud Gets Harder, 2014](#)

Big Data together with the Internet of Everything provides cyber criminals with new attack vectors and an increased attack surface.

Big Data allows for better profiling, which is used by criminals and LE alike, for instance to identify potential targets or to improve social engineering attacks.

Law enforcement considerations

An important application of Big Data in the area of law enforcement is *predictive policing* - the application of mainly quantitative analytical techniques to identify likely targets for intervention and to prevent crime, or solve past crimes by making statistical predictions¹⁶⁵. It is used by law enforcement, e.g. to predict future patterns of crime and identify vulnerable areas¹⁶⁶ as well as for opinion mining¹⁶⁷.

Predictive policing is seen as a method that allows LE to work more effectively and proactively with limited resources. The methods used fall into four general categories: predicting crimes, predicting offenders, predicting perpetrators' identities and predicting victims of crime.

While the concept of predictive policing is not new it is the large amount of data, the different sources of data and the speed at which this data can be analysed that offers new promises to LE in combating crime, including cybercrime, especially when combined with non-traditional crime data such as social media data to provide real-time access to intelligence. It allows LE to react faster and explore more leads.

As Big Data analysis is usually unsuitable to answer the question of causality, it may create more challenges for investigators to produce supporting evidence given the sheer amount of data that needs to be analysed. On the other hand, Big Data analysis can be used to point to the most promising areas for an investigation, i.e. where to find causal relationships. In order to do so, LE needs to be in a position to effectively and efficiently combine evidence from different sources and present it in a meaningful way.

There is however a risk of using Big Data incorrectly or excessively. It is therefore important for LE to use analytical tools carefully, proportionally and in line with relevant legislation and regulations.

Another area of Big Data that is already of relevance to LE and is expected to increase is the analysis of open-source information or open source intelligence (OSINT).

Future threats and developments

Big Data will become 'bigger' and 'faster' and become part of most decision processes. Big Data analysis will continue to be used, among other things, for data-driven security, for instance when looking for criminal patterns in real-time, or as part of the authentication process.

The volume and scope of *Fast Data* - data that is collected and analysed in real-time - will continue to increase, particularly in developing countries where (mobile) Internet access is on the rise. This will allow for novel ways of supporting decision processes in real time, early warning systems based on opinion mining, real-time awareness and real time feedback.

Big Data, together with the Internet of Everything, will expand existing and create new types of critical infrastructure. This in turn will create new privacy issues as these categories of data and their option value will offer new insights. For instance for smart homes this could be 'load signatures' that describe the power consumption of electrical devices that are unique to the appliance - this information can be used to determine when residents are not at home and provide insights into their daily behaviour and even illegal activities.

As more data is captured and cross-referenced, it will become harder to protect privacy and personal data as Big Data aids de-anonymisation - either through patterns and correlations that become visible in bigger data sets and/or the combination with other data sources. This will be further aided by readily available tools to perform OSINT analysis.

As the use of Big Data and predictive analytics will become the norm, the risk of equalling correlation with causality will increase. And so will the risk of using predictive analytics incorrectly.

Moreover, with the widespread adoption of Big Data, more companies will act as data broker by amassing large amounts of data, usually user related. Given the potential value and multi-purpose use of this data, we can expect to see more targeted attacks on data brokers, either to steal and sell the data, for ransom purposes, for political reasons or to actually use Big Data analytics to support more sophisticated attacks.

165 [Perry, W.; McInnis, B.; Price, C.; Smith, S. and Hollywood, J.; \(2013\). "Predictive Policing, the Role of forecasting in Law Enforcement Operations". Rand Corporation](#)

166 [HMIC - Policing in austerity: rising to the challenging compendium, 2014](#)

167 [Gov Lab - New Methods of Making Sense of Human Behavior, 2014](#)



Recommendations

- Law enforcement needs the necessary skills, expertise and tools to perform OSINT and Big Data analysis to identify relevant criminal patterns and collect crime-relevant data.
- As it will become increasingly harder to collect and analyse the ever increasing amount of electronic evidence, there is a need to develop and share guidance, procedures and best practices for law enforcement on how to conduct investigations involving Big Data.

4.4.2 Internet of Everything

Overview

While there is no generally accepted definition of the term the *Internet of Things* (IoT), it is characterised by a constantly growing network of connected devices and actuators that can sense or interact with their internal states or the external environment. Generally speaking, the Internet of Things creates the ability for physical objects, which were previously often unconnected and without computing power, and people to remotely interact through the Internet. One of the threats arising from this is that, whereas people often consciously log into computers and even smartphones, they may not be aware of how they are connected to the IoT environment.

The concept of the *Internet of Everything* (IoE) is understood as the next evolutionary stage of the Internet of Things. It is characterised by the convergence of people, processes, data, and objects with a view to combining communications between machines (M2M), between people and machines (P2M) and between people (P2P)

to deliver new or enhanced services, provide improved and broader contextual awareness, and allow for better informed and faster decisions¹⁶⁸.

The IoE is closely related to Big/Fast Data and Cloud Computing, as more sensors, location tracking and communication modules embedded in devices lead to much more data being collected from different sources and on a variety of aspects, including data that was previously not available or difficult to capture. Cloud Computing provides the dynamic, scalable and distributed infrastructure needed to support the storage and distributed processing of the data collected. Given the potentially very large number of connected devices and networks within networks¹⁶⁹, the large-scale implementation of IoE will also require IPv6 to be in place.

Facilitators and relevant factors

While the IoE is characterised by a variety of different software and hardware products and communication standards, we can expect to see a higher degree of homogeneity or standardisation¹⁷⁰ and the emergence of more monocultures, particularly as these concepts are more widely adopted. As a consequence, IoE runs the risk of *common-mode failures* or failures that result from a single fault. If such an exploitable common-mode failure is detected it will affect a potentially very large number of devices thereby creating a large number of potential victims¹⁷¹. Moreover, fixing vulnerabilities takes time, often years before everyone is safe¹⁷². Some examples are home and business routers that are rarely updated¹⁷³ or bugs in popular software products such

168 [Cisco – Internet of Everything](#)

169 [Gartner Newsroom](#) and [ABI Research](#)

170 [Electronic Design: The Internet Of Things Is A Standards Thing, 2014](#)

171 [Lawfare: Hartbleed as Metaphor, 2014](#)

172 [ZDNET: Conficker: Still spamming after all these years, 2014](#)

173 [Computer World: 'The Moon' worm infects Linksys routers, 2014](#)

as the Heartbleed bug¹⁷⁴ or vulnerabilities in popular content management systems¹⁷⁵.

For criminals, standardisation has a leveraging effect as it significantly increases the number of potential victims; while more devices, processes and people interacting via the Internet create a wider attack surface and more attack vectors. The latter will be exacerbated by devices that are no longer supported or are so small that they do not have security built into them¹⁷⁶ or were not designed with security in mind¹⁷⁷. Moreover, policy makers are often not part of the early phases either which may result in a lack of relevant legislation and regulation.

The concept is a driving factor behind new types of critical infrastructures such as smart cars, smart homes, smart grids¹⁷⁸ or smart cities¹⁷⁹, which create new types of risks and threats. For instance, the control area network (CAN) bus is a standardised protocol often used for internal communications between devices in a vehicle. Combined with GPS tracking and online communication and control technologies, this presents real risks for attacks, particularly since a vulnerability found in one manufacturer is likely to exist in others too¹⁸⁰. Attack vectors for smart homes include smart TVs that may run operating systems used also in smartphones – which are often vulnerable to many of the same attacks – smart meters or home automation devices, to mention only a few¹⁸¹.

Finally, the IoE plays a crucial role in Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) control systems as well as Automatic Identification System (AIS) tracking systems that are used in different types of critical infrastructure. These systems have vulnerabilities¹⁸², are often poorly protected¹⁸³ or run on software that has reached end-of-life (EOL) such as Windows XP¹⁸⁴.

174 [Heartbleed](#)

175 [The Hacker News: Disqus Wordpress Plugin Flaw Leaves Millions of Blogs Vulnerable to Hackers, 2014](#)

176 [BBC News – “The Internet of Things: the ‘ghosts’ that haunt the machine”, 2014](#)

177 [The Register: Miracast Passwords, Value Walk: Tesla’s door-locking security depends on a six-character password which is vulnerable to hacking](#) and [Trend Micro: Securing the Internet of Everything](#)

178 [Trend Micro: Threat Intelligence Resources - The Internet of Everything](#)

179 [Internet of Things Research, 2013](#)

180 [Gizmodo: How to Hack a Car and Control it from 1500 Miles Away](#) and [The Guardian – Internet of Things Security Dangers](#)

181 [IOActive: IOActive Lights Up Vulnerabilities for Over Half a Million Belkin WeMo Users, 2014](#)

182 [Trend Micro: Stuxnet Malware Targeting SCADA Systems](#)

183 [Trend Micro: Blurring Boundaries, Trend Micro Security Predictions for 2014 and beyond](#) and [Reuters: All at Sea: Global Shipping Fleet Exposed to Hacking Threat](#)

184 Threat update – cyber-crime – Jan-May 2014

Law enforcement considerations

The Internet of Everything presents specific investigative challenges for LE because of the number and diversity of hardware, software and communication protocols that LE needs to be able to examine, and in terms of identifying the devices and extracting the data that are of relevance to a particular case. More often than not this will require live data forensics as some or all of the relevant data may be located in the cloud, which will frequently require cross-border co-operation and legal assistance. With some of the smaller IoE devices, however, the amount of relevant data that can be extracted for investigative purposes may be minimal.

Furthermore, extracting, identifying and combining the relevant evidence will routinely become a Big Data problem, requiring LE to have the necessary skills available.

The increasing number and variety of devices is likely to result in a substantial increase in demand for LE forensics examination and investigation resources.

Finally, it can be expected that the IoE will further complicate the attribution of crimes, given the increased attack surface and large number of attack vectors.

Future threats and developments

While a killer app driving the main-stream adoption of the IoE may not be there yet¹⁸⁵, we can expect to see the concept rapidly expanding and being adopted, driven by market pressures, availability and broader acceptance.

Crucial aspects of the IoE are identity, identification, security, privacy and trust¹⁸⁶. For instance, facial and speech recognition features in smart devices will become more wide-spread and pose greater risks in terms of privacy and security, and so will wearable technology that can collect data¹⁸⁷. As mentioned under the section on Big Data, as more data is captured, aggregated and cross-referenced, it will become harder to protect privacy.

With more objects being connected to the Internet and the creation of new types of critical infrastructure, we can expect to see (more) targeted attacks on existing and emerging infrastructures, including new forms of blackmailing and extortion schemes (e.g. ransomware for smart cars or smart homes), data theft, physical injury and possible death¹⁸⁸, and new types of botnets.

185 [Trend Micro: Is the Internet of Everything under Attack?, 2014](#)

186 Contribution to the iOCTA 2014: J. Smith, Leiden University

187 [Wired: Google Glass Snoopers Can Steal Your Passcode with a Glance, 2014](#)

188 [Internet Identity: IID Finds Murder by Internet, NFC Exploits Emerge as Genuine Cybersecurity Threats in 2013](#)



As more (personal) data is being stored in the cloud, we can expect to see more attacks on cloud services with the goal to disrupt services for economic or political motives, to steal/access data – including ransomware - or to use the infrastructure for malicious purposes¹⁸⁹.

Recommendations

- The multi-faceted nature of the Internet of Everything (IoE) demands an equally diverse response by [law enforcement](#) and all other relevant stakeholders. Apart from the necessary skills, knowledge and expertise that [law enforcement](#) needs to investigate IoE-related crimes, co-operation and co-ordination together with public-private partnerships will play an increasingly important role. This could include, for instance, setting up repositories on how to collect, cross-reference and analyse data recovered from a range of devices in compliance with relevant privacy and data protection frameworks and rules.
- As the IoE is becoming more widely adopted, the amount and types of digital forensics resources required by [law enforcement](#) agencies need to adapt and grow accordingly.
- Industries involved in making the IoE a reality need to be encouraged to consider security as part of the design process¹⁹⁰.
- Last but not least, policy makers need to stay abreast of the latest developments in this area in order to ensure that effective, efficient and balanced legislation and regulations are in place.

189 [Security Affairs: PlugX RAT with Time Bomb abuses Dropbox in targeted attacks, 2014](#)

190 [Trend Micro: Securing the Internet of Everything, 2014](#)

4.4.3 Cloud computing and services

Overview

Cloud computing is defined as a model for ubiquitous on-demand network access to a shared pool of configurable resources such as data storage, applications and network infrastructure that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing provides a dynamic and scalable infrastructure to support the distributed storage and processing of data and the virtualisation of hardware and associated infrastructure. This results in what is called elasticity, entailing a frequent reconfiguration of resources.

Cloud computing offers different service models or *Cloud Services*, including Software-as-a-Service (SaaS) e.g. web-based e-mail, Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS) as well as other services that sit on top of these service models. Cloud computing together with Cloud Services form what is usually called the *Cloud*. There are different deployment models ranging from private to community to public Clouds as well as hybrid models that combine two or more of these deployment models.

The Cloud is an enabler for IoE and Big Data by providing the distributed and scalable resources needed to handle the data growth and provide the necessary processing services.

The Cloud represents a paradigm shift in the delivery of resources and services but also in terms of security and traceability. Developments such as bring-your-own-cloud (BYOC) to bring-your-own-everything (BYOX) add to these security challenges as employees not only introduce their own devices to the corporate environment but also their data, applications, etc, thereby essentially creating a 'shadow IT'¹⁹¹.

As cybercriminals recognise the business benefits and opportunities that the Cloud offers, their activities are migrating to the Cloud, often abusing legitimate services¹⁹². The Cloud is used to launch new attacks such as virtual machine-based malware (e.g. virtual machines infected by a preloaded rootkit or malware attempting to infect the hosting machine from within the virtual environment), control Botnets¹⁹³, and to store and distribute illegal material¹⁹⁴. Moreover, the Cloud is a valuable target for cybercriminals for stealing or mining personal or business

191 [McAfee – The hidden truth behind shadow IT, 2013](#)

192 [Trend Micro: Cybercriminals Continue to Migrate to the Cloud, 2014](#)

193 [Wired: How Hackers Hid a Money-Mining Botnet in the Clouds of Amazon and Others, 2014](#)

194 [Cloud Security Alliance: The Notorious Nine Cloud Computing Top Threats in 2013](#)

data. Indeed, it can be said that the Crime-as-a-Service (CaaS) model has already adopted the different Cloud service models by offering, e.g. infrastructure as a service or software as a service, for instance in the form of counter antivirus (AV) services or to launch DDoS attacks.

Law enforcement considerations

The Cloud presents both challenges and opportunities for law enforcement¹⁹⁵. The National Institute of Standards and Technology (NIST) report on Cloud Computing Forensic Science Challenges lists 65 technical challenges for forensic investigators in uncovering, gathering, examining and interpreting digital evidence in dynamically changing, elastic, on-demand and self-provisioning Cloud environments¹⁹⁶. The report clusters these technical challenges in nine categories, including data collection, analysis, legal, standards, training and anti-forensics to specifically prevent or mislead forensic analysis such as obfuscation, data hiding and malware. While these challenges are technical in nature, the report highlights that almost all touch upon legal and organisational aspects.

Data stored in the Cloud might be physically stored in different jurisdictions, which may pose obstacles to investigations particularly if the service provider is not based in the EU. Furthermore, the virtualisation of hardware and infrastructure means that potential electronic evidence will not only be geographically distributed but also become more volatile, resulting in technical and legal challenges for LE. This is exacerbated by limited knowledge and support for keeping records and potential evidence on the part of Cloud providers. The increased use of encryption in the Cloud is likely to further complicate digital investigations¹⁹⁷.

The use of Cloud computing and services necessitates the use of different digital forensics methods such as Live Data Forensics, which is performed on a running (live) system to acquire and/or analyse the data from that system for use in a court. This will put a greater burden of proof on LE as the actions performed during Live Data Forensics will change the data stored on the system. There is also the risk of using digital forensic tools and methods that are not applicable to cloud forensics¹⁹⁸.

Furthermore, LE investigative activities in the Cloud run the risk of disrupting legitimate services and businesses that use Cloud services, and may lead to potential data privacy issues.

Apart from these challenges, the Cloud also offers some opportunities for LE as the service provider can act as a single point of contact for digital investigations.

Future threats and developments

As more and more data is being collected and processed in real time, the demand for Cloud computing and services will only further increase. Developments such as BYOX and the expansion and further adoption of the Internet of Everything will further add to this.

This trend provides risks and creates threats as cybercriminals will start to increasingly attack and abuse Cloud services. In the context of Big Data, some Cloud providers will become large data holders, which will make them high-value targets.

As the public and private sectors continue to outsource data, applications, platforms and entire infrastructures to Cloud providers, the Cloud itself will become a critical infrastructure¹⁹⁹. Consequently, attacks or threats aiming at disrupting Cloud services will become increasingly common.

Recommendations

- Law enforcement should work with the relevant stakeholders, including the private sector, to promote more secure Cloud computing and services, using for instance strong encryption.
- Law enforcement requires the expertise, skills and tools to investigate Cloud-related cybercrimes. As this will regularly require Live Data Forensics, specific protocols and methodologies should be developed in this field, considering existing guidelines and best practices²⁰⁰. To the extent possible, law enforcement should consult with Cloud providers and relevant organisations on the development and implementation of digital investigation standards and protocols that are proportional, protect privacy and ensure business continuity.

¹⁹⁵ [ENISA – Security and Resilience in Governmental Clouds, 2011](#)

¹⁹⁶ [NIST - Digital Crime-Fighters Face Technical Challenges with Cloud Computing, 2014](#)

¹⁹⁷ [Trend Micro: Cloud Security Best Practices: Benefits of Cloud Encryption, 2014](#)

¹⁹⁸ [NIST: NIST Cloud Computing Forensic Science Challenges](#)

¹⁹⁹ [ENISA: Critical Cloud Computing, 2013](#)

²⁰⁰ [Council of Europe: Action against Economic Crime, 2013](#)



EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

The Internet Organised Crime Threat Assessment (iOCTA)

CHAPTER 5 GEOGRAPHICAL DISTRIBUTION

Whether it is as a home to the cybercriminal elite, providing cheap or reliable infrastructure or simply being a target due to wealth or poor digital hygiene, cybercrime affects all countries. Using the United Nation's geoscheme²⁰¹, the following is a brief summary of significant threats and issues affecting various regions globally, based on data collected in 2013-2014.

Africa



Africa's ICT infrastructure is growing rapidly and it is becoming a major player in the global ICT arena. Despite this, only a handful of African countries have any cybercrime legislation²⁰². African ICT infrastructure is exploited for the hosting of malware²⁰³ and phishing²⁰⁴ websites. This is particularly the case in North African countries such as Algeria or Morocco, although South Africa is also host to a high number of phishing sites. Africa now has more mobile subscribers than the USA or EU²⁰⁵. Consequently some North and West African countries have high download rates for malicious apps²⁰⁶.

Some African regions, particularly West Africa, are the source of many of the scams and frauds which pervade the Internet.

The Americas



The availability of cheap, reliable hosting means that globally North America hosts a significant amount of malicious content - generally several times that of any other world region²⁰⁷. North America (typically the USA) hosts the most malicious URLs^{208,209} for websites infected with exploit kits²¹⁰, or content related to phishing or spam²¹¹. North America also hosts the most botnet command and control (C&C) servers²¹² and is the source of much of the world's spam²¹³.

Central America (Mexico) and South America (Argentina, Colombia and Peru) are also important centres for spam distribution²¹⁴, and/or the hosting of phishing sites²¹⁵. A significant proportion of hosting in the Caribbean also hosts malware or phishing websites²¹⁶.

North America holds much of the world's wealth, and with a population of over 300 million, all speaking English, represents a large, lucrative target for cybercriminals. Perhaps also as a consequence of hosting the most malicious material, North America is often the most

²⁰¹ [UN Statistics](#)

²⁰² [Trend Micro: Africa, New Safe Harbor for Criminals, 2013](#)

²⁰³ [Trend Micro: 3Q 2013 Security Roundup](#)

²⁰⁴ Microsoft [SIR v16](#)

²⁰⁵ [Quartz: Africa has More Mobile Subscribers than the US and EU](#)

²⁰⁶ [Trend Micro: 3Q 2013 Security Roundup](#)

²⁰⁷ EUCTF Workshop 09/04/2014

²⁰⁸ [Trend Micro: 3Q 2013 Security Roundup](#)

²⁰⁹ [Kaspersky: Security Bulletin 2013](#)

²¹⁰ [F-Secure: Threat Report H1 2013](#)

²¹¹ [McAfee: Threats Report: First Quarter 2014](#)

²¹² [McAfee: Threats Report: Third Quarter 2013](#)

²¹³ [Trend Micro: 2013 Annual Security Roundup](#)

²¹⁴ [Trend Micro: 2013 Annual Security Roundup](#)

²¹⁵ [Microsoft SIR v16, 2013](#)

²¹⁶ [Microsoft SIR v16, 2013](#)

vulnerable to attack - accessing the most malicious URLs²¹⁷, encountering the most banking Trojans²¹⁸ and harbouring the most botnet victims^{219,220}. South America, Brazil in particular, also encounters high levels of banking malware and has a significant number of botnet victims²²¹.



The majority of cybercrime related activity in Asia is focussed in Eastern Asia, predominantly in China. China hosts a significant number of URLs linked to malicious activity^{222,223}, along with Japan, China is also a top source of spam^{224,225}. China, Taiwan and South Korea all host notable numbers of botnet C&C servers²²⁶.

Central, Western and Southern Asia typically also provide hosting for malware of phishing sites²²⁷. India (Southern Asia) is also a source of spam²²⁸.

Eastern and South-Eastern Asia also house a significant number of global victims accessing malicious URLs and subject to malware attacks²²⁹. In Eastern Asia, Japan and Taiwan are both affected by banking malware and South Korea consistently maintains significant botnet connections²³⁰. Both South (India) and South-Eastern Asia (Malaysia) also have significant botnet activity^{231,232}. South-Eastern Asia also has high levels of malicious app downloads²³³.

217 [Trend Micro: 3Q 2013 Security Roundup](#)

218 [Trend Micro: 2013 Annual Security Roundup](#)

219 [Trend Micro: 3Q 2013 Security Roundup](#)

220 [McAfee: Threats Report: Third Quarter 2013](#)

221 [Trend Micro: 2013 Annual Security Roundup](#)

222 [Trend Micro: 3Q 2013 Security Roundup](#)

223 EUCTF Workshop 09/04/2014

224 [Trend Micro: 2013 Annual Security Roundup](#)

225 [McAfee Labs Threats Report: First Quarter 2014](#)

226 [Trend Micro: 2013 Annual Security Roundup](#)

227 [Microsoft SIR v16, 2013](#)

228 [Trend Micro: 2013 Annual Security Roundup](#)

229 [Sophos Security Threat Report 2013](#)

230 [Trend Micro: 2013 Annual Security Roundup](#)

231 [McAfee: Threats Report: Third Quarter 2013](#)

232 [Trend Micro: 3Q 2013 Security Roundup](#)

233 [Trend Micro: 3Q 2013 Security Roundup](#)

A significant number of child sexual abuse live-streaming cases are originating from South-Eastern Asia, where familial or community level organizations are providing Western sex offenders with real-time, pay-per-view, child abuse sessions.



The majority of cybercrime related activity within Europe is focused in Eastern and Western Europe. Northern Europe, especially the Nordic countries, has one of the lowest malware encounter rates²³⁴, despite having the highest Internet penetration globally²³⁵. Many VPN providers are also located in Sweden.

Like North America, Western Europe enjoys fast and reliable ICT infrastructure which is exploited to host malware and other malicious content. Infrastructure in France, Germany, Luxembourg, the Netherlands and the United Kingdom hosts various exploit kits²³⁶ or other malware^{237,238}, botnet C&C servers^{239,240}, bullet proof hosting and spam and phishing²⁴¹ URLs. Spain and Italy are also notable sources of spam²⁴².

Infrastructure in several Eastern European countries is exploited by cybercriminals. Although activity is predominantly focused in Russia²⁴³, the Ukraine, Belarus, Latvia, Lithuania, and Romania all host malicious content such as exploit kits²⁴⁴, other malware or phishing sites²⁴⁵. Botnet C&C servers are also commonly hosted in Russia and the Ukraine^{246,247}. Eastern Europe, in particular Russia and to a lesser extent the Ukraine, is also considered to be home to the majority of the highly technical

234 [Microsoft SIR v16, 2013](#)

235 [Internet World Stats](#)

236 [F-Secure Threat Report H1 2013](#)

237 [Trend Micro: 3Q 2013 Security Roundup](#)

238 [Kaspersky Security Bulletin 2013](#)

239 [McAfee: Threats Report: Third Quarter 2013](#)

240 [Trend Micro: 2013 Annual Security Roundup](#)

241 [McAfee Labs Threats Report: First Quarter 2014](#)

242 [Trend Micro: 2013 Annual Security Roundup](#)

243 [Kaspersky Security Bulletin 2013](#)

244 [F-Secure Threat Report H1 2013](#)

245 [Microsoft SIR v16, 2013](#)

246 [McAfee: Threats Report: Third Quarter 2013](#)

247 [Trend Micro: 2013 Annual Security Roundup](#)

cybercriminals such as malware developers, and the source of many of the specialised services on the digital underground.

Whilst many cybercrime attacks originate either directly from European countries or via infrastructure held there, these attacks are generally directed at jurisdictions outside Europe. Europe, particularly the West, has some of the lowest malware infection rates. When it comes to malicious app downloads however, several Eastern European countries, including the Ukraine and Russia, have high download volumes²⁴⁸.

Oceania



Generally the Oceanic countries do not feature heavily in cybercrime reporting. Bandwidth in Australia is expensive which is likely to be a deterrent for those seeking to host illicit content. In 2013 Australia did host botnet C&C servers²⁴⁹ although this was likely to be on compromised machines.

Australia, although it has a much smaller population than North America, is also English speaking and likely to be targeted due to its wealth. Australia is heavily targeted by banking malware²⁵⁰.

Non-Specific Geographical Distributions



Factors other than the location and nature of infrastructure play a role in the sources and targets of cybercrime. A common language often means that one country is targeted by cybercriminals from another country. In many cases proximity is another factor, with many jurisdictions reporting that their investigations lead to neighbouring states.

²⁴⁸ [Trend Micro: 3Q 2013 Security Roundup](#)

²⁴⁹ [Trend Micro: 2013 Annual Security Roundup](#)

²⁵⁰ [Trend Micro: 2013 Annual Security Roundup](#)





EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

The Internet Organised Crime Threat Assessment (iOCTA)

CHAPTER 6 LAW ENFORCEMENT

Common issues

Under reporting and limited sharing of information

Under reporting is a notable feature of cybercrime. Other crime areas such as fraud have long established traditional and alternate crime reporting mechanisms such as hotlines and consumer websites. Although many jurisdictions are implementing similar reporting mechanisms for cybercrime, both citizens and industry are still ill-equipped and ill-informed as to how to recognise and report cybercrime.

In addition to a general lack of awareness other issues impact on reporting levels. In child abuse cases, fear is a prevailing deterrent. In cases of data breaches there is a simple unwillingness to report. The damage caused by a data breach or network intrusion goes beyond the disclosure of data or intellectual property; the reputational damage caused by such an event may have considerable impact on a company's image, its customer relationships and stock value. Understandably then, many breaches go unreported to law enforcement for fear of the repercussions of a public exposure.

Furthermore, relevant data and information that is available to LE in one Member State is often not readily shared with other Member States.

Capability, capacity and training

While specialised cybercrime departments are an important first step for LE in combating cybercrime, as a long term solution they are insufficient. The capability to deal with crime on the Internet needs to be extended across *all* of law enforcement. Without officers having the skills and knowledge they need, starting with those on the 'front line', law enforcement will be unable to effectively recognise and react to cybercrimes.

Lack of forensic capability and capacity are often limiting factors in conducting cybercrime investigations. In some instances this can be a lack of digital forensic knowledge

and expertise as well as a lack of forensic tool support. Even for well-equipped and experienced digital forensics units it is not the lack of evidence that poses a problem, it is the volume of material they are required to analyse and the time and manpower it takes to do so. A decade ago a case may have involved a few pieces of media. Today a typical case often involves multiple devices and many terabytes of data. Technology cannot compensate entirely for this growth, the deficit for which must be met by human resources. Moreover, there is a tendency for companies to offer native, built-in encryption in digital devices, rendering even more advanced digital forensics techniques, such as chip-off methods for mobile phones, ineffective.

Forensic efforts are additionally hampered by the increasing level of forensic skills and techniques displayed by cybercriminals, particularly in the area of child sexual abuse online. The increasing use of encryption by offenders also causes issues for law enforcement.

The lack of capacity may also mean that forensic examinations are limited in scope to obtain evidence to support a current operation. Media obtained as part of a criminal investigation may however hold a wealth of intelligence or evidence that may either support existing investigations or could initiate new ones.

Attribution and detection

The investigation of cybercrime offences is also hampered by the level of anti-forensic measures deployed by criminals. *Attribution* is a major challenge for law enforcement, whether this is determining the real world identity behind an online nickname or victim identification in a child abuse case. Anonymisation techniques and the use of virtual currencies make both the technical and money trails difficult to detect and follow.

Jurisdiction

Even if the source of an attack can be identified it is unlikely to be limited to the investigating states' own jurisdiction. Cybercrime investigations often span multiple jurisdictions

globally and many attackers operate within jurisdictions with which the EU has limited co-operation. Even within the EU or when dealing with co-operative jurisdictions, slow and cumbersome Mutual Legal Assistance Treaty (MLAT) processes can significantly hamper investigations and the disproportionate effort involved in even modest cases serves as a constraint in times of austerity.

Legal framework

While some progress has been achieved in establishing a suitable legislative framework, much more requires attention, for instance in relation to the need for coherence and harmonisation of legislation across the EU and in providing the investigative legal instruments required to effectively combat cybercrime.

Current data retention laws are insufficient for law enforcement. The majority of intelligence and evidence for cyber investigations comes from private industry. With no data retention, there can be no attribution and therefore no prosecutions. In this context a new EU Directive on data retention, following the European Court of Justice's annulment of the existing measure is urgently required.



EUROPEAN CYBERCRIME CENTRE
ECC
EUROPOL

The Internet Organised Crime Threat Assessment (iOCTA)

CHAPTER 7 CONCLUSIONS

As rates of global Internet connectivity continue to grow, the volume of attacks and the scale of their economic impact will also increase. In light of the vast cyber threat landscape and the limited availability of resources, it is essential to prioritise the right actions and initiatives.

This is particularly true for the EU given its place as a highly attractive target for cybercrime due to its relative wealth, high degree of Internet penetration, its advanced Internet infrastructure and increasing dependency on Internet-mediated services.

Joint action is required to address Cybercrime-as-a-Service. The array of online criminal services makes it possible for any criminal or organised crime group (OCG) to enter into the lucrative realm of high-tech crimes with very limited understanding of the technicalities. This includes a wide range of services which support and facilitate existing cybercrime, for instance counter-antivirus and money laundering services. These services need to be tackled with priority alongside the targeting of skilled criminal programmers. Focus on disrupting the top identified criminal forums and marketplaces, and on targeting individuals with the highest reputations on these fora therefore should be maintained.

Furthermore, coordinated international action is needed to counter and limit the abuse of anonymity on privacy networks like TOR and I2P. Criminal online markets that facilitate the trade in drugs, weapons, fake IDs and child sexual exploitation online provide a safe haven for criminals. Moreover, there are Darknet sites that promote the communication, exchange of expertise and proliferation of criminal behaviour and extremism. While respecting the privacy of law-abiding users, law enforcement should pro-actively take down these malicious sites and take action against the criminals behind them.

The abuse of anonymity in virtual currency schemes must also be addressed. Although virtual currencies can be used for legitimate financial transactions, the anonymity of such payments make them very attractive for criminals as they leave little trace of criminal transactions and money

laundering. Investigative action against the criminal use of virtual currencies must be a priority.

With regard to regular online payments, citizens and companies need to be better protected against data theft and the abuse of payment credentials. Following successful actions against the procurement of air fares with stolen credit card details, other areas of abuse should be identified and addressed such as the damage caused to online vendors of electronics and luxury goods. Credit card companies and law enforcement should actively support bona fide online retailers with a view to preventing the abuse of stolen credentials and focusing on the prosecution of criminal gangs that are active in this domain.

Proliferation of broadband connection in developing countries has led to growth of on-demand streaming of Child Abuse Material. The mainstream use of social media has also led to an increase in offences such as grooming and sexual extortion.

Not every attempt to hack, intrude or attack is successful. It often takes some experimenting. The lessons learned, also from unsuccessful attempts, can then be used against other victims. Unfortunately, data on successful and unsuccessful cybercrime attempts are usually not shared. This allows criminals to improve their modus operandi while their potential victims get no chance to protect themselves and law enforcement loses the opportunity to intervene and address the threat in a pro-active manner. This calls for collective measures to improve the international sharing of data on such incidents in a standardised and effective way, between all sectors and with law enforcement. The cyber dimension is spreading gradually across crime areas, including traditional crimes that contain progressively more cyber elements. Yet, it appears that EU law enforcement, Europol included, has not fully conceptualised how to integrate this cyber dimension into all relevant aspects of police work, let alone devise a strategy and implementation plan to make this happen. This does not mean that every police officer needs to become a cyber-expert, but rather that every

officer should understand the cyber related aspects of his or her work and be competent to deal with them. Such a fundamental re-thinking of policing and embedding cyber in structures, processes and training is urgently needed, because it will take considerable time to implement the necessary changes properly while in the meantime the cyber dimension in crime continues to expand rapidly.

To keep up with those speedy developments continued investments are also needed in building up and maintaining high-tech cybercrime expertise and digital forensic capability. Considering the cross-border nature of cybercrime, it is worth investing in the (further) development and endorsement of EU-wide standards for digital forensics to ensure that evidence collected in one Member State is admissible in court in all other Member States.

Protection capabilities also must improve. Experience in reducing the number of lethal traffic accidents has demonstrated that a strong impetus by industry to implement minimum safety measures, such as safety belts in rear seats and the additional brake-light, are both possible and effective. In fact the reduction in lethal traffic accidents was successfully achieved by a combination of three strategies:

- Education of drivers and road users through various media channels;
- Engineering: seat belts, airbags, brake lights, removing accident Black Spots by re-engineering roads, etc.; last and not least
- Enforcement: Setting up dedicated well-staffed Traffic Corps dealing specifically with road users and automatic number plate recognition systems, for instance.

The combination of all three makes the highway a safer place to be. A similar approach should be considered for cyber security on the information superhighway. This applies to hardware and software manufacturers as well as to operators of networks and Internet services. In addition, a stronger visibility and presence online should be considered to address the phenomenon of minimisation of authority of police services online and to create credible deterrence for the criminal misuse of technologies and communication.

Moreover, the virtues of prevention and awareness deserve significantly more attention. For law enforcement there should be a clear obligation to translate new criminal *modi operandi* swiftly into awareness messages to inform industry and citizens alike. Governments should consider emphasising the importance of Internet security sufficiently to change the mind-set of Internet users effectively in order to embed security awareness fundamentally in their online activities.

Last but not least, the legislators in the EU should jointly agree on preparing a balanced and coherent package of legislative measures that protect citizens and businesses online and enable law enforcement and prosecution services to intervene where necessary.

This package should strike the right balance between protecting the citizen's right to privacy, while enabling law enforcement to disrupt and investigate when there are clear indications of criminal activity. Those can in particular be identified in anonymised environments that openly aim to attract customers for illicit trade or like-minded individuals for the exchange of experience and proliferation of criminal behaviour.

The empowerment of law enforcement and judicial services should include practical investigative instruments for the detection and attribution of crimes and criminal transactions to end-users and the collection of evidence for that purpose. This implies that relevant data is retained and, where there are clear indications that crimes were committed, made available to law enforcement in accordance with clear criteria and conditions. Furthermore, an obligation for industry and critical infrastructure operators to share threat related data, also with law enforcement, is a condition-sine-qua-non to enable effective protection. The legislative package would ideally be harmonised across the EU and be interoperable with the existing legal frameworks in the Member States. This is of particular importance to facilitate a successful international law enforcement response to the variety of threats that cybercrime poses to EU society.



EUROPEAN CYBERCRIME CENTRE
ECC
EUROPOL

The Internet Organised Crime Threat Assessment (iOCTA)

APPENDICES

A1. The criminal exploitation of the Internet: Views of the academic advisors

The past is much easier than the future to predict, and in an area as dynamic and rapid in its development as eCrimes, it is risky to predict far ahead. There are many ways of approaching the issue of threats, but one helpful way is to break them down into the components of capabilities, intent, and vulnerabilities, both technical and social. An important component of organised crime is scalability, and this is what the web (or webs) have brought to us, enabling much smoother interaction between distant and personally unknown offenders than was possible before, and a huge increase in certain forms of criminality, industrialising crime capabilities to the less technically competent via online kit sales. This in turn creates substantial and permanent problems to individuals, businesses and nation states for awareness of risk, prevention and cross-border policing, as crimes can occur simultaneously in multiple jurisdictions from which the offender is absent, as well as problems for justice systems which have enough difficulty in coping with offline crimes, let alone online ones. Although legal frameworks are important both to surveillance and to cross-border cooperation and evidential admissibility for forensic purposes, even with large increases in cyber-staffing and retraining that are hard to achieve in the climate of European austerity, it is impossible to prosecute our way to eliminating or even very substantially reducing e-crimes. We need to prioritise our resources, leverage public-private cooperative relationships, and marshal our resources carefully to maximise their impact on harms of different kinds. All crime for gain lies at the intersection between what offenders seek to do and what we do (intentionally or not) to counteract it, and we need to live in a constant state of preparedness to manage evolving risks. We need to find ways of motivating European and non-EU MS to act on our behalf against offenders who may not be harming victims in their own jurisdiction, and to support Europol in their analytical and co-ordinating efforts in that direction.

We feel privileged to have contributed to the accompanying threat assessment, and here we offer some brief collective comments on a set of issues that we think are important, to supplement the material that Europol has generated with our modest input as 'critical friends'.

Crime-as-a-Service

Malware

The volume of new malware, speed at which it evolves and the new methods by which it is being deployed cannot be underestimated. Criminals are finding new victims who fall for old tricks as well as developing new ways of infecting even the most knowledgeable. The current commercial product sets struggle to keep up and we feel that there is a growing need for new approaches to defence in this space.

Attacks on Mobile Devices

As we pass the point where the majority of people around the globe use mobiles to connect to the Internet we believe that mobile devices are the current battleground where criminals have the upper hand. With a steady stream of vulnerabilities identified in the Android operating system, which is the single most widely used platform, as well as exploits emerging for what were previously considered secure systems such as iOS, we believe that law enforcement will continue to see cyber-crime on mobile devices as the single biggest challenge.

Credit, Payment Card and Bank Online Fraud

The success of EMV has driven an increasing proportion of crime on European payment cards to Card Not Present, where the PIN may not have to be known. The PIN-less world is shrinking, and even the US is adopting it, so the *proportion* of card fraud that is online will continue to

grow unless the cards themselves can be compromised technically on an industrial scale, which we consider to be unlikely in the period of this assessment.

However, there remain serious risks on the horizon. One is risks arising from mobile phone and tablet banking. Dynamic and spoofed IP addresses make user-reported IP addresses ineffective for identifying devices. Mobile devices frequently change location, and their locations may not match addresses of record. Mobile emulators allow devices to represent themselves with false operating systems.

Another major risk is synthetic (i.e. made up) as contrasted with copied/stolen identities, used to commit fraud. European data protection rules do not allow credit reference agencies to use 'problematic addresses' to aggregate credit applications. Boarded up pubs and residences can accumulate a large number of applications using artificially created data without disturbance by natural surveillance. There is increased chatter in Dark Web Forums about techniques for synthetic id creation, so it will spread. This may mean fewer problems for legitimate people, but commercial risks remain from first party fraud 'bust outs'.

Child Sexual Exploitation Online

The most harmful forms of child sexual abuse imagery involve the exploitation of the children themselves. Much has been achieved by the aggregation of images internationally and by the cooperation of payment card services in cutting off opportunities. There is a tendency for the worst images to be exchanged in networking sites which are vetted by existing members, so they are not freely available. This will continue to be the case, as a form of criminal risk management from law enforcement, and the enforcement challenge is to gain access to and disrupt/destroy the networks.

Data Breaches

Data security is everybody's business, but the periodic massive leakages of financially exploitable personal data and health data by insider compromise, by outsider hacking and by carelessness in throwing away both paper and electronic records remains an enduring feature, increasing public distrust and fear of both business and government. American surveys show that the public tend to blame retailers rather than bankers for data breaches, but despite high profile sackings (at Target), there is a need for regularly reinforced messages to third party data holders and more managerial attention to data leak risks, though corrupt approaches from organised criminals require a different control strategy.

Attacks on Critical Infrastructure

Despite many scare stories we have yet to see tangible evidence of wide scale cyber-crime involving critical infrastructure. However, the potential for damage is high and so we believe it is vital that vigilance is maintained in this area. Many argue that critical infrastructure is likely to be more a target for nation states than criminals. But, it is more a matter of when rather than if crimes emerge involving attacks on critical infrastructure. Critical infrastructure represents a relatively soft target in some cases and the tools are available so it is difficult not to conclude that criminals will work out how to exploit this unfortunate combination.

Enablers

Social Networking

Social Media is a fact of life and is considered by many as a fundamental human right. We do not see its demise in any foreseeable future. That being so, it will remain a very active attack vector for criminals. New variants of phishing attacks via social media are inevitable in our view, and law enforcement will have an increasing battle to keep up with this threat. As more people use social media (and that increase shows no sign of slowing) the scale of the issue for law enforcement can only get larger.

Virtual Currencies

The suspicions about why virtual currencies need to exist has only been heightened with the emergence of new forms of the currencies. Bitcoin and other similar currencies that offer pseudo anonymity raised considerable concern as they could be used for criminal transactions and ultimately exchanged for national fiat currencies through exchanges. As a result law enforcement have had a considerable challenge in tracking such transactions or even identifying activities such as money laundering. We feel it should concern everyone that the latest cyber currencies are intended to be truly anonymous and to facilitate anonymous transactions. We face a situation where law enforcement may be completely unable to trace even very large criminal transactions.

Big Data

The tools that are emerging for use in deriving information from unstructured data gathered from around the Internet are impressive. However, as with all tools there is scope for misuse: subverting the original purpose to, for example, profile potential victims or to commit identify fraud. Law enforcement agencies will have little choice but to deal with the consequences of this. The onus can no longer be put on individuals to protect their data as it may have been given away piece-meal and reconstituted by criminals using Big Data tools. We must all assume that

data that would previously have been thought personal and sensitive by the way in which it is combined, can now be formed from storage of component data none of us intended to be used in the way criminals will now do. If nothing else, we expect the trade in personal data on the Darknet to increase even without the large single data breaches that continue to occur despite bad publicity, regulatory sanctions and the costs of remediation.

The Internet of Everything

The IOE is inevitable. We must expect a rapidly growing number of devices to be rendered “smart” and thence to become interconnected. Unfortunately, we feel that it is equally inevitable that many of these devices will leave vulnerabilities via which access to networks can be gained by criminals. History suggests that as new types of devices become connected to the Internet security can take some time to mature. This is exactly what has happened with mobile phones. The IoE represents a whole new attack vector that we believe criminals will already be looking for ways to exploit.

Cloud Services

The falling price, global distribution and relative anonymity of cloud services means that criminals are bound to see it as a good platform for mounting criminal activity. We feel that the law enforcement agencies must assume that cloud will form an increasingly large part of future criminal activity ranging from acting as command and control platforms for distributing and exploiting malware, right through to acting as a “back office” IT in all manner of technology enabled crimes. This means that law enforcement agencies will have to cooperate globally if they are to stand any chance of both preventing crime and bringing the guilty to justice.

TOR and other anonymizing tools and services

There is a seemingly insatiable desire for anonymity amongst the population as a whole. It is considered synonymous with privacy. Whilst we believe that some technologies that are considered to provide anonymity will soon be shown to be vulnerable to tracing, we believe this will drive a burgeoning number of anonymisation tools and services. The law enforcement agencies cannot hope to prevent these technologies being used as they have legitimate uses. Therefore, we feel that law enforcement agencies will need to put in place programmes for studying these emerging technologies in order to find means of countering their use by criminals. This “arms race” is expensive and so it is an obvious candidate for multi-national collaboration, and the establishment of centres of excellence.

Emerging and Future Developments

Increase in targeted and more sophisticated attacks, including cyber espionage

- Instead of large scale but not very specific attacks, we in addition see an increasing number of attacks that are very specifically designed to attack a concrete target.
- An increase in attacks related to identification instruments, tax and social security benefits using business fronts, often set up specifically for this purpose.
- Attacks on vulnerable individuals, on (and/or via) financial services staff who get into financial or sexually discrediting ‘trouble’ and are compromised, and to high-value IP hacking targets, via spear-phishing or social engineering perhaps using social media.
- Cyber-espionage is a continuing threat. The search for ‘business intelligence’ by hacking/ social engineering is a major threat to European economic actors.
- Increasing attacks against mobile services (such as mobile banking). Due to advanced man-in-the-middle attacks, the very basic two-step verification will not be efficient anymore.

Extortion/Ransomware

- Although extortion is a traditional crime which continues to exist off-line, recent developments show a relation between it and ICT. Offences are committed by using information and communication technology as well as virtual payment systems.
- Increased use of ransomware: Rise in the number of people and organisations hit by this type of attack but also novel variants emerging such as ransomware-affected intelligent devices such as found in transport or even medical devices.

Internet of Everything

- As processing power is increasingly incorporated into everyday objects, it obviously increases the attack surface available for criminal activity. This activity may also be about co-opting these intelligent devices to participate in crime (e.g. becoming part of a botnet). Devices in the IoE are likely to be more vulnerable simply because they are new, and history suggests that such technology remains vulnerable for an initial period.

- Attacks via the Internet of Everything will become increasingly common and that is very disruptive socially.

Data Breaches

- Taking into account the clear trends to Big Data leads to a logical consequence of increasing relevance of attacks against the integrity and confidentiality of data. Taking into account the significant financial losses caused by such attacks underlines the threat.
- Data Breaches are precursors for other things – especially when personal data is involved.

Reflection attacks

Reflection attacks, particularly against choke points on the Internet such as Internet Exchanges can be expected. Having seen DDOS attacks mounted using appropriately configured DNS servers and now NTP servers, we can suspect that criminals will find ways of exploiting other UDP based protocols to increase the volumes they can use in attacking the infrastructure of any organisation, disrupting their function.

Anti-Forensics and Anonymisation technologies

Increased use of anti-forensic software and anonymising technologies; Tor, with its fixed, known exit nodes, loses favour with criminals who will switch to P2P based anonymisations e.g. I2P. Post Snowden, we will see other anonymising technologies being developed for laudable purposes, but these will be rapidly enlisted by criminals to hide their tracks. Despite recent reports about the vulnerability of anonymous communication technology, law enforcement does not yet have the full toolset (both technical and legal) to identify offenders using such technology.

State involvement

State involvement in the commission of crimes, such as attacks against computer systems or espionage are an increasing challenge for law enforcement agencies, as “regular” offenders and state actors operate in different environments, and different legal regimes might apply. There will continue to be controversies over the attribution of criminal acts to state, to state-sponsored, and to state-tolerated actors.



EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

The Internet Organised Crime Threat Assessment (iOCTA)

APPENDICES

A2. Cyber legislation

For law enforcement, observing developments in the field of law is as important as monitoring trends in the commission of crimes and latest investigation techniques. Without criminalisation the hands of law enforcement agencies are bound – and without adequate procedural law, the prosecution of high-tech offenders can be close to impossible.

Trend 1: Legislation related to cybercrime is moving beyond substantive criminal law and procedural law

25 years ago the focus of legislation was on substantive criminal law. When the Council of Europe adopted the 'Expert Report on Computer-Related Crime' in 1989, it was dealing with substantive criminal law (criminalisation of offences)²⁵¹. 20 years ago the discussions started to include elements of procedural law (enforcement of law). The 1995 recommendations of the Council of Europe are an example of this development²⁵². 15 years ago the focus widened again and international cooperation became part of the discussion. This is for example underlined by Chapter III of the 2001 Council of Europe Convention on Cybercrime²⁵³ that addresses aspects of international cooperation.

This development has not stopped. In the last 15 years the way legislation and regional standards are drafted has developed further. The variety of areas of law covered under the umbrella of cybercrime legislation has increased and includes the following:

- Definitions: The 2001 Council of Europe Convention on Cybercrime only includes four main definitions. The list of definitions in other regional instruments, such as the 2013 SADC²⁵⁴ Model Law²⁵⁵ is significantly more complex. A second trend is to move towards more up-to-date definitions. The 2013 EU Directive on attacks against information systems²⁵⁶ for example refers to 'information systems' instead of computer systems to avoid confusion when it comes to devices such as mobile phones or wearable technology.
- Substantive criminal law: Although the 2013 EU Directive on attacks against information systems does not go beyond the 2001 Council of Europe Convention on Cybercrime, when it comes to criminalisation there is global trend towards more inclusive approaches. Recent approaches like the 2013 SADC Model Law for example already include the recommendations from the UNODC Expert Group on Identity-related Crime related to the criminalisation of identity theft – a growing concern also in the European Union. The 2010 Stockholm Programme Action Plan²⁵⁷ included the aim to develop a legislative proposal for the criminalisation of identity theft. This has however not yet been finished.
- Procedural law: While in the past the focus was on search and seizure and the interception of communication, the use of advanced technologies such as VoIP, encryption, anti-forensics and anonymous communication services goes along with the challenges of using such tradition instruments. Instruments like the 2012 HIPCAR

251 [Recommendation No. R \(89\) 9, adopted by the Committee of Ministers on 13 September 1989 at the 428th Meeting of the Ministers Deputies](#)

252 [Recommendation No. R \(95\) 13, adopted by the Committee of Ministers on 11 September 1995 at the 543rd Meeting of the Ministers Deputies](#)

253 [Convention on Cybercrime, Council of Europe, ETS 185](#)

254 [Southern African Development Community](#)

255 [SADC Computer Crime and Cybercrime](#)

256 [Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA](#)

257 [Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions – Delivering an area of freedom, security and justice for Europe's citizens, Action Plan Implementing the Stockholm Programme, COM 2010, 171](#)

Model Law on Cybercrime/e-Crimes²⁵⁸, that was developed with funding from the EU, includes instruments like the application of remote forensic tools (such as keyloggers). As such, it is not only in line with European standards but goes beyond it in terms of criminalisation as well as procedural law and investigation instruments.

- **Electronic evidence:** In 2002 the Commonwealth adopted two model laws: one on computer and computer-related crime and one on electronic evidence. From a practitioner's point of view this is a logical development as the most efficient investigation does not help if the collected evidence is not admissible in court. Unlike other regions, the EU has not yet developed a harmonised approach to addressing issues such as admissibility of electronic evidence collected abroad. Other instruments such as the above mentioned Commonwealth Model Law and the SADC Model Law contain such regulations.
- **Liability of ISPs:** It is almost impossible to commit a cybercrime without the involvement of ISPs. But is an ISP criminally responsible for offences committed by its user and is the ISP authorised to report crimes, for example when the ISP detects illegal content? The 2000 EU E-Commerce Directive contains a set of general liability regulations that have been picked up by other regions of the world.

Trend 2: Slower international harmonisation but more regional approaches

Given the inherently borderless nature of cybercrime, investigations must be facilitated by harmonised legal systems and international cooperation measures.

Speed remains a key requirement in investigations. If law enforcement in two or more countries need to cooperate outside existing legal frameworks their abilities are limited by the general Mutual Legal Assistance Treaty (MLAT) regime. In the best case other international (but not cybercrime specific) instruments for expedited cooperation – such as the United Nations Convention against Transnational Organized Crime (UNTOC), or bilateral agreements, are applicable. The very basic rules of international courtesy, based on reciprocity, apply. The related procedures are strict, are based on a complex workflow and are consequently in general, lengthy. Although partly generalised it is possible to say that from the perspective of law enforcement, when investigating cybercrime, less time-critical procedures do not reflect

the high speed in which cybercrimes are committed and in which important evidence (such as traffic data/meta data) is automatically deleted.

Current trends in the law enforcement community foster more flexible arrangements for cross-border data exchange – such as information sharing for police use only. However, Europol believes that it is desirable to have a legal framework for international cooperation in place that:

- allows expedited cooperation,
- maximises the protection of fundamental rights of the data subject, even and especially in cross-border investigations, for instance by means of pseudonymisation for de-confliction and identification of links,
- has reach beyond the EU and the trustful (usually Western) partnerships, including for instance the US, non-EU Schengen partners, Canada and Australia, and
- eventually leads to the receipt of evidence that can be used in court.

Current legal developments

- **United Nations:** In 2010 the UN Crime Congress examined the need for a global legal instrument in the fight against cybercrime²⁵⁹. It requested UNODC to conduct a comprehensive study. This study was published in 2013²⁶⁰. Since then the results of the study have been discussed but no substantive action has been taken since.
- **European Union:** Following the ratification of the Lisbon Treaty renewed efforts towards the harmonisation of laws in relation to computer crime have occurred. The 2011 EU Directive on child pornography²⁶¹ and the 2013 EU Directive on attacks against information systems are examples
- **Council of Europe:** Until August 2014, 42 countries went through the process of ratification/accession to the Convention on Cybercrime. This includes non-European countries such as Australia, Dominican Republic, Japan, Mauritius, Panama and

258 [Cybercrime/e-Crimes Model Legislative Text, developed under the EU co-funded project HIPCAR \(Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean\)](#)

259 [Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World](#)

260 [UNODC Comprehensive Study on Cybercrime, 2013](#)

261 [Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA](#)

the United States. The EU Member States enjoy good cooperation with those countries that have signed and ratified the Convention. However, from the list of the top 10 countries from where criminal activities originate, only three have ratified the Convention on Cybercrime. Important countries like the Russia, China, India and Brazil have not signed or ratified the Convention. Developments, such as the recent discussion within the Council of Europe about another possible additional protocol to the Convention on Cybercrime that deals with trans-border access, are not relevant to those cases.

- Africa: The Economic Community Of West African States (ECOWAS) Directive on Fighting Cyber Crime within ECOWAS²⁶², the Common Market for Eastern and Southern Africa (COMESA) Cybersecurity Model Bill, the SADC Model Law on Computer Crime and Cybercrime and the Draft African Union Convention on the Establishment of a Legal Framework Conducive to Cybersecurity in Africa all contain provisions related to the fight against cybercrime. This shows the dynamics of regional harmonisation in the African region.
- Caribbean: The aforementioned HIPCAR Model Legislative Text on Cybercrime as the well as the OECS²⁶³ Electronic Crimes Bill²⁶⁴, which were developed in 2012 and 2011.

262 [Directive C/DIR.1/08/11 on Fighting Cyber Crime Within ECOWAS](#)

263 [Organization of Eastern Caribbean States](#)

264 [Electronic Crimes Bill, Fourth Draft, 2011](#)



APPENDICES

A3. The cyberpsychology of Internet facilitated organised crime

Introduction to cyberpsychology

Cyberpsychology is a field within applied psychology, focusing on the impact of emerging technology on human behaviour. Cyberpsychologists study Internet psychology, virtual environments, artificial intelligence, intelligence amplification, gaming, digital convergence, social media, mobile and networking devices. There are now 30 peer-reviewed journals, publishing in this area and over 1000 articles now generated per annum²⁶⁵. As the recently published three-volume Encyclopaedia of Cyber Behaviour notes, it is predicted that as a discipline cyberpsychology will enjoy exponential growth due to the continued rapid acceleration of Internet technologies and the “unprecedentedly pervasive and profound influence of the Internet on human beings”²⁶⁶.

Multi-disciplinary approach

Arguably, academic investigation of criminal behaviour in cyberspace requires interdisciplinary efforts in a practical sense, and transdisciplinary theoretical perspectives in an exploratory context²⁶⁷. Cyberpsychology is an exemplification of how this combination can, and indeed must, be achieved, requiring input from psychology and computer science, but also similarly recent enterprises such as network science, data visualisation and digital humanities. At the same time, academics in this context need to be open to a number of possibilities, across the full spectrum of academic endeavour, ranging from the hard metrics of computational sciences to the qualitative interrogations of the social sciences.

This approach will necessitate methodological and ideological openness on the part of the researcher.

Additionally cyberpsychologists support the use of virtual research methodologies to ensure accurate and robust findings – for example, anonymous confidential crime-related information online submission mechanism²⁶⁸. Consequently, to fully understand, and hence prevent, Internet-facilitated organised crime, we need to incorporate learnings from a variety of disciplines. For example, anthropological, ethnographic and sociological analyses of sophisticated cyber actors and networked organised crime groups could prove useful in illuminating this problem space. Additionally, advances in data visualisation methodology may provide greater speed of insight via graphic (and real-time) illustration of law enforcement digital intelligence.

In that vein, Vishik²⁶⁹ notes “the multi-disciplinary nature of cyber security attacks is important, attacks happen for different reasons, only some of which are technical, other reasons include, for example, socioeconomic issues”. We need to understand all of these reasons to develop strategies to combat criminal behaviour manifested online, from isolated traces of lone cyber criminals, to complex and subtle indicators of sophisticated cyber criminal networks. Multi-disciplinary research in these areas is clearly very important, however it is understood that, for reasons of law enforcement or national security concerns, such may constitute intelligence and be subject to restrictions. While the principle of public dissemination of scientific research is a time-honoured tradition, arguably we should not be in the business of informing criminal populations as to law enforcement’s knowledge base.

265 Yan, Z. (Ed.). (2012). *Encyclopedia of Cyber Behavior*. IGI Global. doi:10.4018/978-1-4666-0315-8

266 Yan, *ibid*.

267 Suler, J. (2013). [Cyberpsychology as Interdisciplinary, Applied, and Experiential](#). RCSI CyberPsychology Research Centre. Retrieved June 26, 2014

268 Berry, M., & Aiken, M. (2014). In Search of Annie: A Study of Viewers’ Feedback to the Crime Documentaries Highlighting Famous Irish Murder and Missing Persons. *Universal Journal of Psychology*, 2(1), 41–46.

269 Belfast 2014: 4th World Cyber Security Technology Research Summit. (2014). In *Centre for Secure Information Technologies*, Queens University Belfast, p. 8.

Behaviour in cyberspace

Regarding behavioural characteristics in cyber space, the “online disinhibition effect”, Suler²⁷⁰ maintains that people may do things in the virtual world that they may not do in the real world, with or without anonymity. There is a need to conceptualise technology in a new way, a need to think about cyberspace as an environment, as a place, as cyberspace. Furthermore there is a need to consider the impact of this environment on vulnerable populations (such as developing youth), criminal and deviant populations. This is required in order to understand *modus operandi* in this space. Cyberpsychology can assist in this regard, delivering insight at the human/technology interface²⁷¹.

The critical point for law enforcement is the crosspollination between the online and virtual environments: concepts that develop in cyberspace but transfer to real world policing environments. One of the more salient concepts in this light is Suler’s²⁷² minimisation of authority (an aspect of online disinhibition) – whereby a person’s status (as law enforcement, for example) is not as readily appreciated in an online context than offline. Politicians, for example, are infamously treated with irreverence on social media. This levelling effect happens in tandem with the general disregard for established social order that also happens in technological contexts. Moreover, because organisations in this area can work at speed and at scale, they can get their product or service to market faster than government and legislators (and as a result, law enforcement) can react. As a result, by the time such services have been curtailed, the public have already spent some time consuming the product or service and are unhappy with it being removed. ‘Disruptive innovators’ such as Aereo (an online television streaming service²⁷³, recently struck down²⁷⁴) and Uber (an app-driven car company²⁷⁵ which has caused protests among taxi drivers²⁷⁶) are good examples in this regard, though illicit online markets such as Silk Road²⁷⁷ should also be seen in this light. These are classic examples of Suler’s²⁷⁸ minimisation of status transferring to an offline context: there is no little online authority to prevent these systems

being put in place, and as a result, they are at scale before ‘real world’ authority can deal with them.

Regarding cybercrime Kirwan and Power²⁷⁹ outline that “governments attempt to respond with law, corporations with policies and procedures, suppliers with terms and conditions, users with peer pressure, technologists with code” but where is the understanding of human behaviour? The challenge is to factor in an understanding of criminal behaviour that has been amplified and facilitated by technology²⁸⁰.

The critical task for cyberpsychology as a discipline is to build up a body of established findings of how human beings experience technology, the critical task in *forensic* cyberpsychology is to focus on how criminal populations present in cyber environments. For many years efforts have focused on technology solutions to intrusive behaviour, arguably without consideration of how that behaviour mutates, amplifies or accelerates in cyber domains. This view is supported by Maughan:

“...discussing the cyber security threat space, and the consideration of this from a technical angle but also from a human angle, as humans are part of the threat, this needs more thinking. From a Department of Homeland Security (DHS) perspective, as a large agency, it is concerned about globalisation, borders, extremists, natural disasters. In cyber space, criminals, hackers, insider threats, the use of malware etc. and social engineering, all define the threat landscape - The consideration of the impact of people in cyber security is important. The White House 2009 cyber space definition talks about equipment, but is missing people. With regard to threats in cyber security, the user is the weakest link and cyber criminals are people.”²⁸¹

Additionally, Rogers, Siegfried and Tidke²⁸² also acknowledge this blind spot in cybersecurity, pointing out that “research focusing on people is vital if we have any real hope of coming to grips with the phenomena of computer crime.”

270 Suler, J. (2004). The online disinhibition effect. *CyberPsychology & Behavior*, 7(3), 321–326. doi:10.1089/1094931041291295

271 Aiken, cited in Belfast, 2014, *ibid*.

272 *ibid*.

273 Gilbert, Ben. (2014) [What you need to know about Aereo's battle with broadcast television](#)

274 [American Broadcasting Cos., Inc., et al. v. Aereo, I. \(2014\). Supreme Court of the United States](#), 13-461

275 Dent, S. (2014), [What you need to know about Uber, Lyft and other app-based car services](#)

276 Fleisher, L. (2014), [Thousands of European Cab Drivers Protest Uber Taxi Apps](#)

277 Zetter, K. (2013), [How the Feds Took Down the Silk Road Drug Wonderland](#)

278 *ibid*.

279 Kirwan, G., & Power, A. (2012). *The Psychology of Cyber Crime: Concepts and Principles* (p. 277). Information Science Reference, p. xvii

280 Europol. (2011). *Internet Facilitated Organised Crime Threat Assessment (abridged)* (pp. 1–11). The Hague.

281 Belfast, *ibid*, p. 8.

282 Rogers, M. K., Seigfried, K., & Tidke, K. (2006). Self-reported computer criminal behavior: A psychological analysis. *Digital Investigation*, 3, 116–120. doi:10.1016/j.diin.2006.06.002, p. S119



Cyber-specific concepts such as those listed below are becoming well recognised. While recognising that such findings may not endure²⁸³, they are with us at present. As a general rule, we should appreciate the possibility that people, including criminals and victims, act differently in cyberspace than they do 'in real life' and is of significance. This is something that mainstream psychology, and society in general, has resisted for some time - that what happens online somehow isn't 'real'. We must recognise that "the virtual complicates the physical, and vice versa"²⁸⁴ - i.e. in terms of criminology what happens online can impact on the real world and vice versa. The Europol Internet Organised Crime Threat Assessment supports this view, stating that in terms of cybercrime there is a "dynamic relationship between online and offline organised crime"²⁸⁵. Crucially, it is likely that, as the barriers to crime participation and syndication online are reduced, there may be a resulting increase in online crime. Logically, given the dynamic relationship between online and offline organised crime, there are two possibilities: an increase in online organised crime may be associated with either an increase or a decrease in criminal activity in real world terms. For example, this is a moot point in the study of child sex offenders: does the consumption of child abuse material online ameliorate or exacerbate actual contact child-related sex offending? This is a long-standing observation in the social sciences with regard to niche or obscure tendencies, whereby prior to the invention of the Internet, those involved would have had difficulty finding other persons with similar interests and collaborating.

In the context of the Internet Organised Crime Threat Assessment, the most relevant cyberpsychological concepts include:

- Anonymity and self-disclosure²⁸⁶
- Cyber immersion²⁸⁷/presence²⁸⁸
- Self-presentation online²⁸⁹
- Pseudoparadoxical privacy^{290 291}
- Escalation online²⁹²
- Impulsivity and problematic Internet use²⁹³
- Dark tetrad of personality²⁹⁴.

283 Walther, J. B. (2009). Theories, Boundaries, and All of the Above. *Journal of Computer-Mediated Communication*, 14(3), 748–752. doi:10.1111/j.1083-6101.2009.01466.x

284 Slane, A. (2007). Democracy, social space, and the Internet. *University of Toronto Law Journal*, 57(1), 81–105. doi:10.1353/tlj.2007.0003, p. 97

285 Europol, *ibid*, p.3.

286 Joinson, A. N. (2001). Self-disclosure in computer-mediated communication : The role of self-awareness and visual anonymity, 192(May 1999), 177–192.

287 Takatalo, J., Nyman, G., & Laaksonen, L. (2008). Components of human experience in virtual environments. *Computers in Human Behavior*, 24(1), 1–15. doi:10.1016/j.chb.2006.11.003

288 Riva, G., Mantovani, F., Capideville, C. S., Preziosa, A., Morganti, F., Villani, D., ... Alcañiz, M. (2007). Affective interactions using virtual reality: the link between presence and emotions. *Cyberpsychology & Behavior : The Impact of the Internet, Multimedia and Virtual Reality on Behavior and Society*, 10(1), 45–56. doi:10.1089/cpb.2006.9993

289 Gibbs, J. L., Ellison, N. B., & Heino, R. D. (2006). Self-Presentation in Online Personals: The Role of Anticipated Future Interaction, Self-Disclosure, and Perceived Success in Internet Dating. *Communication Research*, 33(2), 152–177. doi:10.1177/0093650205285368

290 Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday*, 11(9), 1–11

291 Mc Mahon, C., & Aiken, M. (2014b). [Privacy as identity territoriality: Re-conceptualising behaviour in cyberspace](#). Dublin, Ireland

292 White, R. W., & Horvitz, E. (2009). [Experiences with web search on medical concerns and self-diagnosis](#). *AMIA... Annual Symposium Proceedings / AMIA Symposium*. AMIA Symposium, 2009, 696–700

293 Mottram, A. J., & Fleming, M. J. (2009). Extraversion, impulsivity, and online group membership as predictors of problematic Internet use. *Cyberpsychology & Behavior : The Impact of the Internet, Multimedia and Virtual Reality on Behavior and Society*, 12(3), 319–21. doi:10.1089/cpb.2007.0170

294 Buckels, E. E., Trapnell, P. D., & Paulhus, D. L. (2014). Trolls



In addition to the above cyberpsychological constructs, attention should also be paid to the impact of technology on clinical psychological conditions. For example, disruptive, impulse-control and conduct disorders are known to have real world offline forensic implications²⁹⁵, but research is required to further our understanding of their online manifestations.

Classification of cybercrime

New technologies present ever-increasing numbers of cybercrime opportunities from geotagging apps, to information harvested from social networking platforms. Schlinder²⁹⁶ observes that “*computer networks...done for criminals the same thing they’ve done for legitimate computers users: made the job easier and more convenient.*”

Technology has facilitated historical crimes such as fraud, and evolving crimes such as online child-related sex offending. Kirwan and Power²⁹⁷ classify cybercrime as two distinct categories *Internet enabled crime* such as fraud, and *Internet specific crime* which includes recent crimes such as hacking. Cybercrime is a growing problem in the modern world, from online sexual exploitation of children to cyber terrorism. In considering the threat landscape however, we should note both the benefits and risks of what is likely to be an increasingly mediated, ubiquitous computing social environment. While the barriers to participation in crime are likely to be reduced, at the same time we are fast approaching the point whereby every crime will leave a digital trace. The phrase ‘all crime is cybercrime’ is a useful one²⁹⁸ as it puts us in

the mind frame of thinking ‘digital first’ and, given the continued development of cloud computing storage, it will be increasingly difficult for digital trace evidence to be entirely removed from a crime scene.

Profiling cybercriminals

In 1956, James Brussel provided one of the best known and accurate profiles, that of the New York Bomber, George Metesky. Criminal profiler Paul Britton²⁹⁹ expanded on profiling literature in the 1990s, as did Douglas and Olshaker³⁰⁰. Canter has contributed to the science of profiling over two decades. Bednarz labelled criminal profiling as “a promising but immature science”³⁰¹, however in the last two decades substantial progress has been made. Findings range from a *psychoanalytic approach* describing hacking behaviour as a psycho-sexual urge in young men, a cathartic outlet³⁰², to *Investigative Psychology’s* statistical interpretation regarding geographical profiling of criminal patterns³⁰³.

Allison and Kebbell³⁰⁴ maintain that there are two assumptions that inform criminal profiling methodology, the ‘consistency assumption’ (i.e. behaviour of an offender will remain reasonably consistent) and the

Analyst Service Annual Conference. Dublin, Ireland.

299 Britton, P. (1997). *The Jigsaw Man*. London: Corgi.

300 Douglas, J., & Olshaker, M. (1999). *The Anatomy of Motive*. London: Simon & Schuster.

301 Bednarz, A. (2004), [Profiling cybercriminals: A promising but immature science](#)

302 Taylor, P. A. (2003) ‘Maestros or misogynists? Gender and the social construction of hacking’, in Y. Jewkes (ed.) *Dot.cons: Crime, Deviance and Identity on the Internet*. Cullompton, Devon (UK): Willan Publishing.

303 Canter, D., & Youngs, D. (2009). *Investigative Psychology: Offender Profiling and the Analysis of Criminal Action*. Chichester: Wiley

304 Allison, L., & Kebbell, M. (2006). *Offender profiling: Limits and potential*. In M. Kebbell, & G. Davies (Eds.), *Practical Psychology for Forensic Investigations and Prosecutions*. Chichester: Wiley.

just want to have fun. *Personality and Individual Differences*. doi:10.1016/j.paid.2014.01.016

295 American Psychiatric Association (2013). *Diagnostic and Statistical Manual of Mental Disorders* (Fifth ed.). Arlington, VA: American Psychiatric Publishing. ISBN 978-0-89042-555-8.

296 Shinder, D. (2010). [Profiling and categorizing cybercriminals](#)

297 2012, *ibid*.

298 Mc Mahon, C. (2013). All crime is cybercrime. An Garda Síochána

'homology assumption' (offence style will reflect offender characteristics). However Kirwan and Power³⁰⁵ point out that as technology changes therefore there may also be changes in criminal behaviour, thus presenting a challenge to the consistency assumption. In terms of the homology assumption, given the role of anonymity in cyber contexts can we be certain that offender characteristics will remain uniform, not only between real worlds and virtual worlds but essentially between one cybercrime and another? Again, this is an area in which anthropological work may prove useful (e.g. the work of Gabriella Coleman with regard to the hacking community³⁰⁶). According to Professor Rogers, the real challenge is to understand behavioural motivation concerning cybercrime *"Like in traditional crimes... try to understand what motivates these people to get involved in computer crimes in the first place, how they choose their targets and what keeps them in this deviant behavior after the first initial thrill."*³⁰⁷

Theories of crime aim to provide explanatory value regarding criminal behaviour and therefore may also help to inform the psychology of cybercrime. *The Psychology of Cyber Crime: Concepts and Principles*³⁰⁸ lists important theories of crime as follows; biological theories, labelling theories, geographical theories, routine activity theory, trait theories, learning theories, psychoanalytic theories, addiction and arousal theories and so forth. However concerning the application of theories of crime to cybercrime, an important question is as follows; are real world criminal and psychological theories applicable in virtual environments, do we need to modify them, or develop new theories?³⁰⁹ To date there is a paucity of research regarding how these established theories can be applied to cybercrime, and more importantly if it is methodologically correct to do so. In fact a fundamental problem may exist regarding methodology - can theoretical scales or metrics developed and validated offline be empirically employed whilst investigating criminal behaviour manifested online? A recent report "A primer on research in mediated environments: Reflections on cybermethodology"³¹⁰ considers this very issue.

Given the complex and changing nature of both the technology and the legal landscape, it is difficult to profile

the 'typical cyber criminal'. However, we can point to certain behavioural and psychological factors which are of interest. Former police officer and criminal justice instructor, Shinder³¹¹, for example, notes in 2010 that we should bear in mind at least some degree of technical knowledge (ranging from 'script kiddies' who use others' malicious code, to very talented hackers), though again this barrier is likely to continue to fall. In addition, Shinder notes a certain disregard for the law or rationalisations about why particular laws are invalid or should not apply to them, a certain tolerance for risk, the possibility of a 'control freak' nature, and enjoyment in manipulating or 'outsmarting' others. In terms of motive, Shinder lists monetary gain, emotion, political or religious beliefs, sexual impulses, or even boredom or the desire for 'a little fun.' While these factors are obviously linked to traditional or real world crime, what is not yet clear is whether cybercrime has the same associations or etiology. What is interesting from a cyberpsychological perspective are the behavioural, experiential, and developmental aspects of individual motive. There is a considerable gap in our knowledge regarding the cyberpsychological evolution of how individuals (who may or may not have a criminal history) become incorporated into organised cybercrime. Critical in this regard is the understanding of motive: transition from initial motive to sustaining motive, overlapping motives, and the prediction of evolving motives, along with an understanding of primary and secondary gains.

Future trends and threat assessment

One of the most urgent areas requiring research and investigation is the classification of cybercrime; to date there has been a tendency to simply name apparent 2.0 versions by simply adding the prefix cyber. Are bullying and cyber bullying the same underlying condition, and importantly is the literature on cyberbullying prior to the advent of the smartphone still relevant? Do real world stalkers and cyberstalkers share the same deviant tendencies? Is cyberstalking simply facilitated by technology, or is it a new and differentiated form of criminal behaviour? In the latter, observed differences are as follows; emergence of more female stalkers, stalking of multiple victims simultaneously, and the ability of the stalker to access more personal data of the victim³¹². Current problems regarding cybercrime are well established; hacking, malware production, identity theft, online fraud, child abuse material, online child solicitation, cyberstalking, cyberbullying, IP theft/software piracy, botnets, data breaches, organised cybercrime, ransomware and sextortion – however given the dynamic nature of the environment it is important to consider future

305 Kirwan & Power, 2012, *ibid*.

306 Coleman, E. G., & Golub, a. (2008). Hacker practice: Moral genres and the cultural articulation of liberalism. *Anthropological Theory*, 8(3), 255–277. doi:10.1177/1463499608093814

307 Bednarz, A. (2004), [Profiling cybercriminals: A promising but immature science](#)

308 Kirwan & Power, 2012, *ibid*.

309 Barak, A., & Suler, J. (2008). Reflections on the psychology and social science of cyberspace. In A. Barak (Ed.), *Psychological aspects of cyberspace: Theory, research, applications*, 1–12. Cambridge, UK: Cambridge University Press.

310 Mc Mahon, C., & Aiken, M. (2014a). [A Primer on Research in Mediated Environments: Reflections on Cybermethodology](#)

311 Shinder, D. (2010). [Profiling and categorizing cybercriminals](#)

312 Berry, M. J., Bainbridge, S., & Aiken, M. P. (2011). Cyber stalking in 18-30 year olds in Manchester. Paper presented at the International Crime, Media & Popular Cultures Conference, Indiana State University, US. 26th - 28th September 2011.

trends and put in place a strategy to deal with them. Some future trends, threats and developments for consideration are briefly discussed below:

Cybernetic crime evolution

From a technical perspective, we can expect that there will be an increased **volume of attacks** in comparison to defence capabilities. As Maughan states:

“the volume of traffic used in DDoS attacks is currently about 400 Gbits per second, but this is increasing rapidly, an increase to 4 Tbits per second could happen and current security solutions cannot handle this. There is a need to develop new defences and tools for DDoS attacks, the best product is 15 years old.”³¹³

Increasing human immersion in **cyber physical systems** is a concern for example; houses, cars, and smart cities - such systems have software that can be compromised and are often designed without cyber security in mind³¹⁴. An additional threat posed to cyber security is the **security workforce shortage** - disconcerting when considered in the context of the increased technology skills of criminal populations. Emboldened organised crime **incentivising and recruiting criminal population** is another cause for concern, exemplified by the deep web offer of a Ferrari as a prize for the hacker who ‘dreams up the biggest scam’³¹⁵. **Financial obscurity** - Bitcoin, Dogecoin, Litecoin, etc - there are ever increasing ways for criminals to launder money online. Distribution of malware via **social engineering** tactics is another evolution; that is the infecting of users by perceived trusted sources. **Cyber propaganda** is increasing; that is the gamed use of social media platforms for propaganda purposes and cyberterrorism³¹⁶.

Consequently, there is likely to be a **wider opportunity base** for organised cybercrime, to the point that we expect to see ‘next generation’ sophisticated cyber organisations of significantly increased size, complexity, reach, and confidence. Essentially, there is considerable room for growth for cybercriminal organisations of unprecedented scale, which will present significant challenges to law

enforcement. In a behavioural context, we expect that such cybercriminals may attempt to justify their activities as ideological in nature (note the libertarian philosophy behind the Silk Road³¹⁷). Additionally, we note the following behavioural threats and trends.

Psychological obsolescence: the disruptive impact of technology on youth development is likely to produce a cultural shift which may leave present psychological, social and cultural norms behind, including respect for property rights, privacy, national security, and the authority of law enforcement. What is the prognosis for a generation inured by the consumption of illegally downloadable music, videos software and games? What sort of criminal activities may this generation of ‘virtual shoplifters’ progress to? This is even before we consider more serious threats, such as the environmental developmental effects on those spending large amounts of time in deep web contexts, those exposed to age-inappropriate sexual content online³¹⁸, or those vulnerable to radicalisation online, by cyber terrorist interests.

Cyber criminal sensemaking of Big Data: While there has been a massive increase in the production of data, very little of it is getting analysed, yet at the same time the economic value of personally identifiable information is growing rapidly. This particular analytic gap in itself represents a criminal opportunity.

Ubiquitous victimology: the public need to be aware that increasingly, no matter where they are or what they are doing, they may be at risk of serious organised crime. This is because of the increase in mobile and wearable technologies, which may not have the same level of security features as laptop or desktop devices. In fact, given that mobile devices can now both store large amounts of sensitive information, as well as access cloud storage, the average device-carrying member of the public could now be considered forensically a high-risk victim in a cybersecurity context. This premise is supported by Maughan³¹⁹, noting that:

Mobile devices present a growing challenge in cyber security. The numbers of devices is predicted to double in 5 years. The security of devices is a problem - all device types have been compromised. The security of software on mobile devices is also a concern, along with security issues in apps, many of these store usernames and passwords are vulnerable to man-in-the-middle attacks (p. 6).

313 Maughan, cited in Belfast 2014, *ibid.*, p. 6.

314 Maughan, cited in Belfast 2014, *ibid.*, p. 6

315 Peachey, P., (2014). [Cybercrime boss offers a Ferrari for hacker who dreams up the biggest scam](#)

316 Berger, J. M. (2014). [The Atlantic: How ISIS Games Twitter](#)

317 Olson, P. (2013). [The man behind Silk Road – the internet’s biggest market for illegal drugs](#)

318 [Internet Content Governance Advisory Group Report, 2014](#)

319 Belfast 2014, *ibid.*

In addition, this problem will likely be further exacerbated by the ‘blurring of boundaries between corporate and private life’³²⁰ exemplified by the bring-your-own-device (BYOD) practices increasingly common in corporate life. Furthermore, the IoT presents a variety of additional attack surfaces to organised cybercriminals.

Cyberpsychological insight

As discussed, a key perspective is to consider cyber space as an immersive, as opposed to transactional entity, to consider cyberspace as an actual environment, and address the ‘minimisation and status of authority online’³²¹. The challenge for technology is perhaps to create an impression that there are consequences for the criminal use of technologies, and to develop *digital deterrents* targeting cyber criminals, and *digital outreach* protocols supporting victims. In that light, it is advisable for law enforcement authorities to have increased visibility or presence online. The most promising areas for multi-disciplinary cyberpsychologically-informed research to provide insight to law enforcement organisations tackling Internet-facilitated organised crime are as follows:

1. investigation of the role of social and psychological issues in the lifespan development of an individual into serious organised cybercrime
2. empirical exploration of the dynamic relationship between the real world and virtual world from a serious crime perspective
3. methodologically ‘factoring the criminal’ as a human into the digital forensic investigative process
4. development of a robust typology of organised cybercrime and cybercriminals
5. analysis of cybernetic crime evolution, structure and syndication
6. risk assessment of ubiquitous victimology.

Cyberpsychology research vision is focused on understanding new norms of behaviour online, and to consolidate them with or differentiate them from existing real world behaviours, and in doing so deliver insight. A theoretically profound, experimentally rigorous, developmentally longitudinal, and technically sophisticated research approach is required to achieve long-lasting positive societal effects, along with cooperation between academia, law enforcement and industry - in fact, all parties that have an interest in developing safe and secure societies.

Affiliations

- Mary Aiken, Director RCSI CyberPsychology Research Centre
- Sensemaking Fellow IBM Network Science Research Center
- Fellow Middlesex University School of Law
- Ciarán Mc Mahon, Ph.D., Research & Development Co-ordinator, RCSI CyberPsychology Research Centre

³²⁰ Europol 2011, *ibid*.

³²¹ Suler 2004, *ibid*.



EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

The Internet Organised Crime Threat Assessment (iOCTA)

APPENDICES

A4. The fight against cybercrime through the lens of a data protection believer – a commentary

Personal data is the new commodity driving much of today's cybercrime. It can be reasonably argued that data protection and the fight against cybercrime go hand in hand. Due protection of information relating to identified or identifiable natural persons is a prerequisite for avoiding identity theft and other forms of cybercrime.

However, efforts of law enforcement to prevent and combat cybercrime are sometimes also regarded with suspicion. In this context data protection principles serve as a safeguard against undue and disproportionate forms of government surveillance.

Europol's data protection regime as a law enforcement gold standard

Europol is proud to have one of the most robust data protection frameworks in the world of law enforcement. This is an asset, and at the same time a responsibility, as the legal regime needs to be put into practice and applied in day-to-day operations.

Prominent features of Europol's solid data protection framework are independent data protection supervision, Europol's secure information exchange capabilities, data protection compliant outreach to the private sector and – most importantly - clearly defined purpose specifications for processing operations upon personal data in Europol's databases.

Europol receives information from Member States obtained in the course of investigations on individual criminals or organised criminal groups. Contributions are tailored and respect the purpose limitation principle. They are used in specifically defined analysis projects subject to strict data retention regimes.

The Data Protection Office of Europol has the task of ensuring that the applicable data protection legal

framework is duly complied with. This is done – inter alia – by providing advice, guidance and best practice on personal data processing.

External supervision is carried out by the Joint Supervisory Body (JSB) which comprises experts from all 28 Member States with particular expertise in the area of law enforcement. Also, any form of future supervision under the regime of a Europol Regulation will certainly build on the elements of independency, transparency and expertise.³²²

The particular role of EC3 and the future Europol Regulation

EC3 remains the centre within the Operations Department of Europol which runs the highest number of projects deserving careful consideration from a data protection perspective. This is due to their innovative nature which reflects the fact that cybercrime as such is a particularly dynamic field. The success of EC3 is also based on the fact that no major data protection issues have occurred.

An organisation like Europol is dependent on a good data protection reputation also because it cannot conduct its own investigations. Europol's role is limited to supporting the EU Member States and facilitating their actions. This is why it is crucial that national authorities trust Europol and consequently provide the organisation with data they have lawfully obtained at national level

As far as citizens are concerned it is important to stress that European law enforcement agencies in general, and Europol in particular, do not engage in any form of mass

³²² See Drewer, D. / Ellermann, J., Europol's data protection framework as an asset in the fight against cybercrime, In: ERA Forum (2012) 13, P. 381-395 for a more comprehensive description.



surveillance as discussed in the context of the Snowden revelations. The debate on a good balance between security and privacy is, however, of utmost relevance also to the European Police Office (Europol) including EC3. This is last but not least with a view to the ongoing legislation on a future Europol Regulation. Europol needs the tools to effectively prevent and combat serious crime and terrorism.

In particular, the ever increasing threat posed by cybercrime calls for an open discussion on what law enforcement should be allowed to do online and where the boundaries need to be drawn. Rules on public-private partnership need to be reviewed in order to make cooperation between companies and law enforcement more efficient. As a matter of fact it is not only the security services taking advantage of the Internet and our modern means of communication – cybercriminals do the same with far worse intentions.

The broader perspective

The current debate on the relationship between data protection and the fight against cybercrime certainly goes well beyond the scope of EC3 operations or the future Europol Regulation. An example is the recent landmark ruling by the European Court of Justice (ECJ) issued on 8 April 2014. It demonstrates that processing of bulk data for law enforcement purposes remains a very sensitive issue. In this ruling the court declared Directive 2006/24/EC - better known as the Data Retention Directive - to be invalid. The court found that the directive entails a wide-ranging and particularly serious interference with the

fundamental rights to respect for private life and to the protection of personal data, without that interference being limited to what is strictly necessary.

It is interesting to note that the ECJ clearly acknowledged that the fight against serious crime constitutes an objective of general interest and that the Charter of Fundamental Rights of the European Union not only lays down the right of any person to liberty but also to security. The court held that the retention of data for the purpose of allowing the competent national authorities to have possible access genuinely satisfies an objective of general interest. However, the ECJ ruled that, by adopting the Directive as it stands today, the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality.³²³ In the end this ruling is just another effort to strike the right balance between freedom and security by playing the ball back into the field of the European legislator.

The present iOCTA provides a comprehensive overview on cybercrime related developments as well as on inherent challenges for law enforcement. It may hence serve as an important contribution to the necessary broader societal discussion on where to draw the lines.

At Europol we have a track record of implementing data protection in a way which respects both operational business needs and fundamental rights of individuals. We will do our best to keep it like this and, yes – we are pretty proud of this!

³²³ ECJ, (2014), [Joined Cases C-293/12 and C-594/12](#)

PHOTO CREDITS

All images are © Europol

© Shutterstock: Chapters 3.1a, 3.1c, 3.2a, 3.3a, 3.3c, 3.4a, 3.4c, 3.5a, 3.5c, 3.6c, 3.7c, 3.8c, 4.1a, 4.2a, 4.4.1a (2nd), 4.4.2a, Appendix A2 (1st), all chapter headers and background images.

© Fotolia: Chapters 3.2c, 3.6a, 4.3a, 4.4.1a (1st), 4.4.1c, Appendix A2 (2nd).

© iStock: Chapter 3.8a.



Eisenhowerlaan 73
2517 KK The Hague
The Netherlands

PO Box 90850
2509 LW The Hague
The Netherlands

Website: www.europol.europa.eu
Facebook: www.facebook.com/Europol
Twitter: [@Europol_EU](https://twitter.com/Europol_EU)
YouTube: www.youtube.com/EUROPOLtube

<https://t.me/learningnets>