REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No. 1s (2024)
http://www.veterinaria.org
Article Received: Revised: Accepted:

Dark Web Dynamics: Investigating Cybercrime Trends And Regulatory Responses In The Digital Age

Tripti Singh[1*]

[1*]research scholar, institute of legal studies, shree ramswaroop memorial University, Lucknow, tripti.law11@gmail.com

ABSTRACT
Cybercriminals, terrorists, and state-sponsored spies use the Dark Web, which is notoriously difficult to track, to further their illegal goals. There is no difference between traditional crimes and cybercrimes committed on the Dark Web. Dark Web services pose important difficulties tracing criminals because of their scale, uncertain environment, and anonymity. An essential first step in finding answers to cybercrimes is assessing the dangers of the Dark Web. According to the report, more thorough investigations are needed to uncover criminals operating on the Dark Web's crypto exchanges and discussion forums. Forensic investigations rely heavily on analysis. The anonymity of the dark Web services can be a tool in the fight against crime, but only if digital evidence is processed to keep up with law enforcement's efforts to apprehend criminals and shut down illegal sites on the Dark Web.

Keywords: cyber-crime, dark web, Contemporary Challenges, Digital Landscape, Emerging Technologies VG

I.INTRODUCTION

A component of the deep web, the Darkweb (also spelled "Darknet") stands for the seedier, more retrograde half of the Internet. Notable features of the Darkweb include its evasion of legal search and listing platforms, the need for passwords to access them when available, and the concealment of user identities, IP addresses, network activity, and shared data [1]. Although Darkweb was first created for military communication and to promote free expression, it has given its enemies the tools they need to carry out horrific acts in disguise. All of these things undermine the safety of individuals, neighbourhoods, and the planet: extortion, child and human trafficking, illicit narcotics and weapon trade, and extreme ideology and terrorist promotion. The Darkweb is a communication platform, an online marketplace, a conduit for anonymous financial transactions, a repository for dangerous information, and a front for online crime, according to the authors [2]. Why was it so easy for Darkweb to make all of this possible? Bitcoin, a cryptocurrency, and the Tor network, also known as Onion routers, were two innovative technologies that met users' needs for anonymous financial transactions. Publications on studies and advances on the Darkweb's usage and abuse started in 2010. The Darkweb study aims to battle the range of issues and evolve cyber threat intelligence simultaneously, even though the Darkweb is mostly recognized for fueling crime-as-a-service. Some research [3] addresses the complexity of policy rules surrounding Darkweb. It is very difficult, if possible, to enforce restrictions or block access to Darkweb bridges or relays because of the lengthy and complicated processes. However, the majority of studies have concentrated on creating methods and tools for identifying cyber threat intelligence [1] and criminal and terrorist provocative behaviours [4] that glean useful information from a variety of sources on the surface and the dark web. To address fundamental questions like "what," "when," "which," and "how" about crime facilitators, researchers began by scribbling and analyzing Darkweb markets, as seen in the exploratory data analysis [5]. There have also been efforts to create an automated operating system that could identify and inform about new Darkweb malware or vulnerabilities using a combination of machine learning and artificial intelligence, with an accuracy level of more than 80% [6].

II.LITERATURE REVIEW

Cryptocurrencies have been all the rage in the last ten years. “Using data from the Web of Science and Scopus databases, researchers [7] conducted a bibliometric examination of the scientific output of cryptocurrencies, particularly Bitcoin and Ethereum.” Tableau, R, and VOSviewer tools were used for this purpose. According to their findings, the number of publications has increased by 100% annually over the last three years. Their examination of how blockchain technology has developed in different cryptocurrencies is very intriguing. Among 464 studies [8] examining the use of cryptocurrencies in management and business, four distinct lines of inquiry emerged: cryptocurrency returns, efficiency, portfolio diversification, and regulation. The writers also hint at future research agendas in cryptocurrency. The significance of this research in light of recent developments in underground cryptocurrency marketplaces (Darknets) is underscored by the pivotal role of virtual currencies. “Using data obtained from relevant websites accessible using The Onion Router (Tor), which permits anonymous and encrypted communication, the research of these patterns [9] focuses on the numerous digital items offered in these dark marketplaces.” The information came from one of the most active cryptocurrency marketplaces and was gathered over months. Additionally, Dream Market depicted the price fluctuations and short-term trends of malware items on underground cryptocurrency marketplaces. “Following the research's discussion of the amount of daily anonymous users of the Darkweb (using Tor) in Kosovo and across the globe, the use of the Darknet has grown in popularity [10].” The study included an overview of the Influence of the dark web in many areas of society. We discuss anonymity and get results from the Darkweb search engines Ahmia and Onion City. The

article uses IP addresses and country codes to determine how many people use anonymous Darkweb networks and displays that figure. The anonymity provided by services like Tor makes the Darkweb an ideal environment for criminal activity, including but not limited to pornography, drug trade, terrorism, and weapon trade. The authors investigated crimes, repercussions, and tactics in a comprehensive literature study of 65 publications from top databases [11]. They aimed to help cybersecurity researchers and experts spot and combat new dark web crime risks. The report concluded that further investigation into criminals and cryptocurrency marketplaces is necessary. Forensic investigations rely heavily on dark web forums because of their anonymity, which may be utilized to identify perpetrators. Law enforcement agencies can apprehend offenders and take down illegal dark websites because of the work put into evaluating and processing digital evidence. The literature on dark web research about terrorism was critically reviewed [12]. According to the findings, very little research has been conducted on this subject. “They suggest scanning the Darkweb for signs of terrorist activity and, more crucially, using sophisticated A.I., image processing, and natural language processing, among other methods.” There is a list of systematic literature reviews (SLRs) for researching and identifying illicit activity on the dark web that pertains to the worldwide drug market in a follow-up study [13]. Drug trafficking and other dark web crime episodes, including illicit internet commerce, coordinated criminal events, and possible unlawful marketplaces, need further primary research, according to the study. “Another study [14] examined the pattern of anonymous communication research from 2000 to 2022 using the bibliometric approach and the Citespace tool to examine partnerships among authors, institutions, and journals.” They identified keywords like "Darkweb" and "privacy protection" as having the potential to greatly impact future studies. According to the report, publications on the subject have also grown quickly. “Despite the abundance of evidence showing that Darkweb services are widely used for illicit purposes, researchers in criminology and penology recently conducted a comprehensive literature review and bibliometric analysis of 49 articles [15].” Insights into the development of Darknet-related crimes, such as the role of prolific writers, the contributions of the Global South, and the need of regional publishing parity, are provided by their research. Also included are six suggestions for future studies in this area, some of which include police measures. For those working in the fields of mental health and addiction, an interesting paper summarises what is currently known about prodrug actions on the deep web [16]. Using Google and DuckDuckGo, we performed a non-participant ethnographic qualitative research of surface online pages that promote drugs. Information on using search engines, cryptocurrency, the Darknet, and other online drug-selling sites was among the four main topics covered over fourteen categories. This study provides a comprehensive overview of the deep web and online drug markets for addiction experts. Although it is not as widespread as open commerce on the surface web, the Darkweb does facilitate the illicit trafficking of animals in addition to narcotics. “An example of illicit wildlife trafficking involving the sale and discussion of a cactus species known for its hallucinogenic qualities was discovered in one such research [17].” The piece delves into illicit wildlife trading and how enforcement has failed to curb it, urging readers to take action.

III.CRIMINAL ACTIVITY THREATS IN THE DARK WEB

A. Human Trafficking and Sex Trafficking

Forums, chat services, and the anonymity of the Deep Web have greatly contributed to the rise of human and sex trafficking, which constitute a significant portion of the criminal population [18]. One of the most pressing issues concerning human rights is trafficking in humans. “The U.N. Office on Drugs and Crime estimates that 2.5 million people around the globe are ensnared in modern-day slavery [19], The victims are enslaved and used as sex workers, child soldiers, domestic servants, industrial employees, and in other commercial occupations.” People who engage in human trafficking and sex trafficking often negotiate and enter into contracts in order to attract victims. The government and anti-human trafficking groups utilize detection, censorship, and monitoring systems, but trafficking networks are dynamic so that they may evade these measures [20]. Detecting human trafficking in the hidden nature field is no easy task. “Nearly 40 million people were victims of modern slavery in 2017, according to the International Labor Organization (ILO).” Of this total, 24.9 million were enslaved to work as labourers and 15.4 million were married against their will in 2016. This works out to 5.4% of the global population that has been a victim of modern slavery. “It is very concerning that one out of every four victims is a modern-day enslaved person. Of the (24.9) million people who were enslaved, around 16 million were forced to work in agricultural, construction, or domestic work; about (4.8) million were forced into sexual slavery, and the other 4 million were forced into labour. Nearly all women(99%) and nearly all girls (58%) are victims of sexual exploitation in some form or another [21].” Human trafficking has far-reaching consequences, as shown in a 2014 study detailing the over 21,000 calls received by a federally-funded hotline for victims of human trafficking. From 2013 to 2014, the number of trafficking convictions obtained by the Department of Justice increased from 174 to 184. Of the total number of instances, 157 included victims of sex trafficking and 27 concerned victims of labour trafficking [22]. Many young girls from other nations fall prey to human trafficking, which involves deceit, manipulation, and, in extreme cases, kidnapping and forced prostitution [23].

B. Pornography Industry

Women who have been victims of human or sex trafficking are the most common victims of the pornographic business [24]. “Following the signing of an agreement between a man and a female, traffickers use threats of murder to coerce victims into participating in pornographic productions.” Without the victims' knowledge or permission, sex traffickers

film explicit videos and sell them to pornographic websites. Recordings and photographs are also made public on the websites of traffickers [25]. “The Dark Web is home to several pornographic websites.” Like human and sex traffickers, those involved in the pornography business hide their identities as they recruit or abduct victims using the Dark Web, social media, and online forums [23]. Images and videos of prostitution shared online depict new kinds of illegal behaviour and graphic violence [26]. “The widespread use of social media has also led to an increase in the sophistication of prostitution.” It is very difficult to conduct efficient investigations into prostitution because of the need to interview victims and witnesses and keep track of their activities [27].

C. Assassins and Marketing

Criminals offer their assassin talents for sale on the Dark Web. Criminals might be hired for $10,000 in the U.S. and $12,000 in Europe using the websites C'thuthlu, White Wolves, and MailOnline [28]. The range of salaries for high-ranking politicians to police officers is 40 thousand to 15 million [29]. Since the Deep Web includes hundreds of connections to clandestine onion sites, Hidden Wiki and Deep search engines are the most frequent means to explore it [30]. “Under Commercial Services, the researchers compiled a list of thirteen separate illegal onion sites.” Three of the most sought-after locations were the Silk Road, Sheep Market, and Black Market Reloaded forums [31]. “Between 2011 and 2013, the Silk Road was the most heavily policed Deep Web marketplace for narcotics and political discourse among people who shared a commitment to liberty, free enterprise, and little government intervention.” There was a tremendous influence when the original Silk Road website was up, which was less than three years old. Users of Silk Road believed they could communicate completely anonymously because it was run as a Tor hidden service. In addition, bitcoin transactions were the sole way to make purchases on Silk Road [32]. Regarding Tor hidden-services trading, Bitcoin is by far the most popular currency. Cryptographic transactions can be tracked but not readily deanonymized [33].

The rise and fall of Silk Road was precipitated on October 1, 2013, when the marketplace was taken over, and its creator, Ross Ulbricht, was apprehended by the FBI, the IRS, and the DEA. Separate allegations accused him of covering up the attempted killings of two business partners he felt had betrayed him. “The Justice Department confiscated Bitcoins and shut down the Silk Road website, which had an estimated worth of ($3.6) million [34].”

D. Drug Transactions

There are typically two distinct kinds of drug marketplaces on the Deep Web. Specific drug markets, such as those for heroin, fall under this category. This kind is quite popular because of the vendor-customer interaction and the specialist knowledge of the products. The second category of drug markets consists of general merchandise stores where customers may purchase guns, pornographic material, stolen jewels, illegal smokes, and even credit cards. The most prevalent commodities are narcotics, which comprise drug hardware and chemicals used to manufacture drugs [35]. Because of the anonymity it provides, the Deep Web has become a digital black market for drugs, and the number of drug transactions conducted there has increased dramatically. Illicit dealers purchase and sell narcotics on the Dark Web since there is no need for face-to-face contact in this industry. “The dark web marketplace Silk Road was one example that sold narcotics for over a billion dollars and used DHL or drop shipping to send them [36].”

In the wake of Silk Road's October 2013 shutdown, a number of other Dark Web cryptocurrency marketplaces emerged [37]. According to research conducted from a Swiss perspective, Evolution, a prominent cryptocurrency market that operated from 2014 to 2015, had over 48,000 listings and around 2,700 dealers offering to ship illegal drug goods from 70 different countries. “Three vendors in Switzerland were discovered and identified.” Digital information, including shipment nation, medicine kind, and so on, was the target of the acquisitions. While digital information such as concealing techniques and delivery nation were correct, the quality of the illegal substances was discovered to deviate from what was reported [38].

Mr. Nice Guy was another area on the Dark Web where people could buy and sell narcotics, both legal and illicit, including marijuana and cocaine. The site's security is adequate, and the registration is more protected than on a regular site [39].

E. Child Abuse

Many apps that disguise users' identities, such as Omegle and Ask. Children use Fm for social media and communication [40]. In order to engage with youngsters, pedophiles make use of these apps. Pedophiles and associated criminals use the Dark Web extensively to share photographs and pons featuring children. Hosting children's pornography was made possible by Freedom Hosting's network of 550 servers spread throughout Europe [41].

The FBI apprehended hundreds of pedophiles from the United States and other countries as part of Operation Pacifier. The investigation included 2,000 users, 23,000 sexually graphic photos, and 9, 000 video files [42]. The tragic death of Amanda Todd, a 15-year-old girl from Canada, spotlighted the issue of internet child exploitation on a worldwide scale. A few weeks before her death, she uploaded a video on YouTube in which she detailed her 2012 trauma, using flash cards to describe being physically attacked, tormented, and pressured into showing her breasts via webcam [43]. An increasing number of cases of online child sexual abuse include webcam child prostitution, in which the victim just sells live sexual photos using Voice-over-IP (VoIP) programs. It is possible to capture and sell real-time footage of child

abuse using the video streaming function of VoIP programs [44]. As much as 95% of the child porn on the TOR network was found to be hosted by the freedom hosting firm in 2011. After thousands of subscribers and 100 child porn sites, the site was taken down in 2013 [45]. In 2017, the same group of hackers who had previously compromised Freedom Hosting discovered Freedom Hosting II. Over half of the material on Freedom Hosting, according to the hackers, was child pornographic, and they were able to identify the sites' users thanks to the spilled data [46]. "South Korean 23-year-old Jong Woo Son launched the biggest child sexual exploitation website, Welcome to Video, in 2015." The operator was indicted in 2018, and the facility's location was determined. Law enforcement officials took three hundred and thirty-seven users from eleven different nations and twenty-three U.S. states into custody. Participants on the site were able to rescue 23 mistreated children from the US, Spain, and the U.K. as a direct consequence of this [47].

F. Terrorism

There is a grave risk to national security posed by terrorist groups and acts of terrorism on the Deep Web. "The Dark Web has been used by terrorist groups like al-Qaeda/ISIS and ISIL ISIS to promote propaganda and achieve their evil goals [48]." The Dark Web is a tool that the Islamic State in Iraq and Syria (ISIS) used to communicate information across command structures, seek donations to further their cause, and more. An editor for Defense One's technology section has claimed that there is evidence to suggest that ISIS or parties affiliated with it are using the Dark Web for reasons other than spreading propaganda and promoting their agenda. Services offered on the Dark Web are paid for by ISIS using Bitcoins. U.S. military officials are keeping tabs on ISIS using Dark Web monitoring, but so far, they have not been able to do so without violating people's right to privacy [49].

As a tool of terrorism, ISIS broadcasts and records the execution of condemned inmates over the Dark Web. They broadcast themselves on the Dark Web, posting videos of their inhumane antics. They also use the Dark Web to recruit warriors all across the globe [50]. In order to prevent hackers from gaining access to sensitive information, ISIS resorted to the Dark Net. "Using Dark Web sites and other online channels, they disseminated news and misinformation after the 2015 November attacks in Paris." Al-Hayat Media Center, an ISIS-affiliated news source, explained how to access their new Dark Web site and released a link to it on an ISIS-related forum. Using a TOR browser connection, the message was transmitted using Telegram, an encrypted messaging app utilized by ISIS for Windows and smartphones. Too confident, the Telegram creators offered a monetary incentive to whomever could crack the encryption and decrypt the app [51]. ISIS uses an encrypted public forum to coordinate operations and discuss command and control. They have been able to use tiny drones to gather real-time data for propaganda purposes and use applications like Skype and WhatsApp to transmit messages across the battlefield. ISIS recruits new members by disseminating its ideology and instructions on how to make weapons for terrorist acts in well-produced web periodicals [52]. Several studies have identified five distinct types of online terrorist actions. Propaganda, training and recruiting, communications, funding, and targeting are all part of it [53].

IV. TECHNIQUES TO LOCATE CRIMINALS ON THE DARK WEB

Crimes committed on the Dark Web are not dissimilar to those committed in the real world, with the main difference being the difficulty for law authorities to trace virtual crimes perpetrated on the Dark Web. "Some forensic analysts may have difficulties in investigating criminal activities due to the anonymity offered by Dark Web sites, Because of this, forensic investigations into criminal acts are being impeded." The Dark Web has been the site of much research on illicit activity detection.

A. Law Enforcement

The technological know-how of larger law enforcement organizations makes it impossible for them to combat the growing sophistication of cybercrime. Criminal, civil, and regulatory laws all have a say in what happens when criminals engage in illicit activities on the Dark Web. Crimes committed at the federal, state, or regional levels are the purview of criminal law. Potential punishments include anything from a single life sentence to the death penalty. The death penalty is a possibility, albeit it depends on the state where the crime took place. A party that has been fined or ordered to do community service as a condition of their sentence falls within the purview of civil law. The power to levy fines as a form of punishment lies with the relevant regulatory body within a given jurisdiction. Any person or organization that violates regulations may have their commercial operations halted by the relevant regulatory bodies [54].

B. Social Media

It is possible to find illegal activities occurring on the Dark Web by combining social media with the Deep Web. Social media platforms like Facebook, YouTube, and Twitter are used to identify suspects [55]. According to RSA, cybercriminals discuss and sell credit card numbers, other data, and stolen personal information using social media platforms like Facebook, Instagram, WhatsApp, Telegram, and Snapchat.

Social networking platforms make it easy to share and disseminate everything, including malware, which is why hackers frequently utilize them. In addition to sharing buttons and plug-ins, these platforms also use advertisements to trick people more than other websites. Furthermore, the fact that hundreds to thousands of users are connected on these

platforms makes it easier for cybercriminals to spread malware over a wider audience [56]. A criminology expert from the University of Surrey in the United Kingdom carried out a six-month global study on cybercrime on social media last year. The results of the investigation showed that by misusing popular social networks, fraudsters earn almost $3.25 billion annually [57].

Social media is positively assisting law enforcement in locating leads that result in the solving of crimes. Tips can be obtained from the large user base on social media sites in addition to local crime observations [58]. One of the police's successful use of social media to track down suspects has been the arrest of Raderius Glenn Collins, a burglar from Florida who boasted about a $500,000 jewellery heist in a seven-minute Facebook video that received three thousand views. Another was the 33-year-old Derek Medina's life sentence for killing his wife in the second degree. "The murderer posted a description of his wife's murder on Facebook along with a picture of her corpse; Maxwell, 71 people were taken into custody in Cincinnati following a nine-month operation that utilized social media to identify significant gang members." Among them was Marion Morton, who was accused of first-degree murder after sharing a Snapchat photo of a student who had been shot in the face [59]. "The University of Cincinnati's Institute of Crime Science helped the police capture the gang by fusing information from reports and official records with data from social media [59]." According to LexisNexis, almost 80% of police departments use social media as a tool for investigations. LexisNexis provided guidelines on the use of social media in investigations in 2012 and 2014.

V. CONCLUSION

More precisely, this SLR thoroughly explains the threats presented by the Dark Web, the technological and forensic challenges brought about by the network architecture's anonymity, and the methods, tools, algorithms, and techniques employed to locate and capture criminals using the Dark Web. The methods criminals use to evade capture are growing more sophisticated as they operate on the Dark Web. As a result, challenges become more intense. "Crossing international boundaries are one of the hardest things for law enforcement and security agencies." Because of the vastness of the hidden web, more effective ways to lower its related hazards are needed. Tracking the black market and any transactions that occur there is essential to apprehend the offenders using state-of-the-art methods. Since the Dark Web is layered, fractured, and unindexed, it is more challenging to identify criminal activity. The Dark Web ecosystem is notoriously unpredictable due to the regular birth and disappearance of old and new sites. To overcome these problems, forensic law enforcement must gather robust digital evidence.

VI.REFERENCES

1. R. Basheer, B. Alkhatib, Threats from the dark: a review over darkweb investigation research for cyber threat intelligence, Journal of Computer Networks and Communications (2021).
2. A. Gupta, S.B. Maynard, A. Ahmad, The Darkweb Phenomenon: A Review and Research Agenda, 2021 arXiv preprint arXiv:2104.07138.
3. M. Chertoff, A public policy perspective of the Darkweb, Journal of Cyber Policy 2 (1) (2017) 26–38.
4. H. Chen, W. Chung, J. Qin, E. Reid, M. Sageman, G. Weimann, Uncovering the Darkweb: a case study of Jihad on the web, J. Am. Soc. Inf. Sci. Technol. 59 (8) (2008) 1347–1359.
5. M. Bernaschi, A. Celestini, S. Guarino, F. Lombardi, Exploring and analyzing the tor hidden services graph, ACM Trans. Web 11 (4) (2017) 1–26.
6. E. Nunes, A. Diab, A. Gunn, E. Marin, V. Mishra, V. Paliath, P. Shakarian, Darknet and deepnet mining for proactive cybersecurity threat intelligence, in: 2016 IEEE Conference on Intelligence and Security Informatics (ISI), IEEE, 2016, pp. 7–12
7. F.J. García-Corral, J.A. Cordero-García, J. de Pablo-Valenciano, J. Uribe-Toril, A bibliometric review of cryptocurrencies: how have they grown? Financial innovation 8 (1) (2022) 1–31
8. R.N.U.D. Jalal, I. Alon, A. Paltrinieri, A Bibliometric Review of Cryptocurrencies as a Financial Asset, Technology Analysis & Strategic Management, 2021, pp. 1–16.
9. R. Broadhurst, D. Lord, D. Maxim, H. Woodford-Smith, C. Johnston, H.W. Chung, B. Sabol, Malware Trends on 'Darknet'crypto-Markets: Research Review, Available at: SSRN 3226758, 2018
10. A.S. Beshiri, A. Susuri, Darkweb and its impact in online anonymity and privacy: a critical analysis and review, J. Comput. Commun. 7 (3) (2019) 30.
11. S. Nazah, S. Huda, J. Abawajy, M.M. Hassan, Evolution of Darkweb threat analysis and detection: a systematic approach, IEEE Access 8 (2020) 171796–171819
12. E.D.A. Sonmez, ¨ K. Seçkin Codal, Terrorism in Cyberspace: A Critical Review of Darkweb Studies under the Terrorism Landscape, 5, Sakarya University Journal of Computer and Information Sciences, 2022.
13. R. Rawat, V. Mahor, M. Chouhan, K. Pachlasiya, S. Telang, B. Garg, Systematic literature review (SLR) on social media and the digital transformation of drug trafficking on darkweb, in: International Conference on Network Security and Blockchain Technology, Springer, Singapore, 2022, pp. 181–205.
14. Y. She, D. Xu, Z. Tan, J. Zhao, Research hotspot and trend analysis of anonymous communication based on Citespace, in: 2022 3rd International Conference on Information Science, Parallel and Distributed Systems (ISPDS), IEEE, 2022, pp. 58–62.

15. H.T. Luong, Preliminary findings of the trends and patterns of darknet-related criminals in the last decade, Secur. J. (2023)
16. L. Orsolini, D. Papanti, J. Corkery, F. Schifano, An insight into the deep web; why it matters for addiction psychiatry? Hum. Psychopharmacol. Clin. Exp. 32 (3) (2017), e2573.
17. J.R. Harrison, D.L. Roberts, J. Hernandez-Castro, Assessing the extent and nature of wildlife trade on the Darkweb, Conserv. Biol. 30 (4) (2016) 900–904.
18. D. Décary-Hétu and L. Giommoni, ‘‘Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of operation onymous,’’ Crime, Law Social Change, vol. 67, no. 1, pp. 55–75, Feb. 2017
19. L. Greenemeier. (Feb. 8, 2015). Human traffickers caught on hidden Internet. Scientific American. [Online]. Available: https://www.scientificamerican.com/article/human-traffickers-caughton-hidden-internet/
20. R. Konrad and A. Trapp. (2017). Data Science Can Help Us Fight Human Trafficking. [Online]. Available: https://theconversation.com/datascience-can-help-us-fight-human-trafficking-81647
21. Geneva. (Sep. 19, 2017). Forced Labour, Modern Slavery and Human Trafficking. [Online]. Available: https://www.ilo. org/global/topics/forced-labour/lang–en/index.htm
22. C. Reilly. (Jul. 29, 2015). Human Trafficking: A Crime Hard to Track Proves Harder to Fight. [Online]. Available: https://www.pbs. org/wgbh/frontline/article/what-is-human-trafficking-and-why-is-it-sohard-to-combat/
23. H. J. Clawson and N. Dutch, ‘‘Addressing the needs of victims of human trafficking: Challenges, barriers, and promising practices: Department of health and human services, office of the assistant secretary,’’ Dept. Health Hum. Services, Washington, DC, USA, Tech. Rep., 2008.
24. D. Rathod, ‘‘Darknet forensics,’’ Future, vol. 11, no. 4, p. 12, 2017
25. ConvenantEyes. (Sep. 7, 2011). The Connections Between Pornography and Sex Trafficking. [Online]. Available: https://www. covenanteyes.com/2011/09/07/the-connections-between-pornographyand-sex-trafficking
26. H. Grant, ‘‘Cathryn Lavery of Iona College’ Social Media and the New Generation of ‘Computerated’ Criminals,’’ Crim Forensic Studies, vol. 2, no. 1, 2019, Art. no. 180022
27. K. Beckham and A. Prohaska ‘‘Deviant men, prostitution, and the Internet: A qualitative analysis of men who killed prostitutes whom they met online,’’ Int. J. Criminal Justice Sci., vol. 7, no. 2, pp. 635–648, 2012.
28. M. Chertoff and T. Simon, ‘‘The impact of the dark Web on Internet governance and cyber security,’’ Centre Int. Governance Innovation (CIGI), Waterloo, ON, Canada, Tech. Rep. 6, 2015
29. Daily Mail. (Oct. 12, 2013). The Disturbing World of the Deep Web, Where Contract Killers and Drug Dealers Ply Their Trade on the Internet. [Online]. Available: https://www.dailymail.co.uk/news/article2454735/The-disturbing-world-Deep-Web-contract-killers-drugdealers-ply-trade-internet.html
30. K. M. Finklea, ‘‘Dark Web,’’ in Proc. Congressional Res. Service, 2015, pp. 1–16.
31. B. Backman, ‘‘Follow the white rabbit: An ethnographic exploration into the drug culture concealed within the ‘deep web,’’’ Univ. Nebraska Omaha, Omaha, NE, USA, Tech. Rep. UMI 1551711, 2013
32. J. Lane, ‘‘Bitcoin, silk road, and the need for a new approach to virtual currency regulation,’’ Charleston L. Rev., vol. 8, no. 5, p. 511, 2013
33. D. Moore and T. Rid, ‘‘Cryptopolitik and the Darknet,’’ Survival, vol. 58, no. 1, pp. 7–38, 2016.
34. S. Pfeifer, S. Li, and W. Hamilton. (Oct. 2, 2013). End of Silk Road for Drug Users as FBI Shuts Down Illicit Website. [Online]. Available: https://www.latimes.com/business/la-fi-silk-road-bitcoin-20131003- story.htm’
35. N. Christin, ‘‘Traveling the silk road: A measurement analysis of a large anonymous online marketplace,’’ presented at the 22nd Int. Conf. World Wide Web, 2013.
36. J. Aldridge and D. Décary-Hétu, ‘‘Hidden wholesale: The drug diffusing capacity of online drug cryptomarkets,’’ Int. J. Drug Policy, vol. 35, pp. 7–15, Sep. 2016.
37. A. Celestini, G. Me, and M. Mignone, ‘‘Tor marketplaces exploratory data analysis: The drugs case,’’ presented at the Int. Conf. Global Secur., Saf., Sustainability, 2017.
38. D. Rhumorbarbe, L. Staehli, J. Broséus, Q. Rossy, and P. Esseiva, ‘‘Buying drugs on a darknet market: A better deal? Studying the online illicit drug market through the analysis of digital, physical and chemical data,’’ Forensic Sci. Int., vol. 267, pp. 173–182, Oct. 2016.
39. DeepDotWeb. (2015). Interview: ‘Mr. Nice Guy’ Market Admin Tells His Story. [Online]. Available: https://gir. pub/deepdotweb/2015/06/03/interview-with-mr-niceguy-market-admin/
40. C. Cranford. (Feb. 21, 2015). Dangerous Apps on Your Teen’s Mobile Device. [Online]. Available: https://www. cybersafetycop.com/dangerous-apps-on-your-teens-mobile-device
41. K. M. Finklea, ‘‘Dark Web,’’ in Proc. Congressional Res. Service, 2015, pp. 1–16.
42. FBI. (May 5, 2017). Playpen’ Creator Sentenced to 30 Years. [Online]. Available: https://www.fbi.gov/news/stories/playpen-creator-sentencedto-30-years
43. K. V. Açar, ‘‘Webcam child prostitution: An exploration of current and futuristic methods of detection,’’ Int. J. Cyber Criminol., vol. 11, no. 1, pp. 98–109, 2017
44. E. Puffer, K. McDonald, M. Pross, and D. Hudson, ‘‘Webcam child sex tourism: An emerging global issue,’’ Cedarville Univ., Cedarville, OH, USA, Tech. Rep., 2014

45. K. Poulsen. (Sep. 9, 2013). FBI Admits it Controlled Tor Servers Behind Mass Malware Attack. [Online]. Available: https://www.wired.com/2013/09/freedom-hosting-fbi/
46. The Bitcoin News. (Feb. 9, 2017). Anonymous Hacks Freedom Hosting II, Bringing Down Almost 20% of Active Darknet Sites. [Online]. Available: https://thebitcoinnews.com/anonymous-hacks-freedom-hosting-iibringing-down-almost-20-of-active-darknet-sites/
47. L. H. Newman. (Oct. 16, 2019). How a bitcoin trail led to a massive dark Web child-porn site takedown. Wired. [Online]. Available: https://www.wired.com/story/dark-web-welcome-to-video-takedownbitcoin/
48. G. Weimann, ‘‘Going dark: Terrorism on the dark Web,’’ Stud. Conflict Terrorism, vol. 39, no. 3, pp. 195–206, Mar. 2016.
49. P. Tucker. (Feb. 24, 2015). How the Military Will Fight ISIS on the Dark Web. [Online]. Available: https://www.defenseone.com/ technology/2015/02/how-military-will-fight-isis-dark-web/105948/
50. P. W. Singer and E. T. Brooking, LikeWar: The Weaponization of Social Media. New York, NY, USA: Eamon Dolan Books, 2018.
51. G. Weimann, ‘‘Going dark: Terrorism on the dark Web,’’ Stud. Conflict Terrorism, vol. 39, no. 3, pp. 195–206, Mar. 2016
52. P. W. Singer and E. T. Brooking, LikeWar: The Weaponization of Social Media. New York, NY, USA: Eamon Dolan Books, 2018
53. Y. Wu, F. Zhao, X. Chen, P. Skums, E. L. Sevigny, D. Maimon, and M. J. Feizollahi, ‘‘Python scrapers for scraping cryptomarkets on tor,’’ presented at the Int. Conf. Secur., Privacy Anonymity Comput., Commun. Storage, 2019
54. D. Shinder, ‘‘What makes cybercrime laws so difficult to enforce,’’ Tech. Rep., 2011
55. R. Surette, ‘‘Performance crime and justice,’’ Current Issues Criminal Justice, vol. 27, no. 2, pp. 195–216, 2015
56. H. Bleau. (Apr. 24, 2019). Social Media and the Digital Transformation of Cybercrime. RSA Security. [Online]. Available: https://www.rsa.com/enus/blog/2019-04/social-media-and-the-digital-transformation-ofcybercrim
57. N. Lindsey (Mar. 12, 2019). Cyber criminals have turned social media cyber crime into a $3 billion business. CPO Magazine. [Online]. Available: https://www.cpomagazine.com/cyber-security/cyber-criminalshave-turned-social-media-cyber-crime-into-a-3-billion-business/
58. M. Tsikerdekis and S. Zeadally, ‘‘Multiple account identity deception detection in social media using nonverbal behavior,’’ IEEE Trans. Inf. Forensics Security, vol. 9, no. 8, pp. 1311–1321, Aug. 2014
59. P. Dughi. (Jun. 26, 2016). 17 times social media helped police track down thieves, murderers, and gang criminals. Medium. [Online]. Available: https://medium.com/the-mission/17-times-social-media-helped-policetrack-down-thieves-murderers-and-gang-criminals-a814b6c40fb