Beyond the Surface Web: How Criminals Are Utilising the Internet to Commit Crimes

Kaycee Jacka

Abstract The internet has revolutionised society and plays a key role in users lives. The rapid advances in technology means that now more than ever, users have the right to anonymity online, a service which is greatly invaluable to some, however, is leading to illicit behavior in others. Security threats and the distribution of illegal materials and substances continue to take place online, with a combination of legal loopholes and advancing anonymity subsequently leading to slow investigatory processes. This research considers how criminals are using services to their advantage and remaining largely undetected by the criminal justice system. This research also considers how ethically the criminal justice system works when dealing with its investigations with recommendations for the future. The growing use of cryptocurrencies are also considered with its security advantages for users but how the virtually anonymous features are enticing for criminal activity. This research considers whether digital forensics is keeping up with demand within the criminal justice system and whether new services with the standardisation and collaboration of governments is required to aid further investigations.

Keywords Deep web · The Onion Router · Digital forensics · Bitcoin

1 Introduction

In everyday use of the internet, we use what is referred to as the surface web; however, this only makes up 4% of what the internet has to offer. This gives users access to websites such as Google, YouTube, social media, or any website that can be accessed via a link. "Searching on the Internet today can be compared to dragging a net across the surface of the ocean. While a great deal may be caught in the net, there is still a wealth of information that is deep, and therefore, missed" [4]. Comparably, as

K. Jacka (✉)
Department of Criminology, Sociology and Social Policy, School of Social Sciences, Swansea University, Singleton Park, Swansea SA2 8PP, UK
e-mail: 854956@Swansea.ac.uk
URL: http://www.swansea.ac.uk

R. Montasari et al. (eds.), *Digital Transformation in Policing: The Promise, Perils and Solutions*, Advanced Sciences and Technologies for Security Applications,
https://doi.org/10.1007/978-3-031-09691-4_6

specialist equipment is used to explore deeper parts of the ocean, it is used to explore the web. The deeper you explore and seek to find, the more knowledge is needed on how to navigate the 96% of the internet referred to as—the deep web [13]. This gives users access to anything that can't be accessed by a link or password protected domains such as private emails or workplace servers. Making up 1% of the deep web is the dark web, accessible only via specialist tools and equipment that protect the user's identity. Considering the scale and invitation of anonymity that the dark web has to offer, the advantages of using it for purposes such as communication platforms are endless.

However, with advantages come disadvantages and with every legal and well-meaning platform, the dark web has become home to illegal services ranging from child pornography and human trafficking to fraud and data selling. Added complexities have emerged making it easier than ever before to partake in crime online anonymously. The emergence of cryptocurrencies has enabled users to exchange goods in a completely anonymous nature meaning the selling and purchasing of drugs and weapons, human trafficking and money laundering is all possible. There is no need to provide any form of identification to purchase bitcoin and it cannot be traced back to a user making it a great asset to those who advocate for privacy, especially online. Government agencies have had to come up with unique and inventive ideas to track down these online criminals who can be anywhere in the world and usually have the knowledge and technology to distort their IP addresses, not leaving behind traces that other internet users would. These have posed ethical questions as to how far agents can go to stop illegal activity before it reaches entrapment and violates laws. Since this field of criminal activity is still a relatively new one that is rapidly advancing, establishing laws such as the Computer Misuse Act (2003) and following the RIPA Act (2000) has been vital in convicting online offenders. This chapter aims to understand how criminals are utilising all the mentioned resources to take part in illegal activity, and largely getting away with it. I seek to understand the shortfalls and loopholes within the criminal justice system and provide recommendations on how to address these ethically whilst keeping up with rapid technological advances.

2 Background

2.1 The Layout and Purpose of the Web

The concept of a worldwide communications and information platform was initially discussed in memos written by J. C. R Licklider in 1962, whereby the idea of the Galactic Network was envisioned. In essence, what Licklider was laying out is extremely similar to what is known as the internet today. A "globally interconnected set of computers through which everyone could quickly access data and programs from any site" [18]. In 1966, a proposal was put forward for a digital communications network whereby Donald Davies coined the word packet, a "small

subpart of the message the user wants to send" and later introduced "the concept of an "interface computer" to sit between the user equipment and the packet network". Though a lot simpler than what is known of the internet today in 2021, these beginnings remain the foundation of the technology that is used to communicate and store data online. By 1969, the 'connecting' began, meaning four computers were then able to communicate with each other via the 'ARPANET' [2]. Through development of the ARPANET, the first mail communications were sent in 1972 via traditional circuit switching methods and "special purpose interconnection arrangements between networks were another possibility". In 2021, users now have access to a range of websites with a multitude of purposes at the click of a finger. Search engines, such as "Ask Jeeves", "Google", "MSN", and "Yahoo!" can take a user to a host of websites such as books, online shopping, social media etc. These are public webpages whereby your I.P address is tracked across sites and does not require authentication or permission to access. "The other content is that of the Deep Web, content that has not been indexed by traditional search engines such as Google." [9]. Using specialist software such as The Onion Router (TOR), users can navigate the deep web to find otherwise hidden webpages. TOR was created with legitimate purposes by the U.S. Naval Research Laboratory as a tool for anonymously sending sensitive information online. "Those who run dark websites that end in ".onion" are able to hide their identities and locations from most, if not all, Internet users" [7] making it extremely difficult once found, to prosecute those that are involved in the selling or distribution of illegal content or materials.

2.2 The Layout and Purpose of the Web

Since the internet is used for communications and intelligence and stores a lot of information, there are ways in which this has been exploited. Cyber trespassing occurs when crossing boundaries into other people's virtual property and/or causing damage to it. Whilst a relatively simple concept, establishing when a boundary has been crossed and whether there was malicious intent behind the action is still a debated one. Cyber theft is another type of crime committed whereby an individual steals online property including money, personal information to be used for fraud, intellectual property, and piracy. According to NFIB Cybercrime Assessment 2020/21 the top three instances of cybercrime were:

- Hacking social media and email—13,948 reports
- Computer Virus/Malware/Spyware—7,794 reports
- Hacking Personal—5,587 reports.

The key enablers of this were 'phishing emails' in which an individual clicks a link to what seems like a credible website, follows the link and enters their sensitive information. The report also found that users had weak or the same passwords across multiple platforms, meaning the hackers were able to access more than initially intended. Contrastingly to stereotypical fraud whereby the high-risk victims were

aged 65+ [22], the high-risk age categories identified by the National Fraud Investigations Bureau for cybercrimes were aged between 20 and 39. These crimes typically target users and take place on the surface web. With an added layer of anonymity that is provided by the deep web, far more malicious crimes can take place. The assumed anonymity of using a router such as TOR to distort the users IP address, making them harder to locate means that the deep web has become a gateway for criminal activity. With the advances of digital currencies such as bitcoin, it means that users can trade illicit content such as child pornography as well as use sites for human trafficking and the selling/purchasing of illegal drugs and weapons.

3 Challenges

3.1 Ethical Hacking or Blatant Computer Misuse?

There is a blurred line of ethics when it is discussed what information should be public knowledge and what should remain private within organisations. Simply defined, hacking is "the unauthorised use of, or access into, computers or networks by exploiting identified security vulnerabilities" [6]. When looking at the case of Raphael Gray, the teenager who hacked into and published over 6,500 pieces of stolen credit card information, there is a clear ethical challenge. This was done as a statement to corporations about their weak security defences. Gray considered his actions not only ethical but needed and encouraged others to do as he did and controversially received praise from a lot of the public. His defence included that obtaining this information was legal as the on these sites, "because there was no warning that access was prohibited" [12]. The cost of closing the accounts and redistributing cards to those who had their information stolen by Gray, was set at an estimated cost of $3m [3]. The average cost of a data breach reached U.S. $6.53 million in 2015 [11]. When the Sony PlayStation Network was hacked, "compromising the personal and financial information of more than 77 million user accounts" [21] in 2011, it was the largest recorded data breach of the time with the direct costs estimated at $171 million.

3.2 When Cybertrespass Is a Crime

As previously mentioned in the case of Raphael Gray, establishing that a cybercrime has taken place can be challenging however the introduction of the Computer Misuse Act (2003) has sought to clarify to prevent cases like this happening again. Whilst establishing cyber trespassing, if there is no contract established between the two parties it is difficult to decipher whether a crime has taken place. In a review of Unauthorised access as legal mechanisms of access control, Wong sets out that;

"Like their US federal counterpart, the UK and Singapore computer misuse statutes also reveal a property-based notion of computer crime, as well as a lack of clarity or definition as to the concept of 'unauthorized access'" [24]. This is where the first legal challenge of cybercrimes begins. As there is no geographical crime, it cannot simply be compared to breaking into a house and classifying the act as trespassing, as there is no physical house only virtual boundaries and walls. However, much like the physical counterpart, clues are left behind and it is the role of Digital Forensic analysts to find these traces left behind. Causing a computer to perform a function can be as simple as opening an unauthorised file to as complex as hacking and stealing information.

3.3 Ethical Considerations of Police Using the Dark Web

Honey traps are a technique used by undercover agents to gain access to a user's IP address if they are committing illegal activities online. The ethical use of honey traps have been debated due to the lack of evidence for its efficacy. "There is no defence of entrapment in English law, but it is considered to be an abuse of the process of the court for state agents to lure a person into committing illegal acts and then seek to prosecute him for doing so" [20]. In 2015, a notorious darknet site called 'Playpen', hidden through the TOR network was uncovered by the FBI. "Playpen hosted 215,000 user accounts and distributed 50,000 images of child pornography before the site was taken down" [8]. After its discovery, the FBI infiltrated the site and maintained it for 14 days in an attempt to monitor its users hoping it would lead to arrests where the FBI injected the site with malware to crack TOR's anonymity of IP addresses. "The Justice Department has said that children depicted in such images are harmed each time they are viewed, and once those images leave the government's control, agents have no way to prevent them from being copied and re-copied to other parts of the internet" [14]. According to the United States Government statistics, as a direct result of the operation to seize the darknet site Playpen, there were 350 U.S. arrests and 548 international arrests. When directly compared to the number of users on the site, this means that 0.42% were arrested and of those 200 are active prosecutions as of May 2017.

3.4 Bitcoin and the Illicit Use of Cyber Currencies

The emergence of bitcoin was not only revolutionary in the tech world but changed societies globally. To have use of a currency that isn't controlled by any national government was a first and for liberal thinkers, a step in the right direction for freedom of privacy. The development of a digital currency also revolutionised the use of the dark web, meaning that the layers of anonymity already created were greater facilitated by the means to make untraceable transactions via bitcoin. Bitcoin

"has a value proportional to the credibility attributed to it, the fees involved in the transactions are low, have no limits of territorial use, cannot be frozen or confiscated and have no prerequisites for use or limits imposed per transaction (any amount may be transferred to any person, by any person, to any person, without prior authorization or further justification) [15]. This is the greatest invitation for users of bitcoin, from a simple set up with low fees and no risk, it is the safest way to trade online, along with its complete anonymity. The introduction of cyber currencies has allowed online transactions to be treated with the same level of anonymity as cash transactions in the real world, which is welcomed by many that advocate the right to privacy of expenditure. However, bitcoin quickly became the number one currency used on the dark web and has been linked to many online crimes. Most notorious is that of Silk Road and its seizure by the FBI in October 2013. The darknet site was large on a scale not seen before and was an intricate, well organised operation that quickly grew into a community that dealt with the trade of illegal substances. According to the FBI's criminal complaint filed in Ross Ulbright's trial, the Silk Road market had almost 150,000 buyers and almost 4,000 vendors [23]. Since the trading involved the sole use of bitcoin, detecting any venders or buyers was a virtually impossible task due to the complex combination of TOR and bitcoin with users taking great care to conceal their IP addresses. "Silk Road used tumbler to process Bitcoin transactions as well as tracking individual transactions through Bitcoin blockchain. When a buyer buys something and makes the payment on the website, the tumbler would obscure the link between the buyer's and vendor's Bitcoin addresses" [16].

3.5 Digital Forensics and Criminals

Technology has advanced rapidly which means that lay users of the internet have access to numerous software and Cloud storage not previously available. With the sheer number of users of the Cloud, Google Drive and Dropbox a new challenge has emerged in the field of Digital Forensics. Unlike traditional storage, when information is stored on the cloud it is distributed into multiple nodes rather than a single node. "Due to the distributed nature of cloud services, data can potentially reside in multiple legal jurisdictions, leading to investigators relying on local laws and regulations regarding the collection of evidence" [10]. Not only does this cause legal complications in compiling evidence, but it also leads to significant time delays. The chain of custody that must be followed becomes more difficult due to the nature of multiple nodes making traditional DF technology redundant. This creates a real 'needle in a haystack' scenario for investigators and criminals are utilising these advances in technology more and more to conceal files and remain undetected, without the use of the deep web.

4 Recommendations

4.1 Rectifying the Mistakes of the Playpen Operation

Regarding the darknet site Playpen seized by the FBI in 2015, there are several steps which could have been taken to protect the vulnerable children subject to online abuse. Whilst the investigation was effective in successfully identifying or rescuing 55 American children [8], there are clear safeguarding risks that were not considered. By allowing the website to run for a further 14 days, the FBI allowed the victims of the online abuse to have their material downloaded and possibly redistributed an infinite number of times. The priority of the FBI should have been to safeguard these victims and not provide further harm, as they did. Technology is ever advancing, and an operation could have been as equally effective using such advances. The use of deep fakes or CGI rather than real images of abused children could have reduced harm to the victims resulting in a more ethical investigation. There is no significant data that determines honey traps as the most effective method of policing the dark web and until data supports its use then alternatives should be fully explored before its complete implementation as a standard operation procedure of policing.

4.2 The Next Steps of Digital Forensics

Digital forensics is an extremely important field of technology and must continue to adapt itself to advancing software to adequately support the criminal justice system. "Since December 2010, in the Netherlands a new approach is used for processing and investigating the high volume of seized digital material" [1] using 'Digital Forensics as a Service' or 'DFaaS'. Due to the introduction of the storage spaces such as the Cloud, the time it takes for digital forensic analysts to retrieve information can be an extremely lengthy process. Most crimes now include some cyber element in which an analysts will be brought in to aid the police. However, when they are brought in and what they are asked to investigate varies. This model, which works as an extended process to typical digital forensics, claims to save an invaluable amount of time harvesting data for an investigation. "At a large scale it makes sense to implement a central system that can be used by multiple departments. With this model, it is expected that the system spends less time idling and more time processing data. If digital material becomes available sooner in the investigation, it can be used to form hypotheses instead of only using it to test hypotheses" [1]. There is a clear need for and gap in the market for resources such as these and as criminals get more technologically complex. It is time for the justice system to make provisions, even if this means outsourcing services to better aid their digital investigations. The process is by no means perfect however more funding and research in this field is an investment worthwhile to aid investigators and create a smoother process for criminal proceedings.

4.3 The Standardisation of Law for Cryptocurrencies

There is a clear lack of deterrence for online criminals due to the unclarified legality of cryptocurrencies. Although currencies such as bitcoin are converted from 'real' state currencies, they are still not regarded as a form of tender in most countries creating a legal loophole when cases of money laundering using bitcoin arise. As more users adopt cryptocurrencies as forms of transaction, at the very least there should be standardised legal definitions globally to enable criminal justice systems to prosecute those using it illegitimately. There also needs to be a consideration for the global carbon footprint effects that arise due to 'mining'. It is estimated, that if bitcoin alone were a country, it would use more electricity that Argentina [5]. Bitcoin is arguably one of the most stable currencies to protect against fraud and can be utilised by users safely and legitimately. The mining process verifies each transaction which "makes it extremely difficult for bitcoins to be double-spent or counterfeited" [17] this is a feature that credit card companies currently lack.

5 Discussion

There are clearly many different resources currently available to users to facilitate cybercrimes and new technology is advancing rapidly. The field of Digital Forensics is becoming increasingly complicated due to a number of factors, and it is becoming easier for cyber criminals to conceal their data. "Evidential data is no longer restricted to a single host but instead spread between different or virtual locations, including: online social networks, cloud resources, and personal network–attached storage devices" [19]. New advances, including DFaaS should be a welcomed collaboration to combat the growing number of cyber facilitated crimes to ensure criminal justice services are able to keep up the demand and ultimately reduce harm to users creating a safer space. The investigation process has clear flaws when identifying illicit websites, especially on the dark web. A standardised way of proceedings is necessary, not only to mitigate victim harm but again, to aid investigators when these websites are discovered or reported. Cyber law is also a field that requires more collaboration. Since it is difficult to establish the geographical elements of cybercrime, it is in the interest of all governments to ensure that they are working with the same or similar proceedings due to the legality loopholes that offenders seem to uncover. There is a clear need for the deep web and the services it provides are invaluable when used legally. As more advocates for online privacy arise, it is likely that an increasing number of users will migrate to using services such as TOR or I2P for everyday use. When the number of users grow and begin to protect their anonymity online, digital investigators will have to develop new means in which they are able to detect users they believe are exploiting the anonymity features. As cryptocurrencies are concerned, they are still a relatively new concept to many users. With the many protective features of bitcoin, its stability is dependent on its users, and it is uncertain

at this time whether it will ever be able to function as an everyday global currency. The collaboration of governments will have an impact on cryptocurrencies, with many observing El Salvador as a model of its success or failure.

6 Conclusion

The deep web's sole purpose is clearly not to aid criminal activity, and it has many practicalities for its users and as an invaluable business resource for both corporations and governments. It is clear however, that many of its features are designed in a way that easily facilitates illicit activity. There must be more clarity concerning cyber laws and computer misuse for all users to determine illicit activity quickly and effectively. As anonymity in all service arise, digital forensics must adapt its method of investigations to limit criminal behavior and safeguard all users of the web. Further monitoring of cryptocurrencies is needed to detect trends in who is using them and the extent to which it is being used for legal or illegal services. Digital investigators must continue to monitor the dark web as long as illicit materials are being shared, carefully considering not to cross boundaries and document their investigations clearly and thoroughly allowing users to still maintain their rights to anonymity online.

References

1. Banda R, Phiri J, Nyirenda M, Kabemba M (2019) Technological paradox of hackers begetting hackers: a case of ethical and unethical hackers and their subtle tools. Zambia ICT J 3(1):40–51. https://doi.org/10.33260/zictjournal.v3i1.74
2. Bay M (2019) Conversation with a pioneer: Larry Roberts on how he led the design and construction of the ARPANET. Internet Hist 3(1):68–80. https://doi.org/10.1080/24701475.2018.1544727
3. BBC News | WALES | Teen hacker escapes jail sentence (2001). http://news.bbc.co.uk/1/hi/wales/1424937.stm. Accessed 3 Jan 2022
4. Bergman M (2001) White Paper: the deep web: surfacing hidden value. J Electron Publ 7(1). https://doi.org/10.3998/3336451.0007.104
5. Cambridge Bitcoin Electricity Consumption Index (CBECI) (2021). https://ccaf.io/cbeci/index. Accessed 10 Jan 2022
6. Cybercrime—prosecution guidance | The Crown Prosecution Service (2021). https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance. Accessed 3 Jan 2022
7. Dingledine R, Mathewson N, Syverson P (2004) Tor: the second-generation onion router. ACM Digital Library
8. Farivar C (2017) Creator of infamous Playpen website sentenced to 30 years in prison. https://arstechnica.com/tech-policy/2017/05/creator-of-infamous-playpen-website-sentenced-to-30-years-in-prison/. Accessed 11 Jan 2022
9. Finklea K (2017) Dark web. Congressional Research Service. http://www.crs.gov
10. Focus F (2016) Current challenges in digital forensics—forensic focus. https://www.forensicfocus.com/articles/current-challenges-in-digital-forensics/. Accessed 11 Jan 2022
11. Goode S, Hoehle H, Venkatesh V, Brown S (2017) User compensation as a data breach recovery action: an investigation of the Sony PlayStation network breach. MIS Q 41(3):703–727. https://doi.org/10.25300/misq/2017/41.3.03

12. Gray (2001) https://www.theguardian.com/technology/2001/jul/06/security.internetcrime
13. Hatta M (2020) Deep web, dark web, dark net. Ann Bus Adm Sci 19(6):277–292. https://doi.org/10.7880/abas.0200908a
14. Heath B (2016). https://eu.usatoday.com/story/news/2016/01/21/fbi-ran-website-sharing-thousands-child-porn-images/79108346/. Accessed 11 Jan 2022
15. How do bitcoin and crypto work? | Get started with Bitcoin.com (2016). https://www.bitcoin.com/get-started. Accessed 6 Jan 2022
16. Kethineni S, Cao Y, Dodge C (2017) Use of bitcoin in darknet markets: examining facilitative factors on bitcoin-related crimes. Am J Crim Justice 43(2):141–157. https://doi.org/10.1007/s12103-017-9394-6
17. Lee D (2015) Handbook of digital currency. Bitcoin, innovation, financial instruments, and big data. Elsevier Inc., London
18. Leiner B, Cerf V, Clark D, Kahn R, Kleinrock L, Lynch D et al (2009) A brief history of the internet. ACM SIGCOMM Comput Commun Rev 39(5):22–31. https://doi.org/10.1145/1629607.1629613
19. Montasari R, Hill R (2019) Next-generation digital forensics: challenges and future paradigms. In: 2019 IEEE 12th international conference on global security, safety and sustainability (ICGS3). https://doi.org/10.1109/icgs3.2019.8688020
20. Nexis L (2021) Entrapment | legal guidance | LexisNexis. https://www.lexisnexis.co.uk/legal/guidance/entrapment. Accessed 11 Jan 2022
21. Richmond S, Williams C (2011) Millions of Internet users hit by massive playstation data theft | alternative | before it's news. https://beforeitsnews.com/alternative/2011/04/millions-of-internet-users-hit-by-massive-playstation-data-theft-591301.html. Accessed 11 Jan 2022
22. UK A (2021). https://www.ageuk.org.uk/latest-press/articles/2019/july/older-person-becomes-fraud-victim-every-40-seconds/. Accessed 10 Jan 2022
23. USA v. Ross Ulbricht (Southern District of New York 2013)
24. Wong M (2006) Cyber-trespass and "unauthorized access" as legal mechanisms of access control: lessons from the US experience. Int J Law Inf Technol 15(1):90–128. https://doi.org/10.1093/ijlit/eal014