UDK:004-049.6:343.525
004-049.6:343.721

SECURING CYBERSPACE – COMBATTING CYBER FRAUD AND ONLINE IDENTITY THEFT

Detective Inspector Andrew Staniforth
Head of West Yorkshire for Innovation, West Yorkshire Police and Office of the Police & Crime Commissioner for West Yorkshire (UK)
Andrew.Staniforth1@westyorkshire.pnn.police.uk
Francesca Barrett
Project Delivery Officer, West Yorkshire for Innovation, Office of the Police & Crime Commissioner for West Yorkshire (UK)
Francesca.Barrett@westyorkshire.pnn.pcc.uk

ABSTRACT

Online activities have now become central to the very way in which millions of people across the world live their lives. While the Internet has positively enriched societal communications and economic opportunities, these technological advancements have changed – and continue to change – the very nature of crime, serving to breed a new sophisticated and technically capable criminal and terrorist. The scale of contemporary cybercrime is significantly challenging the capacity and capability of even the most sophisticated Law Enforcement Agencies (LEAs). Of critical concern to authorities is the continued rise of cyber fraud which has now become the most prevalent crime within numerous European Member States, with people ten times more likely to become a victim than they are to suffer a traditional theft. To tackle the phenomenon of cyber fraud and online identity theft, police officers, academics and private industry partners have joined forces through project ARIES (reliAble euRopean Identity EcoSystem), funded by the Horizon 2020 Secure Societies programme of the European Commission, which seeks to achieve a reduction in levels of identity fraud, identity theft and other related cybercrimes by creating a new system to improve the security of personal online data. This paper explores the new and emerging threats from cyber fraud and identity theft and examines how project ARIES will design a new system to prevent impersonation and reduce types of identity fraud and identity-related crimes which is recognised a major vulnerability in securing cyberspace and combatting contemporary organised crime and international terrorism.

1. INTRODUCTION

Online activities have now become central to the very way in which millions of people across the world live their lives. While the Internet has positively enriched societal communications and economic opportunities, these technological advancements have changed – and continue to change – the very nature of crime, serving to breed a new sophisticated and technically capable criminal. The nature of some 'traditional' crime types have been transformed by the use of Information Communications Technology (ICT) in terms of their scale and reach, with threats and risks now extending to many aspects of social life. New forms of criminal activity have also been developed, targeting the integrity of computers and computer networks. Threats exist not just to individuals and businesses, but to national security and critical infrastructures. Furthermore, the borderless nature of

the phenomenon of cybercrime means that any citizen, community or country, can be targeted from any jurisdiction across the world. The purpose of this paper is to explore the current cybercrime threats and their impact on society from Law Enforcement Agency (LEA) perspectives, spotlighting the operational challenges of combatting cyber fraud and online identity theft and recommending measures required to meet the contemporary cybercrime challenge of keeping people safe online.

2. ORGANISED CYBER CRIMINALITY

The scale of contemporary cybercrime is significantly challenging the capacity and capability of even the most sophisticated LEAs. By its very nature, cybercrime has a far-reaching trans-national dimension which substantially increases the complexity beyond the detection of other crimes. It is a type of crime that has been embraced by criminals who are now working together in what is a new era of collaboration and coordination of organised cybercrime. According to Europol, there are an estimated 3,600 Organized Crime Groups (OCGs) active in the European Union (EU) [1]. These groups are becoming increasingly networked in their organization and behaviour, characterized by a group leadership approach and flexible hierarchies [2]. The advances in international trade, an ever-expanding global transport infrastructure and the rise of the Internet, have served to engender a more international and inter-connected form of serious and organized crime which has never been seen before. As a direct result, there is an increased tendency for OCGs to cooperate with or incorporate into their membership a greater variety of nationalities. The majority of these cybercriminals will never physically meet, and only communicate to progress their activities in the virtual world of cyberspace. This phenomenon has seen an increase in the number of heterogeneous groups that are no longer defined by nationality, ethnicity, or criminal bonds or kinship. Contemporary criminals act undeterred by geographic boundaries and can no longer be easily associated with specific regions or physical centres of operation [3]. These developments, as part of the relentless rise of organised cybercrime, have caught many LEAs off-guard who remain behind the pace of change from the dynamic and evolving cybercrime threat.

2.1 Changing threat landscape

The cybercrime threat landscape is subject to constant change, development and diversification. As an example, cyber criminals are now streamlining and upgrading their current techniques, while companies and governments struggle to prevent and detect their old tactics. Cyber attackers continue to breach computer networks with highly targeted spear-phishing attacks which are increasing in volume [4]. At the same time, as the development of mobile communications provides a larger attack surface, organised cybercriminals are increasing their volume of mobile malware and rogue mobile applications as half of the world's adult population now own a smartphone [5]. The technological advancements of the smartphone have made it the go-to device over the computer, and the one to which people are always connected. Cybercriminals are increasingly looking to exploit this change in user device preference by switching an expanding proportion of their attacks to mobiles. As a result, more standalone attacks on mobile devices are expected in the future which presents a real and present menace to the individual smartphone user [6]. In addition, future attacks on online payment systems are also expected to rise as their popularity and use grows.An increase in large-scale retail and banking breaches is also anticipated, as cybercriminals seek more efficient and profitable

types of attack [7]. In summary, organised cybercrime threats continue to grow more targeted and more advanced, raising acute concerns for cyber security practitioners.

2.2 A new reality

Cyber security professionals across the world are coming to terms with the uncomfortable truth that private bio-medical identity data is now more valuable to cybercriminals than bank or credit card details. Cybercriminals are currently attacking the healthcare industry at a higher rate than any other sector with more than 100 million healthcare records being compromised in the last year [8]. The sudden rise in the theft of bio data has raised acute concerns for national security practitioners as it now exceeds attacks on manufacturing, financial services, government and transportation industries. The phenomenon of cybercrime has now entered a new era of healthcare hacks where the most intimate aspects of our personal identity data are being stolen.

According to US Government figures from the Department of Health and Human Services (HHS), five large cyber-attacks have recently led to 108.8 million people having their medical records illegally accessed [9]. During 2015 hackers gained access to 80 million personal records kept by Anthem, a health insurance plan provider in the United States. Stolen data included social security numbers, birthdays, addresses, email and employment information and income data for customers and employees, including its own chief executive. The hackers are thought to have infiltrated Anthem's networks by using a sophisticated malicious software program that gave them access to the login credential of an Anthem employee [10]. Anthem officials became aware of the breach when one of their senior administrators noticed someone was using his identity to request information from the database. While working with the Federal Bureau of Investigation (FBI), Anthem officials said they did not know who was responsible for the attack, but the level of sophistication has made cyber security professionals suspicious that the hackers while carrying out their crimes may have been working with the support of a foreign government, or with people with ties to a foreign government. The Anthem cyber-attack is currently the largest known incident of its kind which serves to highlight a worrying trend. In the last year, hackers have gained access to more than 4.5 million medical records from the University College of Los Angeles (UCLA) medical network, including the Ronald Reagan Medical Centre, and 11 million records from the American health insurance company Premera Blue Cross. The rate of attacks against the healthcare sector climbed to the highest level of all industries studied in 2015 and it appears that this pattern is set to continue as data breaches in the healthcare sector are getting larger.

The healthcare sector is an attractive target for personal identity data by the anonymous cybercriminal as compared with other sectors because the healthcare industry's approach to cybersecurity is generally regarded as poor, being amplified by a culture which has neither recognised nor prioritised the real security risk concerning the theft of patients' sensitive data records. Recent cyber security studies across multiple industries have found an alarming laxity in many organisations' approach to data security. A Cyber Security Breaches Survey revealed that two thirds (65%) of large UK businesses were hit by a cyber breach or attack every year [11]. The research also found that almost half of the top FTSE 350 businesses regarded cyber-attacks as the biggest threat to their business, but only a third of the UK's top 350 businesses understand the threat of a cyber-attack [12]. A survey by Sophos during 2016 found that the healthcare sector had one of the lowest rates of data encryption, with only 31% of healthcare organizations reporting extensive use of encryption [13]. A Sophos survey of the National Health Service (NHS) organizations in the UK found that encryption was "well established" in just 10% of them; while a 2016

study of hospital cyber security found that patient health records are "extremely vulnerable" because of a lack of focus on cyber-attacks and insufficient training [14].

Beyond data breaches perpetrated by hackers, health data is frequently exposed through accidental loss, device theft and employee negligence. And it is not just hospitals, doctors' offices and insurance companies that are failing to protect healthcare data – private employers frequently leave their employees' private healthcare information unencrypted. This information is attractive to cybercriminals as it typically contains credit card data, email addresses, social security numbers, employment information and medical history records – much of which will remain valid for years, if not decades. Cyber thieves are using this data to launch spear-phishing attacks, steal medical identities and commit fraud by making false insurance claims. The information that healthcare providers maintain about consumers is now more valuable on the black market than the credit card information that is often stolen from a retailer. Katherine Keefe, global focus group leader for breach response services at Beazley, which underwrites cyber liability policies, states that: "The value to a criminal of having a full set of medical information on a person can go for $40 to $50 on the street. By contrast, a credit card number is often worth $4 or $5" [15].

3. COUNTING THE COST OF CYBERCRIME

The financial impact of cybercrime has quickly become a threat to the economic stability, security and well-being of many nations across the world. The rapid digitalisation of consumers' lives will increase the cost of data breaches to an estimated $2.1 trillion globally by 2019, increasing to almost four times the estimated cost of breaches in 2015 [16]. Figures collated for the Crime Survey of England and Wales for a six-month period during 2016 for the first time included questions about fraud and cyber offences. The results indicated that fraud and computer misuse accounted for 5.8 million crimes, meaning that on average, one in ten adults fell victim to cybercrime [17]. The figures also revealed that when compared to other more traditional crimes, cyber fraud has now become the most prevalent crime in the UK with people ten times more likely to become a victim than they are to suffer a theft.

LEAs continue to be challenged on many fronts in their efforts to protect online users from the volume of cybercrime. Through constant innovation, cybercriminals are developing increasingly sophisticated malware, rogue mobile apps and more resilient botnets. Cyber vulnerabilities – similar to those highlighted in the healthcare sector – remain a big part of the security picture and all the evidence from cybercrime-related threat and risk assessments indicate that the attackers are moving faster than the practical and operational implementation of effective cyber defences and counter measures. This position is unlikely to change and the cyber attackers will continue to have the upper hand unless more can be done to anticipate future threats and risks, which requires the ability to horizon scan for weak signals indicating the early signs of new trends. The current focus of hackers to conduct attacks on the healthcare sector represents another step in the evolution of cybercrime, but there are growing concerns that cybercriminals will seek to steal more citizens' bio identity data through fingerprint, facial and iris recognition data used to confirm identity for security clearance at ports, borders and other critical infrastructures and facilities, adding a new and sinister dimension to the phenomenon of cybercrime. According to academic research and security industry estimates, the rise of cybercrime will continue because criminals are, in reality, just starting to embrace the full extent of the three distinct opportunities created by the internet which includes: more opportunities to

commit traditional crime; new opportunities to commit traditional crime; and new opportunities to commit new types of crime.

4. CRIMINOLOGY PERSEPECTIVES

Understanding cybercrime is the key to kerbing the continued growth of this criminal phenomenon. Many police officers and security policy makers may regard the threats from cybercrime as something relatively new, but its origins can be traced back decades. In 1970, over the course of three years, the Chief Teller at the Park Avenue branch of New York's Union Dime Savings bank manipulated the account information on the bank's computer system to embezzle over $1.5million from hundreds of customer accounts [18]. Cited as one of the very first crimes associated with the misuse of computers, the cunning of the Chief Teller provides evidence of how technological developments have been exploited for criminal gain. From the first introduction of computers in the work place to today's ever-expanding cyberspace, new opportunities have been created for criminals to commit crimes through a set of unique features, features that are described as the 'transformative keys of cybercrime' which includes:

- Globalisation – providing opportunities to exceed conventional boundaries;
- Distributed networks – generating new opportunities for victimisation;
- Data trails – creating new opportunities to commit identity theft [19].

The transformative keys of cybercrime have served to challenge traditional criminological perspectives which have defined crime by social, cultural and material characteristics and have viewed crimes as taking place at a specific geographic location. Such perspectives of crime have allowed for the characterisation of crime, and the subsequent tailoring of crime prevention, mapping and measurement methods to the specific target audience. However, this characterisation cannot be carried over to cybercrime, because the environment in which cybercrime is committed cannot be pinpointed to a geographic location, or to a distinctive social, ethnic or cultural group which adds further complexity to understanding cybercrime and the threat it poses to neighbourhood safety and national security.
Acknowledging the global reach of cybercrime and the requirement to establish a common understanding of the threat and risks posed to multiple countries, the Council of Europe (CoE) adopted its Convention on Cybercrime Treaty, known as the Budapest Convention, which identified several activities to be present as offences of cybercrime. These activities served to shape what elements constituted contemporary cybercrimes and included:

- Intentional access without right to the whole part of any computer system
- Intentional interception, without right, of non-public transmissions of computer data
- Intentional damage, deletions, deterioration, alteration or suppression of computer data without right
- Intentional and serious hindering of the function of a computer system by inputting, transmitting, damaging, deleting, deterioration, altering or supressing computer data
- Production, sale, procurement for use, importation or distribution of devices designed to commit any of the above crimes, or of passwords or similar data used to access computer systems, with the intent on committing any of the above crimes [20].

Despite attempts by authorities to define cybercrime, whose efforts commonly sought to construct a definition designed to protect and indicate violations of the confidentiality, integrity and availability of computer systems, a universally recognised definition of cybercrime remained elusive and presented a real challenge to LEAs across the world. But the sudden and dramatic increase of the sheer volume of varying types of cybercrimes served to shape and inform the collective understanding of cybercrime. When discussing cyber-related crime generally today, there are four recognised different types of cybercrime and they are as follows:

- traditional forms of crime using computers and the tools and services within the cyber domain (i.e. theft and fraud)
- illegal content (i.e. pirated music, indecent images and child pornography)
- crimes unique to electronic networks (i.e. hacking and denial of service attacks)
- crimes unique to cyberspace which threaten physical structures, systems and infrastructures (i.e. manipulation of process control systems to damage power stations and their supply) [21].

5. MEETING THE CYBERCRIME CHALLENGE

To meet the cybercrime challenge, all in authority would be wise to treat cyberspace for what it is; a separate socio-spatial dimension in which people choose not only to communicate, but also to dwell, trade, socialise and cultivate; to create intellectual property, generate economic wealth, to begin and end relationships; to forage, feud and thrive, to heal, harm and steal [22]. Viewed in this way, cyberspace is another continent, vast, viable and virtual, a distinct jurisdiction requiring its own constitution and legal system with its own LEAs and agents. To police this new cyber continent effectively and protect all online citizens and communities requires a dedicated, determined and strategic response. Most importantly, it requires an unprecedented level of cooperation, coordination and collaboration between LEA's and the private sector across the world if authorities are ever going to stem the flow of organised cybercrime and keep citizens, consumers, companies and countries safe in cyberspace.

LEAs now recognise that without adequate protection, personal data and individual identities are vulnerable in a virtual world, and combined with the lack of a coherent and joint approach across Europe (in terms of legislation, cross-border cooperation and policy) to address identity-related crimes, the costs to companies, countries and citizens will continue to rise at an alarming rate. Moreover, LEAs have come to learn that they cannot tackle contemporary threats from crime alone, and they are stronger when they work together with other agencies, departments and sectors including academia and private industry. An excellent example of collaboration to combat cybercrime threats can be found in the multi-disciplinary, pan-European consortium of partners who have joined forces through project ARIES (reliable euRopean Identity EcoSystem), a cybercrime research and innovation project funded by the Horizon 2020 Secure Societies Programme of the European Commission.

The ARIES project brings together professionals from government, academia and the private sector to tackle the phenomenon of cyber fraud and identity theft. The four strategic objectives of ARIES seek to:

i. Achieve a reduction in levels of identity fraud, identity theft and other related cybercrimes by creating a new system to improve the security of personal online data.

ii. Strengthen the link between physical documents linked to biometric identity and the digital (online and also mobile) identity.
iii. Validate the ARIES approach in two high societal and economic impact scenarios that allow proving an effective reduction of identity theft and associated crimes.
iv. Address the key legal, ethical, socio-economic, technological and organisational aspects of identity-related crimes [23].

ARIES will support online users in managing their identities and enable identity derivation mechanisms, allowing users to choose the identity that better suits the online services and digital technologies they use, including the creation of a 'secure electronic wallet' for users to handle their ID-related data in a secure and convenient way in a highly digitised society. ARIES will build an Electronic Identification (eID) ecosystem offering the citizen an efficient and convenient way to manage identities, including the possibility to anchor the trust on a secure and high level of assurance infrastructure that will be used to derive additional virtual identities supporting different levels of privacy preserving and anonymization capabilities. To enhance the capability of LEAs, ARIES will make electronic identity data available to law enforcement without breaking privacy by placing citizen's information needed for enrolment in a secure vault only accessible by police forces and will exchange best practices and promote the new ecosystem advantages for fraud prevention, to law enforcement and security industry partners.

The strategic aim of ARIES is for the system to enable secure, reliable and privacy preserving identity management and derivation techniques to allow a secure user interaction with services and to prevent and reduce the risk of identity theft and fraud crimes. ARIES will provide means for stronger and more trusted authentication, in a user-friendly and efficient manner and with full consideration to data subject's rights for personal data protection. ARIES will also provide means to present a proof of identity without the need to disclose more personal data than actually needed in a given interaction. Figure 1 provides an overview of the ARIES eID ecosystem solution, where interactions between entities are depicted. The user manages several identities and credentials, which are issued by Identity Providers (IdP) and presented to the Service Providers (SP) to access the services offered by them providing increased security of personal identities to reduce the risk of cyber-related fraud [24].

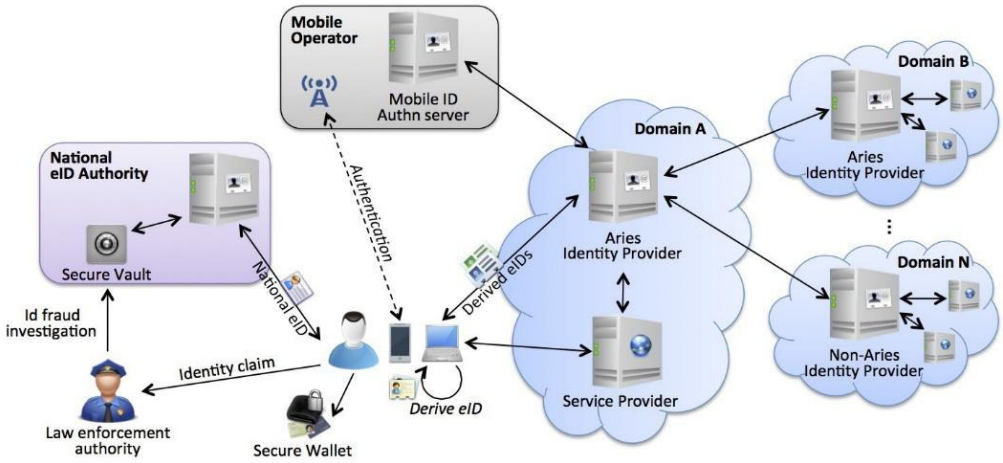

Figure 1 – Overview of the ARIES eID ecosystem

The ARIES approach empowers online users to better protect their identities and personal information. The ARIES vision is therefore to develop and test secure technologies contributing to further establish a European electronic ID ecosystem which is trustworthy for citizen use. For this purpose, ARIES is to design easy-to-use and private-preserving tools dedicated to identity management which will serve to reduce the risk of identity theft leading to cyber fraud.

6. CONCLUSION

The cybercrime landscape continues to evolve as criminals look to adopt more efficient and profitable attack tactics. At the same time, the market for cybercrime-as-a-service is advancing rapidly, with competition among malware vendors leading to increased criminal innovations. The most significant change in the cybercrime threat landscape is the increasing use of smart mobile devices. Mobility provides a larger attack surface for cybercriminals to operate and the volume of mobile malware and rogue mobile apps is increasing as half the world's adult population now owns a smart mobile device which has amplified the risks of identity theft and cyber fraud. As cybercrime threats continue to grow more targeted and more advanced, of pressing concern to security policy-makers is the rise of organised cybercrime. Criminal groups are expected to adopt nation-state tactics as they realise the full potential of cybercrime. This approach will result in large enterprises and other organisations becoming increasingly vulnerable through their use of commodity equipment, which attackers quickly learn how to bypass, so defending against these attacks and identifying perpetrators will be a real challenge for the police and private industry.

The rise of cybercrime reveals that the cyber threat landscape is subject to constant change with far-reaching vulnerabilities, faster attacks, files held for ransom and the continued presence of data breaches. Cyber vulnerabilities remain a big part of the security picture and all the evidence from cybercrime-related threat and risk assessments indicate that cyber criminals are moving faster than the practical and operational implementation of effective cyber defences and counter measures. Unfortunately, this pattern is unlikely to change and cyber criminals will continue to have the upper hand, but by working together, sharing challenges and expertise, LEAs, academics and representatives from the private sector can, through applied research, development and

innovation, design and develop new tools and technologies to combat pressing threats from all manner of cybercrimes. The approach and preventative ethos of project ARIES provides one such example of how collaboration in the prevention of cybercrime can fill the lacuna in current operationally-focused cybercrime research and innovation. Advances in, and the amplification of, multi-disciplinary cybercrime research, is absolutely essential as all in authority would be wise to recognise that the phenomenon of cybercrime remains in its infancy and represents the dawn of a new era of criminality – the future of crime has arrived.

1. Europol, The Internet Organised Crime Threat Assessment Report (2015) https://www.europol.europa.eu/sites/default/files/publications/europol_iocta_web_2015.pdf (accessed on 12/12/16)
2. Europol, The Internet Organised Crime Threat Assessment Report (2015) https://www.europol.europa.eu/sites/default/files/publications/europol_iocta_web_2015.pdf (accessed on 12/12/16)
3. Brown, S D. Combatting International Crime: The Longer Arm of the Law (2008) Oxon: Routledge-Cavendish
4. Symantec, 2016 Internet Security Threat Report (2016) https://www.symantec.com/security/center/threat-report (accessed on 5/1/17)
5. Symantec, 2016 Internet Security Threat Report (2016) https://www.symantec.com/security/center/threat-report (accessed on 5/1/17)
6. EMC, The current state of cybercrime 2014 – An inside look at the changing threat landscape (2014) https://www.emc.com/collateral/white-paper/rsa-cyber-crime-report-0414.pdf (accessed on 15/12/16)
7. EMC, The current state of cybercrime 2014 – An inside look at the changing threat landscape (2014) https://www.emc.com/collateral/white-paper/rsa-cyber-crime-report-0414.pdf (accessed on 15/12/16)
8. Sophos, Cybercrime Healthcare Report: Why cybercriminals attack healthcare more than any other industry (2016) https://nakedsecurity.sophos.com/2016/04/26/why-cybercriminals-attack-healthcare-more-than-any-other-industry/ (accessed on 3/12/16)
9. Daily Mail, Cyber attackers hacked private medical records (2015) http://www.dailymail.co.uk/news/article-3372890/Cyber-attackers-hacked-private-medical-records-100-MILLION-people-2015.html (accessed on 12/1/17)
10. New York Times, Experts suspect lax security left Anthem vulnerable to hackers (2015) http://www.nytimes.com/2015/02/06/business/experts-suspect-lax-security-left-anthem-vulnerable-to-hackers.html?_r=0 (accessed on 21/12/17)
11. UK Government, Cyber security Breaches Survey 2016 (2016) https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/521465/Cyber_Security_Breaches_Survey_2016_main_report_FINAL.pdf (accessed on 29/11/16)
12. UK Government, Cyber security Breaches Survey 2016 (2016) https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/521465/Cyber_Security_Breaches_Survey_2016_main_report_FINAL.pdf (accessed on 29/11/16)

13. New York Times, Experts suspect lax security left Anthem vulnerable to hackers (2015) https://nakedsecurity.sophos.com/2016/04/26/why-cybercriminals-attack-healthcare-more-than-any-other-industry/ (accessed on 9/1/17)
14. Sophos, Cybercrime Healthcare Report: Why cybercriminals attack healthcare more than any other industry (2016) https://nakedsecurity.sophos.com/2016/04/26/why-cybercriminals-attack-healthcare-more-than-any-other-industry/ (accessed on 18/12/16)
15. New York Times, Experts suspect lax security left Anthem vulnerable to hackers (2015) http://www.nytimes.com/2015/02/06/business/experts-suspect-lax-security-left-anthem-vulnerable-to-hackers.html?_r=0 (accessed on 18/12/16)
16. Office of the National Statistics, UK Government, British Crime Survey: Crime in England and Wales – year ending June 2016 (2016) https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingjune2016 (accessed on 18/1/17)
17. Office of the National Statistics, UK Government, British Crime Survey: Crime in England and Wales – year ending June 2016 (2016) https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingjune2016 (accessed on 18/1/17)
18. Cybercrime Final Project: The dark side of modern technology (2014) https://sites.google.com/site/cybercrimefinalproject/ (accessed on 9/1/17)
19. Wall, D S. Cybercrime: The Transformation of Crime in the Information Age (2007) Cambridge: Polity Press
20. Council of Europe, Budapest Convention on Cybercrime (2004) https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 (accessed on 30/11/16)
21. Wall, D S. (2007). Cybercrime: The Transformation of Crime in the Information Age. Cambridge: Polity Press
22. Sampson, F (2014) Chapter 14 Cyberspace: The new frontier for policing? Cyber Crime and Cyber Terrorism Investigator's Handbook. London: Elsevier.
23. Notario, N ARIES project proposal (2015) Horizon 2020, Executive Research Agency, European Commission, Work Programme Topic: FCT-9-2015, Proposal Final ID: 700085
24. Notario, N ARIES project proposal (2015) Horizon 2020, Executive Research Agency, European Commission, Work Programme Topic: FCT-9-2015, Proposal Final ID: 700085