Article - Ambassadeurs de la Jeunesse - @ October 21, 2019

Ambassadeurs de la Jeunesse

Combating organised crime: The analysis, effects, and control of crimes committed by means of the emerging Dark Net

*By **Alexandru-Ionuț Săndoiu,***
Analyst, Digital & New Technologies
Centre International de Recherche & d'Analyse (C.I.R.A), Ambassadeurs de la Jeunesse

The opinions expressed in this text are the sole responsibility of the author

How to cite this publication :
Alexandru-Ionuț Săndoiu,
« Combating organised crime: The analysis, effects, and control of crimes committed by means of the emerging Dark Net »,
Ambassadeurs de la Jeunesse, October 21, 2019.

Ambassadeurs de la Jeunesse
31 Rue de Poissy 75005 Paris
E-mail : contact@ambassadeurs-jeunesse.org
Site internet : www.ambassadeurs-jeunesse.org

Summary

ABSTRACT

Modern technologies have definitely improved many aspects of life by increasing the speed of information processing, but these modern technologies have become a proxy for committing crimes and nowadays, the emergence of cybercrime has become a phenomenon that hundreds of governments are challenged to control, for instance, the challenge to combat the crimes committed through the infamous Dark Net. The objectives of this research study are to provide an understanding of cybercrime by analysing the way the Dark Net operates, to provide an in-depth analysis of what kind of crimes are committed via the Dark Net, to analyse the effects of this "cybercrime venue" from an international perspective and how law enforcement agencies address this issue, and to identify suitable methods of prophylaxis. There will be a focus on the link between two controversial offences: that of human trafficking and child pornography. Therefore, the research question encompasses the aforementioned objectives – "How does this criminal venue fuel human trafficking and child pornography, and what can law enforcement improve in order to provide a better prophylaxis of such crimes?".

Alexandru-Ionuț Săndoiu
He is a graduate of the University of Essex, School of Law, with an LLB in Law with Business. He is currently a student at the University of Vienna, pursuing an LLM in European and International Business Law. He does research in Criminal Law, Cybercrime, Corporate Law and Intellectual Property Law. His most recent publication is « How does judicial review tangibly protect the rights of citizens? »

CHAPTER ONE

WHAT IS CYBERCRIME? WHAT IS THE DARK NET?

This research paper has the objectives of providing an understanding of cybercrime by analysing the way the Dark Net operates. It will provide an in-depth investigation of the effects of this "cybercrime venue" from both domestic and international perspectives, with a strong focus on the link between human trafficking and child pornography. The research question encompasses the aforementioned objectives: "How does this criminal venue fuel human trafficking and child pornography, and what can law enforcement improve in order to provide a better prophylaxis of such crimes?". The key terms that will be used throughout this research paper will be "cybercrime", "Dark Net", and "organised crime".

"Cybercrime" refers to crimes where the offender uses special knowledge in order to engage in crime on cyberspace, while "computer crime" refers to crimes where the offender possesses knowledge about computer technology and such criminal activity is tailored strictly on actions which fall under the umbrella term of "computer misuse".[1]

"Dark Net", or "Dark Web" represents a portion of the internet which is not accessible without a special encryption software. TOR (The Onion Router) is a free proxy and encryption protocol which gives the user anonymity while surfing various pages on the hidden internet[2]. "Hidden

[1] Thomas J. Holt, Adam M. Bossler and Kathryn C. Seigfried-Spellar, *Cybercime and Digital Forensics: An Introduction* (2nd edition, Routledge 2018) 11.

[2] *Ibid*., 6.

internet" is a term which refers to websites which are not readily accessible, as they are not indexed by common search engines[3].

"Organised crime" can be defined as serious crime planned, coordinated and conducted by people working together on a continuing basis. Their motivation is often, but not in all cases, financial gain. Organised criminals working together for a particular criminal activity or activities are called an "organised crime group"[4]. By statute, a person participates in the criminal activities of an organised crime group if the person takes part in activities that the person knows or suspects that they are criminal activities of an organised crime group, or will help an organised crime group carry out criminal activities[5].

Because modern technologies have, in the last two decades, become a proxy for committing crimes, the emergence of cybercrime has become a phenomenon that hundreds of governments are challenged to combat. This research question addresses two of the most controversial offences, that of human trafficking and child pornography. The research question will be answered through prisms which illustrate the importance, the need to combat and prevent such criminality. Regardless of the subject matter, risk of detection from law enforcement is much lower in online environments than in the real world. Taken as a whole, the global reach of the internet has created substantial difficulties for domestic and international law enforcement agencies to properly impose cybercrime laws and find methods of combatting such an issue which has proven to become one of the most complicated threats nowadays[6].

The research paper is structured in five chapters, which focus on the examination of the aforementioned offences, digital forensics, and particular findings which shed light on the future of cybercrime and possible improvements in detection and prevention.

---

[3] Keith Becker and Ben Fitzpatrick, "In Search of Shadows: Investigating and Prosecuting Crime on the Dark Web" (2018) 41 U.S. Att'ys Bull., 41.

[4] National Crime Agency, 'Crime threats, Organised crime groups' (National Crime Agency).

[5] Serious Crime Act 2015, s. 45(2).

[6] Thomas J. Holt, Adam M. Bossler and Kathryn C. Seigfried-Spellar, *Cybercrime and Digital Forensics: An Introduction* (2nd edition, Routledge 2018) 16, 19/

CHAPTER TWO

THE DARK NET AND ITS VIRAL SPEED OF GROWTH

As previously mentioned, the Dark Net represents a portion of the internet which is not readily accessible without special encryption software. The internet is commonly seen as being constituted of three parts. It is depicted as an iceberg with a part above the surface and one larger part, below it, comprised of two sections.[7] First, the part above the surface is the open internet, with publicly-accessible web pages which are indexed by search engines. Second, below the water line, the deep web, which is comprised of web pages whose contents are not indexed by standard search engines, and the reason why it is as such is because they are within internal corporate, government or academic computer networks, or because they are behind subscriptions or pay walls. Third, the dark web, which consists of computer networks that require specific software or software configurations in order to be accessed[8].

Being deeply embedded in the deep web, the dark web appears to host the ideal cyberspace for criminals to operate in and through, and that is why this area of the hidden internet has attracted so much attention in the last decade – because of it becoming a proxy for committing crimes and because of its immunity, as it cannot be shut down or eliminated. It is a place of trade, where perpetrators such as professional hackers who break into corporate and government networks to steal data and commit extortion, paedophiles circulating child pornography, traffickers of drugs, guns and humans, all gather to communicate with each other and provide illegal

[7] Paul Anderson, *Web 2.0 and Beyond: Principles and Technologies* (CRC Press 2012) 11, 12.

[8] Keith Becker and Ben Fitzpatrick, "In Search of Shadows: Investigating and Prosecuting Crime on the Dark Web" (2018) 41 U.S. Att'ys Bull., 41.

goods or services. This trade is anonymous, as transactions are performed through cryptocurrencies such as Bitcoin, and therefore paperless transactions such as these are extremely difficult to trace[9]. This entire underground market is vast enough to have established its own search engines, community forums and rating systems just like the open internet[10]. As the Dark Net in itself is an underground market, it is evidently comprised of several illicit markets. These illicit online markets provide criminal vendors the opportunity to purvey all manner of illicit commodities. Law enforcement agencies have found that the Dark Net market ecosystem is extremely unstable, due to the closure of larger markets has led to the closure of smaller ones, but has also led to an increase in the number of smaller vendor shops and secondary markets which cater for specific language groups or nationalities[11].

Among the first illicit online markets were those which enabled the buying and selling of stolen credit card details. The more prominent of these were ShadowCrew, CarderPlanet and DarkMarket. The world of commerce soon expanded to include technologies for skimming and counterfeiting credit cards, malicious software such as viruses, and robot networks[12]. To avoid the attention of law enforcement, many sites established elaborate processes for the vetting of customers, encryption of communications, and the concealment of underground markets. One of the most famous illicit markets was Silk Road, which was one of the first TOR-based narcotics markets. It provided an encrypted internet forum for the purchase and sale of illegal drugs and other products such as firearms, stolen credit cards, counterfeit currency, forged passports and IDs, computer hacking services, and as well as murder for hire[13]. The market gained attention due to the nature of the products sold, and the fact that transactions were paid using Bitcoins[14]. Silk Road put Dark Net markets into the spotlight for the law enforcement agencies and the general public, and it was closed in October

[9] Thomas J. Holt, Adam M. Bossler and Kathryn C. Seigfried-Spellar, *Cybercrime and Digital Forensics: An Introduction* (2nd edition, Routledge 2018) 203.

[10] George Hurlburt, "Shining Light on the Dark Web" (2017) 4 Computer, IEEE Computer Society, 100.

[11] EUROPOL, *Internet Organised Crime Threat Assessment (IOCTA) 2018* (2018) 46, 47.

[12] Peter Grabosky, Cybercrime (Oxford University Press, 2016) 13.

[13] Ibid., 13, 14.

[14] Thomas J. Holt, Adam M. Bossler and Kathryn C. Seigfried-Spellar, *Cybercrime and Digital Forensics: An Introduction* (2nd edition, Routledge 2018) 7.

2013 by the FBI. The argument that the Dark Net market ecosystem is unstable is proven by the fact that even after its closure, successors of Silk Road had dwarfed in size, and "Operation Onymous" in late 2014 resulted in the closure of 33 Dark Net markets. After this operation, several smaller illicit business have migrated to the largest two illicit marketplaces at that time, Agora and Evolution. In 2017, law enforcement has taken down three other major markets, those being AlphaBay (which hosted over 200,000 users and 40,000 criminal vendors), RAMP (which did not use a market interface and was almost exclusively in Russian), and Hansa (which traded high volumes in illicit drugs and other commodities)[15].

However, the sale of drugs, firearms and other services are not the only items which are traded on the Dark Net. One of the most troubling issues present on the Dark Net is the problem of child criminal exploitation. Operating on TOR hidden services, communities where like-minded child sex offenders gather to promote and normalize both the trafficking and sexual abuse of children, educate each other about how to perpetrate child sex abuse without getting caught, and share images and videos depicting the sexual abuse and exploitation of children as young as infants and toddlers[16]. Snuff films, also, are marketed on the Dark Net and, according to research, Russia is one of the leading countries which have a high production level for this sort of films[17]. Snuff films, by definition, are video recordings of people or animals getting tortured or killed. The makers of such movies "recruit" young children from orphanages or rural areas by promising them money or a simple warm meal[18]. The speed with which the Dark Net has grown is far from ordinary, and its status has departed from "emerging", as it now proves to be highly operational and organised. There is increasing consensus that the cyberspace offers plenty of new possibilities for committing serious types of crime, including crimes traditionally associated with organised crime, as a cyber-organised crime narrative has been developing over the last decade also in policy documents at European and international level,

[15] EUROPOL, *Internet Organised Crime Threat Assessment (IOCTA) 2018* (2018) 47.

[16] Keith Becker and Ben Fitzpatrick, "In Search of Shadows: Investigating and Prosecuting Crime on the Dark Web" (2018) 41 U.S. Att'ys Bull., 43.

[17] Janine Kremling and Amanda M. Sharp Parker, *Cyberspace, Cybersecurity, and Cybercrime* (SAGE Publications, 2017) 171.

[18] *Ibid.*, 171.

where the notion of cyber-organised crime has been used to emphasise certain security threats as they ought to be organised crime[19].

[19] Anita Lavorgna and Anna Sergi, "Serious, therefore Organised? A Critique of the Emerging "Cyber-Organised Crime" Rhetoric in the United Kingdom" (2016) 10(2) International Journal of Cyber Criminology, 175, 176.

CHAPTER THREE

ANALYSIS – HUMAN TRAFFICKING AND CHILD PORNOGRAPHY

The increased use of the internet by consumers to identify and purchase goods has enabled the development of online subcultures which engage in both deviant sexual behaviour and human trafficking. These subcultures can also move into criminal activity when the actors victimise children, whether online or offline[20]. The internet became a hub for the distribution of sexual images and videos of children, and public anxiety grew over the potential that children could be solicited online to engage in sexual acts in the real world[21]. Child pornography is defined as the depiction of the sexual or sexualised physical abuse of children 16 years of age or who appear to be less than 16, that would offend a reasonable adult[22]. What makes child pornography different than any other obscene content is the fact that children are the main focus of the sexual nature of these images and videos, as both the subject of the work and participants in the acts[23]. Because of individuals actively seeking out child pornography, they frequently access content which exists on a similar continuum of obscene content, and this is what brought the development of the 10-point Combatting Paedophile Information Networks in Europe (COPINE) scale. The scale was created to categorise the sexual content on the basis of harm involved in erotica and

[20] Thomas J. Holt, Adam M. Bossler and Kathryn C. Seigfried-Spellar, *Cybercrime and Digital Forensics: An Introduction* (2nd edition, Routledge 2018) 24, 25.

[21] *Ibid*., 297.

[22] *Ibid*., 298.

[23] *Ibid*., 298, 299.

pornographic content involving children[24]. The typology was derived from a detailed analysis of more than 80,000 images that were obtained from websites, and the scale has been used by the courts in England and Wales as a measure of seriousness of the offense, as well as to provide insight into the dangerousness of the offender. The severity ranges from non-erotic and non-sexualised material showing children in their underwear, that depict touching or self-stimulation, to showing children in a context of sadism or bestiality[25]. The content considered as most extreme begins in COPINE scale category 8, which features overt sexual acts involving adults, other children, or even animals. Although it may seem unconscionable to pay and view such images or videos, let alone create them, there is a high demand of this content within the community of child pornography consumers on the Dark Net[26]. For the purposes of this analysis, three major law enforcement operations which shed light on how surreptitious the exchange of child pornography and human trafficking are on the Dark Net are "Operation Delego", "Operation Pacifier" and the Black Death Gang criminal case, have been chosen.

"Operation Delego" was an investigation conducted by the U.S. Immigration and Customs Enforcement (ICE) and the Child Exploitation and Obscenity Section (CEOS) of the U.S. Department of Justice's Criminal Division with assistance from several international law enforcement agencies across the world against Dreamboard[27]. Dreamboard was an international criminal network which was dedicated to the sexual abuse of children and creation and dissemination of graphic images and videos of child sexual abuse throughout the world. Members traded graphic images and videos of adults molesting children twelve years of age and under, often violently, collectively creating a massive private library of such material. The international group prized and encouraged the creation of such content,

---

[24] *Ibid*., 300.

[25] Juliane A. Kloess, Jessica Woodhams, Helen Whittle, Tim Grant and Catherine E. Hamilton-Giachritsis, "The Challenges of Identifying and Classifying Child Sexual Abuse Material" (2019) 31(2) ATSA Sexual Abuse, 175.

[26] Thomas J. Holt, Adam M. Bossler and Kathryn C. Seigfried-Spellar, *Cybercrime and Digital Forensics: An Introduction* (2nd edition, Routledge 2018) 302.

[27] ICE, 'Dreamboard member found guilty for participating in international criminal network organized to sexually exploit children' (U.S. Immigration and Customs Enforcement, May 18, 2012) <https://www.ice.gov/news/releases/dreamboard-member-found-guilty-participating-international-criminal-network-organized#wcm-survey-target-id> accessed March 23, 2019.

and links to such content were required to be encrypted with a password that was shared only with members of the network. Members could access the board via proxy servers, disguising the actual location of the user and preventing law enforcement from tracing internet activity. Evidence obtained during this investigation revealed that at least thirty-eight children across the world were suffering sexual abuse at the hands of Dreamboard members, with a high possibility that the children subjected to such atrocities were either kidnapped or trafficked. A total of seventy-two individuals have been charged as a result of this operation, and, to date, fifty-five of the seventy-two defendants have been arrested in the U.S. and abroad[28].

"Operation Pacifier" is an example to illustrate how law enforcement sought to meet the significant challenges posed by a particular group of offenders' use of anonymising technology to perpetrate serious crimes on a massive global scale. Playpen was a highly-sophisticated, global enterprise dedicated to the sexual exploitation of children, on similar lines as Dreamboard, which operated as a hidden service on the TOR network[29]. The Playpen administrator, Steven W. Chase, created the website in 2014, and it allowed its almost 215,000 members to upload and view tens of thousands of postings (more than 117,000)[30] of young victims, indexed by age, sex, and the type of sexual activity involved[31]. Due to the hidden nature of the TOR network, the FBI struggled with discovering IP addresses until Chase revealed Playpen's unique IP address and a foreign law enforcement agency notified the FBI, which launched "Operation Pacifier" in 2015. Members of his enterprise who were raping other children and producing child pornography all around the world continue to be indicted and prosecuted,

[28] *Ibid*.

[29] Keith Becker and Ben Fitzpatrick, "In Search of Shadows: Investigating and Prosecuting Crime on the Dark Web" (2018) 41 U.S. Att'ys Bull., 45.

[30] Mary-Ann Russon, *FBI crack Tor and catch 1,500 visitors to biggest child pornography website on the dark web* (International Business Times, January 7, 2016) <https://www.ibtimes.co.uk/fbi-crack-tor-catch-1500-visitors-biggest-child-pornography-website-dark-web-1536417> accessed February 1, 2019.

[31] DOJ, 'Florida Man Sentenced to Prison for Engaging in a Child Exploitation Enterprise' (U.S. Department of Justice, May 1, 2017) <https://www.justice.gov/opa/pr/florida-man-sentenced-prison-engaging-child-exploitation-enterprise> accessed February 1, 2019.

and as of 2017, there have been 548 international arrests, with 296 sexually abused children identified or rescued[32].

The Black Death Group is another criminal network present on the Dark Net, which has developed a reputation for selling kidnapped women on hidden websites, despite none of its alleged crimes ever being confirmed by law enforcement agencies[33]. This case got considerable attention due to the kidnapping of British model Chloe Ayling, who was lured by Łukasz Herba to a fake studio in Milan, injected her with ketamine, and took her to a secluded place where she was tied to a wooden dresser for six days. Herba had told her that she would be sold and that he had made over $17.7 million by sex-trafficking kidnapped women and selling them via the Dark Net on the Black Death Group website. He organised online auctions for the sale of abducted girls through advertisements describing prey and setting a starting figure. Herba also had in his possession disturbing materials that he claimed were related to the group, including one that seemed to be an advertisement for an 18-year-old girl with her complete body measurements. The Black Death Group presented the kidnapped girls as set for auctions only, but are willing to kidnap specific targets for the needs of the customer, including outside of Europe, but the price will be substantially higher, and also claimed to have a doctor on call who would check the girls for sexually transmitted diseases[34].

Even if there is tenuous and questionable proof that links human trafficking to child pornography, the possibility that children who are victims of sexual abuse are trafficked is very high, as it has earlier been stated that makers of such videos “recruit” or kidnap children from orphanages or rural areas by promising them money, a warm meal, or a

[32] FBI, ‘’Playpen’ Creator Sentenced to 30 Years: Dark Web ‘Hidden Service’ Case Spawned Hundreds of Child Porn Investigations’ (Federal Bureau of Investigation, May 5, 2017) <https://www.fbi.gov/news/stories/playpen-creator-sentenced-to-30-years> accessed February 1, 2019.

[33] EU OCS, ‘Black Death Group linked to abduction and attempted dark web auction of UK model’ (EU-OCS Legal Watch, August 7, 2017) <https://eu-ocs.com/black-death-group-linked-adduction-attempted-dark-web-auction-uk-model/> accessed February 11, 2019.

[34] Barbie Latza Nadeau, ‘Inside ‘Black Death Group’, the Dark Web Gang That Kidnapped a Model’ (The Daily Beast, July 8, 2017) <https://www.thedailybeast.com/the-case-of-the-kidnapped-model-exposes-dark-corners-of-the-deep-web> accessed January 29, 2019.

"better" place to stay[35]. Another way of justifying this possibility is with proof that child sexual exploitation services fall under the same category with kidnapping and raping services, but also through the fact that the number of posts available for these services has surpassed the number of posts available for drug trafficking: drug-related posts have a number of 4,626 while child sexual exploitation, kidnapping and rape-related posts have an astonishing number of 11,783[36].

[35] Janine Kremling and Amanda M. Sharp-Parker, *Cyberspace, Cybersecurity and Cybercrime* (SAGE Publications 2017) 171.

[36] Hussein Alnabulsi and Rafiqul Islam, "Identification of Illegal Forum Activities inside the Dark Net", 2018 International Conference on Machine Learning and Data Engineering (ICMLDE, 2018) 25.

CHAPTER FOUR

APPLICABLE LAW, DIGITAL FORENSICS AND LAW ENFORCEMENT

SUBSECTION ONE – APPLICABLE LAW

It is imperative to state that the term "cybercrime" is not synonymous with "computer misuse", not only for the purposes of this research paper, but also for the purposes of correctly identifying the applicable law. By contrast to computer misuse, cybercrime is not a legal term of art. It might carry with it a certain degree of contextual mutability, but, as stated in the introduction of this paper, computer crimes are those in which computers have either been the object, subject or instrument of a crime (for instance, hacking), and cybercrimes are those offences aided by the use of computers (for instance, online drug, human or firearm smuggling)[37]. This distinction is crucial because different pieces of legislation govern over computer misuse and cybercrime. For computer misuse offences such as unauthorised access to computer material[38] or unauthorised access with intent to commit or facilitate commission of further offences[39], the only statutory provisions are those made in the Computer Misuse Act 1990. Additionally, for cybercrime offences committed via the Dark Net, such as human trafficking or child pornography, the two activities presented in this paper, relevant provisions are made in the Asylum and Immigration (Treatment of Claimants, etc.) Act

[37] Stefan Fafinski, *Computer Misuse: Response, regulation and the law* (William Publishing 2009) 5, 6.

[38] Computer Misuse Act 1990, s. 1.

[39] *Ibid*., s. 2.

2004[40] and the Sexual Offences Act 2003[41] for human trafficking, and, furthermore, the Protection of Children Act 1978[42], and the Criminal Justice Act 1988[43] for possessing or supplying child pornography. A new offence[44] relating to non-photographic images of children was adopted, designed to capture certain types of computer-generated images, including cartoons.[45] In addition, the Convention on Cybercrime (CoC) deals with child pornography under Article 9, requiring Member States to make it illegal to produce, distribute, offer, procure, or possess child pornography via computer or media storage device[46].

SUBSECTION TWO – DIGITAL FORENSICS

Forensic science is the application of science to the law, meaning the scientific process of gathering and examining information to be used by the criminal justice system. In comparison to other fields of forensic science, digital forensics is in its infancy, and digital forensics developed with the onset of the "Digital Age"[47]. Even though, as stated above, that the Dark Net is organised and structured and digital forensics are used to combat it, digital forensics is in its developing stages because the effects of the Dark Net came about much later. This shift to digital forensics was marked by the increased production, transmission, consumption of, and reliance on information[48]. Ever since 1983, international law enforcement agencies have agreed that there is a need for an international response to cybercrime and develop new strategies to combat this phenomenon, and due to changing

[40] Asylum and Immigration (Treatment of Claimants, etc.) Act 2004, ss. 4, 5.

[41] Sexual Offences Act 2003, ss. 57-60.

[42] Protection of Children Act 1978, s. 1.

[43] Criminal Justice Act 1988, s. 160.

[44] Coroners and Justice Act 2009, ss. 62-68.

[45] Chris Reed, *Computer Law* (7th edition, Oxford University Press 2011) 689, 690.

[46] Thomas J. Holt, Adam M. Bossler and Kathryn C. Seigfried-Spellar, *Cybercrime and Digital Forensics: An Introduction* (2nd edition, Routledge 2018) 322.

[47] *Ibid*., 492.

[48] *Ibid*., 492, 493.

trends in technology, the analysis of digital evidence provided by internet traffic, malware, mobiles and computers became the main medium to seize data and apprehend criminals on the cyberspace[49]. One of the most valuable examples to showcase the efficiency and importance of digital evidence is the aforementioned "Operation Pacifier". The FBI, after being notified of the unique IP that the child pornography website utilised, used a hacking tool to unlock TOR and obtain evidence. The FBI seized the computer server running the website, ran the website from their headquarters, deployed a hacking tool and using a single warrant, they uncovered 1,300 IP addresses, tracing them back to actual individuals, which resulted in over 1,500 cases from the investigation[50].

SUBSECTION THREE – LAW ENFORCEMENT

Cybercrime presents a diverse and complicated threat that affects everyone, whether it is an individual, corporation, or government entity. Usually, the highest level of law enforcement are national police forces[51], for instance, the National Crime Agency (NCA), in the United Kingdom, and the Violent Crimes Against Children (VCAC) division of the FBI in the United States. Both agencies investigate a range of criminal activities that affect youth, such as child pornography, kidnapping, and human trafficking[52]. Across the years, several reasons why cybercrime poses significant challenges have been developed, such as: the difficulty to investigate invisible crimes; the difficulty in acquiring and maintaining the technologies required to investigate these activities; or the difficulty in training, retraining, and retaining trained officers[53]. In order to aid law enforcement, non-profit organisations have also made significant efforts to

[49] *Ibid*., 495, 499.

[50] Mary-Ann Russon, *FBI crack Tor and catch 1,500 visitors to biggest child pornography website on the dark web* (International Business Times, January 7, 2016) <https://www.ibtimes.co.uk/fbi-crack-tor-catch-1500-visitors-biggest-child-pornography-website-dark-web-1536417> accessed February 1, 2019.

[51] Thomas J. Holt, Adam M. Bossler and Kathryn C. Seigfried-Spellar, *Cybercrime and Digital Forensics: An Introduction* (2nd edition, Routledge 2018) 40, 48.

[52] *Ibid*., 325.

[53] *Ibid*., 42, 43.

identify and take down child pornography and child sex exploitation. Organisations such as the Internet Watch Foundation (IWF) in the UK and the National Center for Missing and Exploited Children (NCMEC) in the US have the main objective to reduce the amount of child pornography and trafficking[54]. One of the most recent developments in efforts to combat criminality on the Dark Net is Europol's initiative to establish a dedicated Dark Net team to work alongside EU partners and law enforcement globally to reduce the size of this underground illegal economy[55].

[54] *Ibid.*, 323.

[55] EUROPOL, 'Crime on the Dark Web: Law Enforcement Coordination is the Only Cure' (EUROPOL, May 29, 2018) <https://www.europol.europa.eu/newsroom/news/crime-dark-web-law-enforcement-coordination-only-cure> accessed November 23, 2018.

CHAPTER FIVE

FINDINGS AND WHAT THE FUTURE OF CYBERCRIME HOLDS

With the analysis provided above, it has been demonstrated that this criminal venue fuels human trafficking and child pornography not only through the high demand for these services available on the Dark Net, but also because of the rapid advancement of technology and criminal ingenuity of finding new methods of concealing their activities and identities.

In order to provide a better prophylaxis of such crimes, law enforcement will have to continue their global coordination and develop as many useful tools as possible, whether technical or ordinary, and put in place as many task forces which receive proper training for investigating, seizing, and apprehending, in order to provide an efficient prophylaxis. Undercover investigations are of help, but its efficiency is not observed immediately, as most undercover investigations require a law enforcement agent to establish trust within a criminal network, process which takes months, even sometimes years to accomplish, and the outcomes are not always positive. Evidently, there will always be a challenge, because some postings which can be found on the Dark Net are not genuine and can easily induce anyone who surfs this cyberspace into a trap, putting both the user's computer and life at risk, whether it is about infecting the system with malware or immediately finding out the user's live location. In terms of national and international law, there are not a lot of actions which can be taken, besides making it a requirement for every country to have cybercrime-related laws in place, meaning the expansion of the existing criminal law provisions, or to impose stricter sentencing guidelines for the already-existing offences.

As for what the future of cybercrime holds, since law enforcement already works on strategies to combat the abuse of the Dark Net and other cyberspaces for illicit trade, a continuing fragmentation of the markets on the Dark Net is highly predictable. This continuing fragmentation of larger markets will result in the creation of smaller markets and vendors migrating to these smaller markets in order to avoid detection by law enforcement. Moreover, these vendors and smaller markets will, evidently, cater to specific nationalities and this will result in an unlikelihood that it will attract the attention of global law enforcement. As earlier stated, besides the development of better, useful tools to combat cybercrime, law enforcement may also be required to adhere to tactics used by Dark Net sites, for instance, distributed denial of service (DDoS) attacks or malware infiltration. If such tactics are employed, exigent guidelines must be put into place and the investigation's result must be genuine. It is true that most of the content available on TOR is illegal, but not all users surfing the Dark Net are cybercriminals, as some users just prefer to browse anonymously.

The low number of arrests of cybercriminals and market closures only prove that it is a challenge of substantial magnitude, and it would be a superficial expectation to mobilise resources immediately. The Dark Net will not cease to exist, but it is not completely shielded from law enforcement penetrating the walls of this underground economy. Currently, the Dark Net is a hidden safe haven for crime, but there is definite room for improvement and global coordination is key to combat this infamous phenomenon.

BIBLIOGRAPHY

Statutes

(a) Asylum and Immigration (Treatment of Claimants, etc.) Act 2004
(b) Computer Misuse Act 1990
(c) Criminal Justice Act 1988
(d) Coroners and Justice Act 2009
(e) Protection of Children Act 1978
(f) Serious Crime Act 2015

Books

(a) Anderson, P., *Web 2.0 and Beyond: Principles and Technologies* (CRC Press 2012)
(b) Fafinski, S., *Computer Misuse: Response, regulation and the law* (William Publishing 2009)
(c) Grabosky, P., *Cybercrime* (Oxford University Press 2016)
(d) Holt, T. J., Bossler, A. M. and Seigfried-Spellar, K. C., *Cybercrime and Digital Forensics: An Introduction* (2nd edition, Routledge 2018)
(e) Kremling, J. and Sharp Parker, A. M., *Cyberspace, Cybersecurity, and Cybercrime* (SAGE Publications, 2017)
(f) Reed, C., *Computer Law* (7th edition, Oxford University Press 2011)

Journal articles

(a) Alnabulsi, H. and Islam, R., "Identification of Illegal Forum Activities inside the Dark Net", 2018 International Conference on Machine Learning and Data Engineering (ICMLDE, 2018)
(b) Becker, K. and Fitzpatrick, B., "In Search of Shadows: Investigating and Prosecuting Crime on the Dark Web" (2018) 41 U.S. Att'ys Bull.
(c) Hurlburt, G., "Shining Light on the Dark Web" (2017) 4 Computer, IEEE Computer Society
(d) Kloess J. A., Woodhams, J., Whittle, H., Grant, T. and Hamilton-Giachritsis, C. E., "The Challenges of Identifying and Classifying Child Abuse Material" (2019) 31(2) ATSA Sexual Abuse
(e) Lavorgna A. and Sergi, A., "Serious, therefore Organised? A Critique of the Emerging "Cyber-Organised Crime" Rhetoric in the United Kingdom" (2016) 10(2) International Journal of Cyber Criminology

Websites and blogs

(a) DOJ, 'Florida Man Sentenced to Prison for Engaging in a Child Exploitation Enterprise' (U.S. Department of Justice, May 1, 2017) https://www.justice.gov/opa/pr/florida-man-sentenced-prison-engaging-child-exploitation-enterprise, accessed February 1, 2019

(b) EU OCS, 'Black Death Group linked to abduction and attempted dark web auction of UK model' (EU-OCS Legal Watch, August 7, 2017) https://eu-ocs.com/black-death-group-linked-adduction-attempted-dark-web-auction-uk-model, accessed February 11, 2019
(c) EUROPOL, 'Crime on the Dark Web: Law Enforcement Coordination is the Only Cure' (EUROPOL, May 29, 2018) https://www.europol.europa.eu/newsroom/news/crime-dark-web-law-enforcement-coordination-only-cure, accessed November 23, 2018
(d) EUROPOL, Internet Organised Crime Threat Assessment (IOCTA) 2018 (2018)
(e) FBI, ''Playpen' Creator Sentenced to 30 Years: Dark Web 'Hidden Service' Case Spawned Hundreds of Child Porn Investigations' (Federal Bureau of Investigation, May 5, 2017) https://www.fbi.gov/news/stories/playpen-creator-sentenced-to-30-years, accessed February 1, 2019
(f) ICE, 'Dreamboard member found guilty for participating in international criminal network organized to sexually exploit children' (U.S. Immigration and Customs Enforcement, May 18, 2012) https://www.ice.gov/news/releases/dreamboard-member-found-guilty-participating-international-criminal-network-organized#wcm-survey-target-id, accessed March 23, 2019
(g) Latza Nadeau, B., 'Inside 'Black Death Group', the Dark Web Gang That Kidnapped a Model' (The Daily Beast, July 8, 2017) https://www.thedailybeast.com/the-case-of-the-kidnapped-model-exposes-dark-corners-of-the-deep-web, accessed January 29, 2019
(h) National Crime Agency, 'Crime threats, Organised crime groups' (National Crime Agency) http://www.nationalcrimeagency.gov.uk/crime-threats/organised-crime-groups, accessed February 21, 2019
(i) Russon, M. A., 'FBI crack Tor and catch 1,500 visitors to biggest child pornography website on the dark web' (International Business Times, January 7, 2016) https://www.ibtimes.co.uk/fbi-crack-tor-catch-1500-visitors-biggest-child-pornography-website-dark-web-1536417, accessed February 1, 2019