The Dark Web as a Phenomenon: A Review and Research Agenda

COMP90019: Distributed Computing Project (25 pt)

Conventional Research Project

Abhineet Gupta - 719080

The University of Melbourne

Semester 1, 2018

Supervisors:

- **Dr. Atif Ahmad**
- **Dr. Sean Maynard**

Abstract

The internet can broadly be divided into three parts: *surface*, *deep* and *dark* among which the latter offers anonymity to its users and hosts. The dark web has become notorious in the media for being a hidden part of the web where all manner of illegal activities take place. The more restrictions placed upon the free exchange of information, goods and services between people the more likely there exist hidden spaces for it to take place. The 'black market' of the internet – the dark web - represents such a hidden space. This review looks at the purposes it is widely used for with an emphasis on cybercrime, and how the law enforcement plays the role of its adversary. The review describes these hidden spaces, sheds light on their history, the activities that they harbour – including cybercrime, the nature of attention they receive, and methodologies employed by law enforcement in an attempt to defeat their purpose. More importantly, it is argued that these spaces should be considered a phenomenon and not an isolated occurrence to be taken as merely a natural consequence of technology. The review is conducted by looking at existing literature in academic journal databases. It contributes to the area of the dark web by serving as a reference document and by proposing a research agenda.

Academic Declaration

I certify that:

- this thesis does not incorporate without acknowledgement any material previously submitted for a degree or diploma in any university, and that to the best of my knowledge and belief it does not contain any material previously published or written by another person where due reference is not made in the text.

- clearance for this research from the University's Ethics Committee was not deemed necessary given the scope of this work.

- the thesis is ~9800 words in length (excluding text in images, bibliographies and appendices).

Acknowledgements

I would like to thank both of my supervisors – Dr Atif Ahmad and Dr Sean Maynard – for their encouragement, ideas, support and eagerness that permeates this work and manifests itself in the successful completion of this scholarly endeavour over the course of the whole semester.

I would also like to thank my partner for her continual support in enabling me to devote a significant amount of time to this exercise.

Table of Contents

List of Figures

List of Tables

1. Introduction

The internet has been a catalyst for significant change in the modern world. Its decentralised nature coupled with relatively low levels of regulation have allowed for its use in a plethora of ways. It provides global connectivity and renders the concept of distance and location near irrelevant (Broadhurst, 2017a) as signals travel at the speed of light. Geographical separation is thus not a barrier for engagement unlike in the physical world. Proponents of collaboration would argue that such a high level of interactivity between many people means the world is better off. However, unlawful activity can also scale up as attribution becomes more and more challenging and the fear of legal consequences are reduced. This is made possible by new technologies, and due to borders (or lack thereof) – in geography and jurisdictions – which do not map well from the digital to the physical world.

One such digital environment on the internet is the *Dark Web* or *Darknet,* with the *Tor Network* being the largest deployed anonymity network (The Tor Project, 2018a). This overlay network – a distributed system – affords its users anonymity and makes attribution for activities challenging by encrypting and routing users' traffic via multiple nodes (The Tor Project, 2018b). The most popular version of the dark web – The Onion Routing (Tor) network and protocol – has become a haven for criminals to conduct their operations, including sharing illegally-acquired information, trading illicit contraband, and recruiting others – all with disregard for borders and legality (Chen et al., 2008; Dalins et al., 2017; Ghappour, 2017; Vogt, 2017).

The dark web became popular with the launch of *Silk Road* – a drug marketplace – in 2011, and also by its demise in 2013 (Phelps and Watt, 2014; Van Buskirk et al., 2014). Ever since, it has been notorious for being a place focused on facilitating the trade of illicit drugs, and one which is increasingly being targeted and monitored by authorities. As per popular media, it would seem that this trading is the main activity on the dark web and that law enforcement's increasing involvement is leading to a decline in drug marketplaces, especially with the recent shut down of Hansa and AlphaBay (Bugge, 2017).

The motivation behind this literature review is to gauge the current state - and growth - of the dark web in relation to the roles it plays, investigate how the dark web enables cybercrime, and examine law enforcement's efforts. More specifically, the following research questions are under focus:

i) What general roles does the dark web currently serve given its existence?
ii) What significance does the dark web have in cybercriminal activities and operations?
iii) How successful is law enforcement in its attempts to curb illegal activity on the dark web?

We also investigate the existence of the dark web as being a phenomenon that is increasing with growing regulation, surveillance and law enforcement (LE) capabilities. The nature of activities occurring on the dark web – more specifically the Tor network – are investigated and categorised as part of a literature review. Additionally, its resistance to law enforcement is examined based on the methods by which LE has curbed operations on the network. We then speculate on the future of the dark web phenomenon and how it is overcoming its current bottlenecks in achieving its intended goal. Finally, a research agenda is proposed to continue research on such phenomenon and allow for better predictions on how it may unfold over time and as technology improves.

2. Research Method

A major initial challenge of performing a literature review includes identifying and structuring the most relevant literature surrounding the topic. The primary approach taken for this included performing a keyword search with filters in major databases, going backwards and forward, i.e. reviewing citations for key articles, and reviewing material which cites those key articles, respectively (Webster and Watson, 2002). A PAFMRQ-style analysis (Mathiassen, 2017) was conducted on the topic to better articulate the task at hand (Appendix 6.1).

2.1 Sources and Keywords

Search engines which index academic content from databases and journals were used to search for literature. The two primary sources used for this were *EBSCOHost*[1] via the University of Melbourne's library services and *Google Scholar*[2].

The identification process, described below, was adapted from Mathiassen et al. (2007). The broad keywords used for the searches initially included "dark web" or "darknet" as these represented the main idea under investigation. Once Tor was determined to be the most popular version of the dark web, "tor" and "tor hidden services" were added to the keyword list. The search was also restricted to contain articles only published in the last five years, i.e. 2013-current. Due to the results being broad in nature, a random selection of papers was reviewed, and key themes of research around the dark web identified. From these, the themes of interest were then searched for specifically along with the main keyword ("dark web") by adding keywords like "markets", "cybercrime", future", "tor hidden services", "incident response", "information warfare" and "threat intelligence" one at a time. These additional keywords were used to allow a more detailed discussion on each aspect of the topic. This keyword search was completed on 13th April 2018 and a list of 151 journal articles, books and theses was compiled.

2.2 Filtering for Ranking and Relevance

From the list, papers published in leading journals were identified via the use of *Computing Research & Education* Journal Portal (CORE, 2018) and *ACPHIS* Journal Ranking (ACPHIS, 2018). However, such papers were a small minority (<10%). Overall, there is limited availability of research which focuses on the dark web itself, and not just mentions it in passing. This may be due to multiple reasons, and the restrictive nature of the topic which makes it difficult to collect data on is speculated to be one of them. By nature, Tor Hidden Services are not indexed on a search engine which makes it necessary to

[1] https://library.unimelb.edu.au/
[2] https://scholar.google.com

manually compile a list of *'.onion'* addresses before they can be crawled. Additionally, users of the dark web are by nature anonymous which makes it difficult to collect data about them e.g. geography. While the Tor Metrics project does present numerical data around Tor's usage, details of the traffic flows remain unknown. These two limitations: lack of collectible metadata and unindexed web content, in combination with specialised software required to access the network, make the dark web not a well-researched, or published, topic in academic literature.

The list was then used to populate a concept matrix based on a brief reading of each article. Papers were then manually filtered for stronger relevance by selecting only those which focused on the dark web and not merely considered it as a peripheral relevance. This resulted in 41 articles in the final list.

3. Discussion of Literature

The internet has become the basis for a global online community of people from all over the world interacting with each other on a scale and a rate unprecedented in history. It has enabled the formation of a global digital society that transcends boundaries, be they nationalities, legal jurisdictions, race, religion, and others. This society, despite its amorphous nature, still constitutes of individuals bound by the laws of their country and similar restrictions. The governments have policies in place which allow for prosecution of said individuals if they were to participate in illegal behaviour. For example, file sharing of illegal or copyrighted content online could be considered a breach of law and could result in legal prosecution of the people involved. This is possible because online identities, mainly IP addresses, are linked to the individuals or websites who possess them. In the case of a home desktop computer, the IP address assigned to it by the Internet Service Provider (ISP) is logged as such under the account holder's identity. This IP address is also logged by any service requested from that computer, e.g. by a news website. When this level of logging and accountability is extrapolated across the web, and internet, attribution for most activities conducted online - without precaution - is easy to perform especially for law enforcement as they can either monitor traffic on their own or request logs from those who possess them. Even companies which store our data privately must comply with the rule of law and hand over personal data if subpoenaed under a valid warrant. Therefore, the idea of digital anonymity – a lack of attribution between a digital identity and a physical one – is an important one and forms the basis of our discussion that follows.

3.1 Classification of Internet Spaces

It is worth discussing the internet under the three broad categories that result from analysing its components with the following two attributes: public vs private and accountable vs anonymous.

The first category is the *surface web*. This refers to parts of the internet considered public and accountable. It is public because access is not restricted by authentication or payment, indexed by search engines, and it is accountable as the stakeholders (host and user) are identifiable thus subject to law enforcement. The BBC News website is an example: it is publicly accessible by visiting the URL which can be reached via a search engine (e.g. Google or Bing), and it is accountable as the BBC is liable for the content it publishes. The users can also be held accountable for their visit to the website as their visit will be logged by the server – and anyone monitoring the network – providing details like an IP address which can be traced back to them.

The *deep web*, on the other hand, refers to parts of the web not publicly accessible, i.e. private and thus not indexed by search engines, but still subject to accountability. Its access is usually restricted due to authentication requirements or because it forms part of an internal network. One example is

someone's personal account on a bank's online portal. It is private as no one other than the person with the correct credentials can access the webpage. However, all participants (user and bank) remain identifiable to each other. This accountability in some ways is even stronger given authentication requirements.

Finally, the *dark web*, also known as *darknets* or *hidden services,* is a subset of the network not indexed by search engines because it requires the use of special software for access. It consists of both public and private elements, i.e. accessible publicly or by only those with credentials – provided the correct software is in use. The key difference between the dark web and surface or deep web lies in the lack of accountability present on the dark web. Users are unidentifiable to the network – or anyone monitoring – and their actions are thus effectively anonymised. Furthermore, the dark web allows for hosting of web services (hidden services) which remain anonymous with regards to their true IP address, and thus location, even to the users who use those web services. The difference thus between the dark and deep web is that the former is characterised by unique technology-enabled protocols and anonymity, whereas the latter is more reliant on authentication and thus a lack of public access. Anonymity is not a feature of the deep, and surface, web and both have their unauthenticated parts readily indexed by search engines. By conferring anonymity, private engagements between people have been institutionalised by the dark web.

The above is further illustrated in Figure 1 below (Cambia Research, 2016).

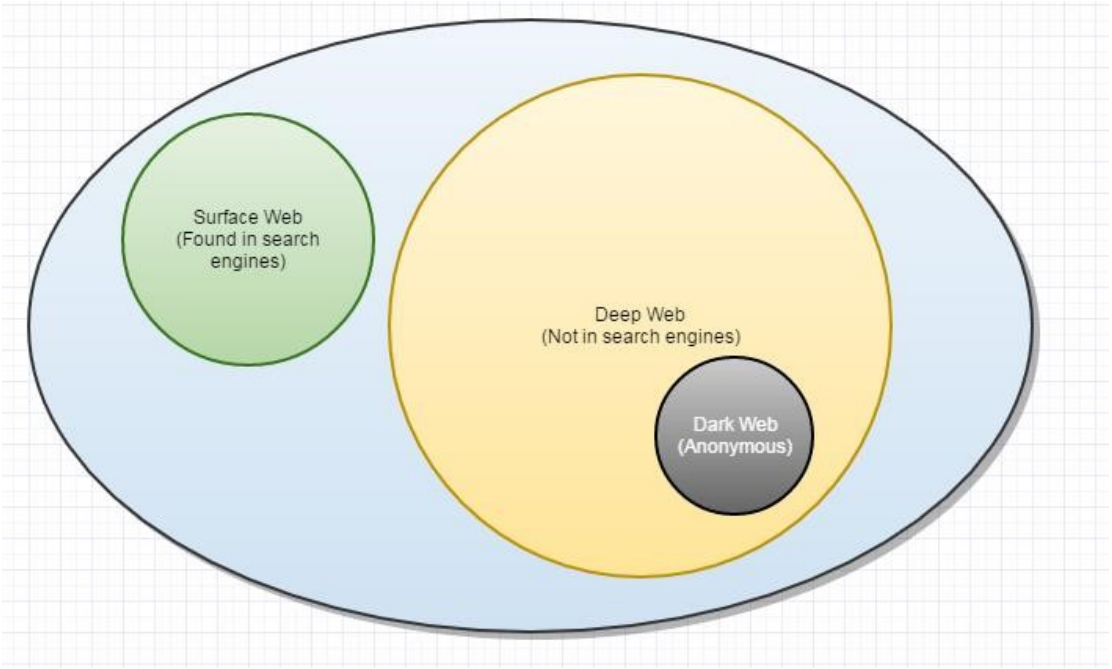

Figure 1: Surface, Deep and Dark Web

3.2 The Dark Web Examined

The dark web is a feature of specific overlay distributed systems that exist atop the global internet. These networks provide the functionality of remaining untraceable and promise to be a haven from prying eyes, mainly law enforcement (LE). Multiple avenues making this promise have existed over the years, and some have been temporary in their popularity and even operation. Technological improvements have allowed for novel ways to enable the dark web to exist and sustain itself longer than before. It is possible that the current generation of tools and networks in use will outlive their predecessors as they learn from their failures and improve upon them.

3.2.1 History of anonymous spaces on the internet

Peer-to-Peer communication has existed as a form of distributed systems since the 1990s in the form of *Napster*, *LimeWire*, *Kazaa*, and other P2P file-sharing systems. These systems have been popular choices for sharing illegal content from pirated media to child pornography (Hughes et al., 2006) as being distributed networks they have had the advantage of being scalable and difficult to shut down (Balakrishnan et al., 2003).

Some surface web platforms with centralised servers have also been used to engage in questionable sharing of information over the years. *Internet Relay Chat* (IRC) has existed since 1988 and continues to be used today for collaboration, e.g. on open source projects. However, before Tor was invented and became famous, IRC was the go-to choice for private communication (Franklin et al., 2007). Another popular centralised platform used in this manner is *4chan* - a message board on the surface web which allows anonymous posting and cybercrime groups like Anonymous to coalesce (Dewey, 2014). The platform maintains a steady participation rate due to its ephemeral nature and encouragement of anonymity (Bernstein et al., 2011). However, posting, or consuming, illegal content via 4chan is still a risky manoeuvre and is likely to lead to prosecution (The Smoking Gun, 2011).

3.2.2 The Onion Routing (TOR) Protocol & Hidden Services

The most popular of the overlay distributed systems promising anonymity, i.e. the dark web, rely on The Onion Routing (TOR or Tor) protocol accessible via the Tor browser (The Tor Project, 2018b). The Tor browser can be used to access websites normally accessible on the surface web, but with added privacy, as the source IP is nearly unidentifiable. This is possible because the Tor protocol sets up an encrypted connection to each destination consisting of multiple nodes along the way which act as relays. These relays include the *entry* (guard) node, *middle* relay and an *exit* node. These nodes are selected from a collection of thousands of Tor relays and bridges that make up the network and are operated voluntarily by organisations and individuals. This system, when combined with public-key cryptography and layering of traffic in such a way that for each connection a node is only aware of its

neighbouring nodes, means that any one participant in the network never has complete knowledge of the identity of any end-to-end communication channel. For many users, the prime reason for using an overlay network like Tor is not just for anonymous access to regular websites, but to access a range of websites that are not otherwise accessible on the surface web, except for only via the Tor network. This exclusive digital space and collection of websites are collectively referred to as the *Dark Web, Darknet* or *Tor Hidden Services* (Broadhurst et al., 2017).

3.2.3 Dark Web as a Distributed system

The most prominent manifestation of the dark web – the Tor network – works by routing internet traffic via multiple nodes, each of which is only aware of the sender and destination in their immediate vicinity and thus unaware of the original sender and destination of that traffic. Much like the Internet, and because of it being an overlay, the dark web exists on a system which is decentralised – and to an extent distributed - in nature with no central servers or point of control. This leads to an inability to quickly shut the system down (Tanenbaum and Van Steen, 2007) and facilitates interactions between people which could otherwise be regulated by legal authorities.

The Tor overlay network exists only to the extent that internet-connected hosts are running the Tor software allowing them to function as relays and bridges for other users. This is a distributed system with no governing or operational authority and thus its expansion, and reduction, depends primarily on the hosts which willingly form a part of this network. Many organisations such as activist groups that promote human-right causes or universities promoting open access to knowledge resources are known to actively donate bandwidth to this cause and run relays (Owen and Savage, 2016).

3.2.4 Accessing the Dark Web

The different dark web networks – I2P, Freenet, Tor – all have their mechanisms for participation. Tor being the most popular is also the one focused on in this review. Given access to the internet, accessing the Tor network is as easy as downloading the Tor browser – a modified version of the open-source Firefox browser[3] – and accessing websites and hidden services just the same as one usually would on the surface web. The method is near transparent from an end user's perspective. Once downloaded and installed, the Tor browser retrieves a list of Tor nodes from a directory server, chooses three (or more) nodes from the list, retrieves all cryptographic keys required to encrypt packets and sets up a virtual circuit through the network (see *Figure* 3 below (The Tor Project, 2018b)). Each packet sent from the browser is encrypted with the keys of all nodes along this circuit and passed on to the first node. The first node decrypts only the first layer – corresponding to its cryptographic

[3] https://www.mozilla.org/en-US/firefox/new/

key – and passes on the still-encrypted packet to the next node which repeats this decryption in a manner similar to peeling off layers of an onion (hence the name 'onion routing'). Only the final/exit node sees the original packet and passes it to the destination. The original packet even though not encrypted as part of the Tor circuit may still be encrypted as part of other encryption protocols being used between a browser and website, e.g. HTTPS.

3.2.5.1 Using Tor vs a VPN Service

Using the Tor network in the interest of anonymity can also be compared to using a third-party Virtual Private Network (VPN) service (Hotspot Shield, 2018). A VPN service provides an endpoint that all generated internet traffic is sent to which then gets routed out to the internet from the VPN provider's gateway (see Figure 2 below from Bradley (2018)).

The difference between a VPN and Tor, thus, is that: a) a VPN adds only a single hop/node through which traffic is encrypted and routed whereas Tor does this over three other nodes; b) a VPN provider – being a third party – may keep logs of its connections which would allow for the linking of the source and destination of all packets i.e. deanonymize the user, whereas Tor is built on a protocol which ensures that no single node has sufficient information to be able to perform deanonymization. Moreover, hidden or *onion* services can only be accessed over the Tor network.

Figure 2: How a VPN works

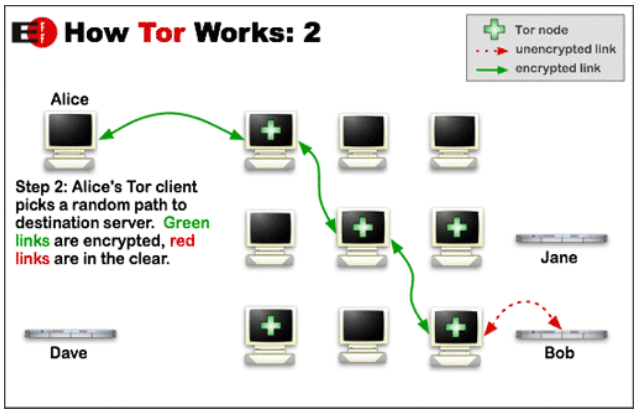

Figure 3: How a Tor connection works

3.2.5 Dark Web as a Phenomenon

The dark web's original offer of anonymity and lack of attribution to a real-world entity makes it a lucrative place for activity that would otherwise be hindered by government control (Weimann, 2016a). There are many ways in which this aspect of the dark web manifests itself. These include having marketplaces for illegal contraband; partaking in social interactions involving training, recruitment and propaganda on controversial topics; conducting and facilitating financial transactions

without a paper trail; and others discussed in later sections (Chertoff and Simon, 2015). All of these are features typical of a black market economy which in itself is a consequence of the market phenomenon of parties engaging in exchange (Ablon et al., 2014). The existence of a digital space which encompasses the above functions, people and technologies could suggest that the dark web is not just a technological product, but is a *phenomenon* arising from a need for secrecy and anonymity between members of a community, similar to that of a physical-world black market existing from a need for unregulated exchange of goods and services between individuals.

Also similar to a black market, the dark web's hidden services, or at least those with illicit content, are the main reason behind the dark web's adversarial relationship with law enforcement. LE attempts to shut down certain hidden services or to deanonymize its users while at the same time participants in this phenomenon find ways to mitigate those attempts. The common goal of anonymity and trading has brought together people in a sort of global private space that is indifferent, and immune to an extent, to local jurisdictions in which their participants reside. The bestowment of anonymity on willing global citizens has translated into a market-based society of its own which tries its best to resist outside efforts of disruption.

3.4 Major Roles of the Dark Web

The promise of anonymity on the dark web opens itself up for use in multiple ways. Some legitimate reasons include civilians looking for protection from irresponsible corporations, censorship, ability to research into sensitive topics without concerns; militaries hosting hidden command and control services, journalists conducting their operations in countries without access to free media and speech; law enforcement performing sting operations, activists and whistle-blowers reporting abuses and speaking out against governments. All of these are applications which necessitate use of the dark web in some countries while not necessary in others (Chertoff and Simon, 2015) due to the variation in the legal landscape across nations.

While not all scenarios that benefit from anonymity are by default illegal, the dark web phenomenon indeed enables a fair share of illegal activities. One of these is providing adversaries – cyber threats – with an enabling infrastructure. This infrastructure includes command-and-control endpoints for botnets, markets allowing zero-day exploits to be traded, hackers for hire, private communication, coordination for attacks, variable-sized botnets for hire to launch DDoS attacks and pawning of breached data (Winkler and Gomes, 2016).

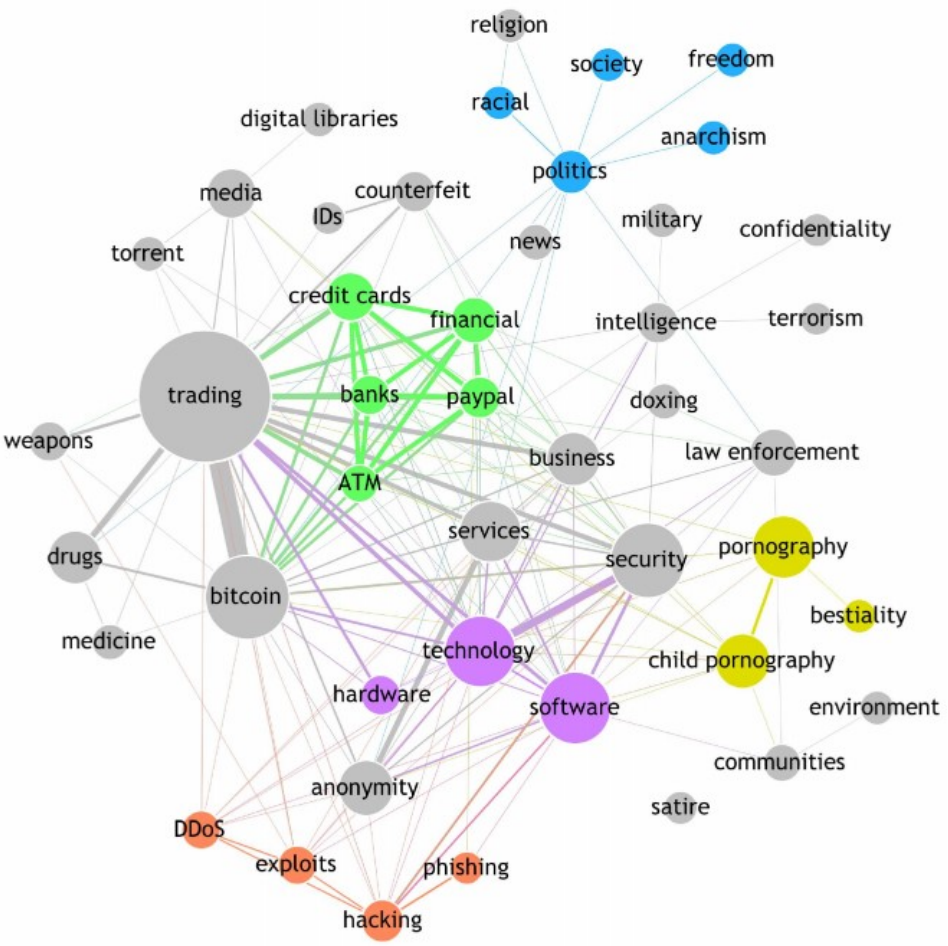

Figure 4: A topic taxonomy of Tor Hidden Services, as a graph.

The graph in *Figure* 4 above (Spitters et al., 2014) is a representation of the various topics about which Tor hidden services – at least those with a website front – exist. [Size of a node is proportional to its topic presence, and weight of an edge expresses relatedness of the nodes.] Trading of illicit products, laundering currencies to facilitate those trades, security/hacking software, and illicit sexual content make up the top topics present (Spitters et al., 2014).

Furthermore, individuals who wish to remain anonymous in the physical world can have a persona, or pseudonym, which represents them across multiple services online. They can have a stable and consistent presence online while at the same time be physically mobile and always on the move – something that may be a necessary extra step in avoiding legal prosecution in the physical world, especially in the highly collaborative nature of developed countries.

3.4.1 Markets/Illegal Content

Marketplaces like *Silk Road*, *Hansa* and *AlphaBay* have been popular over the years for allowing trade of questionable goods like illicit drugs, weapons, stolen identities, stolen credit card details, child pornography, and others. Silk Road specifically was one of the first major such marketplaces reaching

sales of over USD 1.2 million per month (Christin, 2013) mainly consisting of controlled substances and narcotics. Weapons are also a popular commodity on such marketplaces but remain overshadowed by the sale of illicit drugs (Rhumorbarbe et al., 2018).

The dark web is not the only place for cybercrime groups to sell their skills and products. Surface web forums, including Facebook, have long been used by criminals to offload and sell their services of spamming, fraud, DoS attack-for-hire services, stolen credit card details, among others. However, being on the surface web, these avenues are ripe for easier takedowns (Krebs, 2018) and prosecution.

Breached information is also found for sale on these markets as it provides the criminal, and its acquaintances, anonymity. This data can include the sale financial fraud-related documents, e.g. credit card details or identity theft enabling documents like medical records as these typically have a higher shelf life (Hoffman and Rimo, 2017).

3.4.2 Communication/Recruitment

The deregulated and anonymous nature of dark web networks are of appeal to terrorist groups. Of concern are the violent extremist (VE) groups which conduct terrorist acts across the globe and use the internet's global prevalence in reaching a worldwide audience. This way they can spread their ideologies, conduct recruitment, share knowledge/train, advertise, fundraise, target and form communities overall without concern for geographical separation or even the presence of a local leader (Brynielsson et al., 2013; Chen et al., 2008; Weimann, 2016b, 2016a). This 'leaderless revolution' has been seen in events like the Arab Spring where social media – albeit on the surface web – played a key role in enabling the revolution in multiple countries (Lotan et al., 2011). Comparably, violent extremist groups use the surface and dark web to further their agenda. Similarly, the Anonymous hacktivist group operates its training chat messaging platform on the dark web, for "training the next generation of Hackers" (Anonymous, 2016).

Due to the extensive use of dark web forums for such purposes, they have been the target for various forms of monitoring ranging from manual observation to crawling combined with natural language processing techniques for automated threat intelligence and various other insights (Abbasi, 2007; Chen et al., 2008; Ho and Ng, 2016; Scanlon and Gerber, 2014).

3.4.3 Cybercrime & Terrorism

A general term for someone who gains unauthorised access to a system for malice or personal gain exists - a Black Hat (Springer, 2017). However, given the breadth of actors and intentions involved, a classification system has been proposed to simplify discussion on cybercrime which can be of multiple types: offences against CIA of data/systems e.g. Advaned Persistent Threat (APT) – a highly evolved,

sophisticated and well-resourced threat actor - involved in espionage; computer-related e.g. identity theft; content-related e.g. child pornography, religious opinions in countries where it is illegal; copyright infringements; and a combination of the above e.g. cyberwarfare (Tsakalidis and Vergidis, 2017). The offenders can also be categorised into individuals, e.g. insiders, hacktivists and script kiddies, or entities, e.g. nation state agencies.

Cybercrime has become increasingly accessible to anyone who wishes to engage in low-risk criminal activities while still having an impact on the target. Conducting Distributed Denial of Service (DDoS) attacks on websites is as convenient as hiring a botnet which offers DDoS-as-a-Service (DDoSaaS) (Crawley, 2016), or launching Ransomware attacks on unsuspecting victims via phishing emails which contain malicious attachments or links (Skopik, 2017). These services let malicious actors – script kiddies in this case – pick the 'low hanging fruit,' i.e. targets without adequate security controls or training in place. Moreover, darknets also inadvertently serve as breeding grounds for future law enforcement personnel as these young 'hackers' amass knowledge about this underground infrastructure which later becomes valuable for the role of an information security professional; companies are starting to 'hire hackers' (Crawley, 2016).

Sophisticated attacks involving a command-and-control (C2) channel being maintained between the attacker and the victim can be facilitated by Tor's hidden services. Tor's offer of anonymity and thus difficulty in being shut down is apt for purposes of a C2 server as seen in the fact that one of the most popular hidden services found on the Tor network was botnet C2 services (Biryukov et al., 2014).

Nation states have been expressing their concern at their need to prepare for warfare in the digital realm and realise that physical boundaries are meaningless in this domain (Stoddart, 2016). This is of particular concern in cases where this warfare affects Critical Infrastructure (CI) and Industrial Control Systems (ICS) with the potential to have adverse real-world outcomes (Stoddart, 2016). This ease-of-entry into being a cybercriminal is further helped along given the asymmetry of the warfare environment. Despite the cybercriminals not being as well funded or resourced as the organisations they target, they possess an advantage on the digital battlefield due having the liberty of choosing their tactic, timing and location whereas the defenders are required to be on alert at all times (Ahmad, 2010).

In warfare, deterrence and dissuasion have worked as useful military strategies in the past due to many reasons, one of them being the high barrier of entry into nuclear weapons. However, this does not apply in cyberspace as a weapon can be coded by people on, or bought easily from, the dark web (Nye Jr, 2017). By the same token, deterrence is no longer the domain of governments as sometimes

non-state actors can also become active participants in cyber warfare against common enemies (Nye Jr, 2017).

Law enforcement agencies and hacktivist groups around the world have been active in the reduction of terrorist groups' activities on the surface web (Weimann, 2016a). This has led to their migration to the dark web and made their conduct even more resilient to being disrupted (Denic, 2017; Weimann, 2016b). Supporters can now freely express their opinions anonymously; the groups are less likely to be victims of hacktivists/vigilantes who try to shut down terrorism-related websites, and their operations can continue to be funded via virtual currencies, as discussed later in section 3.4.5. Further to that, the dark web serves as a potential recruitment centre and training ground for newly formed groups or 'lone-wolf' terrorists. The latter has been attributed to a significant amount of terrorist activity around the globe and their identification on the dark web forums via natural language processing is an ongoing effort (Brynielsson et al., 2013).

3.4.4 Cyber Threat Intelligence (CTI)

As there is an established cybercrime community on the dark web, it is also expected for law enforcement and for security product and service providers to be in regular observation of the activities in this space. Usually, antivirus and other security companies have protected its users from malware based on signatures derived from past attacks (Samtani et al., 2017). However, there is a shift towards a more proactive approach to security. Situation Awareness (SA) can be integrated into the Information Security Risk Management (ISRM) systems of organisations (Webb et al., 2014) and part of SA is the collection and processing of data which can help with managing security. This idea has given rise to practices in Cyber Threat Intelligence (CTI) which involves gathering data about up and coming exploits and cybercriminal activity, particularly on the dark web forums (Samtani et al., 2017).

A system in place currently generates over 300 high-quality CTI leads from analysing darknet forums and marketplaces with the use of various data mining and machine learning techniques (Nunes et al., 2016). History shows that CTI would have been of immense value: in Feb 2015 Microsoft identified a Remote Code Execution (RCE) vulnerability in Windows[4]; by April there was an exploit for it available for sale on a darknet market for 48 Bitcoins[5]; and by July a popular banking trojan (Dyre[6]) which affected over half of the world's banking organisations was found to be using that exploit (Nunes et al., 2016).

[4] https://nvd.nist.gov/vuln/detail/CVE-2015-0057
[5] Worth ~AUD 20 000 in April 2015
[6] https://www.symantec.com/connect/blogs/dyre-emerges-main-financial-trojan-threat

Zero-day vulnerabilities - security holes in systems which have not been made public yet and are thus not yet patched – are one of the weapons cybercriminals use to gain unauthorised access to systems. Because these vulnerabilities are unknown to the public and systems manufacturers, malware exploiting them is very likely to go unnoticed and defeat defences like signature-based anti-virus software. Malware exploiting these vulnerabilities is traded on the darknet forums and marketplaces (Bilge and Dumitras, 2012) thus making it even more valuable a resource for observation. Zero-day exploits are particularly of interest as the APT phenomenon is known to use zero-day exploits as a means to gain privileged access to the systems they target (Ask et al., 2013; Tankard, 2011). Furthermore, their creative tactics make it a challenge to handle incidents, even by incident response teams of a high maturity (Ahmad et al., 2015, 2012).

3.4.5 Financial transactions

Finance is an essential aspect of any operation, and its availability (or lack thereof) could be used to predict 'success' in a project. While the majority of financial transactions are traceable to individuals or entities in the real-world, the emergence of cryptocurrencies like Bitcoin (Nakamoto, 2008) has allowed for the near-anonymous exchange of money. This is achieved using *blockchain* – a distributed ledger – which requires no central authority for verification of transactions. This decentralised and distributed form of currency complements well dark web's nature to supply funding for operations without attribution of the source (Broadhurst et al., 2017). However, Bitcoin does not offer anonymity, but pseudonymity, i.e. Bitcoin wallets addresses can be created by anyone without involving personal information, but all transactions associated with an address are public and thus can be monitored. If a wallet address can be linked back to an individual, it would immediately deanonymize their future transactions to and from the same wallet. Thus, it makes sense for the darknet to be used in operating one's cryptocurrency wallets, as a form of extra precautions in preserving one's anonymity. There are multiple 'tumbling' or 'mixing' services in operation which effectively launder cryptocurrency money by transferring chunks through multiple accounts. This makes it difficult to link deposits and withdrawals from a particular digital wallet and to link it to specific transactions which may be under investigation (DiPiero, 2017). Other cryptocurrencies, like Monero, are gaining popularity in an attempt to provide relevant anonymity that Bitcoin does not (Chu, 2017).

Cryptocurrencies are used to facilitate activity on the dark web not just for marketplace payments but also to fund crime – cyber and otherwise. Ransomware victims are typically presented with the option of paying the attacker in Bitcoins in exchange for having their files decrypted (Sabillon et al., 2016).

It is proposed that a well-resourced attacker may be able to compromise the identity of Bitcoin-over-Tor users (Biryukov and Pustogarov, 2015). However, with an increasingly distributed nature of

financial transactions and the markets themselves, it is argued (DiPiero, 2017) that efforts are best utilised in identifying offenders such as sellers and buyers instead of trying to disrupt the technology itself as the technology continually improves and continues to deliver on its promise of anonymity.

3.4.6 Proxy to Surface Web

Many civilians also use the Tor darknet infrastructure to browse the surface web, or hidden service versions of popular websites on the surface web (Lexie, 2016) e.g. Facebook[7] (social media), ProPublica[8] (news), DuckDuckGo[9] (search engine), Blockchain.info[10] (Bitcoin wallet), The Intercept[11] (secure drop for anonymous submissions), and other services which may be restricted locally or provide cause for concern on privacy/ad tracking. Residents in China employ it for bypassing the 'great firewall of China' internet filter which prevents them from accessing many popular services like Facebook, Google and YouTube. Journalists also use the dark web to write about politically sensitive content which may be punishable by the law of their country. Similarly, whistleblowers may communicate with journalists and leak sensitive data to have it published on the surface web, but fear for their safety (Chertoff and Simon, 2015).

3.5 Summary of Roles

Table 1: Roles played by the Dark Web as per literature

Broad Role	Specific Cases	Description
As a Market	*Illicit drugs* traded on markets	All range of drugs from marijuana to cocaine are being sold on eBay-like platforms, e.g. Silk Road 3.0 (Bhaskar et al., 2017; Christin, 2013; Maddox et al., 2016; Rhumorbarbe et al., 2018; Tzanetakis, 2018)
	Malware and exploits – zero-day + known vulnerabilities traded on markets	Exploits targeting a wide range of systems – from specific low-popularity software to prevalent operating system bugs, e.g. WannaCry Ransomware, Eternal Blue exploit (Ablon et al., 2014; Almukaynizi et al., 2017; Armin et al., 2015)
	Credit card, identities, breached	Stolen credit card info, medical profiles, personally identifying information (PII) allowing identify theft

[7] https://www.facebookcorewwwi.onion
[8] https://www.propub3r6espa33w.onion
[9] http://3g2upl4pq6kufc4m.onion
[10] https://blockchainbdgpzk.onion
[11] https://y6xjgkgwj47us5ca.onion

	data made traded on markets	(Broadhurst et al., 2017; Denic, 2017; McCallister et al., 2010)
	Child Abuse media made available on markets or being sold separately	Child sexual abuse images and videos, available for sale. E.g. on the now-defunct *Playpen*[12] (Biryukov et al., 2014; Dalins et al., 2017; Denic, 2017; Kirkpatrick, 2017; Spitters et al., 2014)
	Weapons traded on markets	Guns for sale, especially in countries where banned (Nunes et al., 2016; Rhumorbarbe et al., 2018)
As a Communication platform	*Forums* for discussion	Sharing ideas, knowledge, propaganda, recruitment, training. Used by hackers, terrorists, journalists, citizens concerned about sensitive topics (Abbasi, 2007; Broadhurst, 2017a; Chen et al., 2008; Ho and Ng, 2016; Sapienza et al., 2018; Scanlon and Gerber, 2014)
	Chat for real-time communication	Instant Messaging/Chat facilitated by Tor, e.g. *TorChat*[13], or end-to-end encrypted chat software, e.g. *Telegram*[14] and *Signal*[15], known to be in use for private communication in real-time. (Maddox et al., 2016; Sabillon et al., 2016; Weimann, 2016a)
As an enabler of Cybercrime	*Malware-as-a-Service* business model for criminal services	DDoS and Ransomware is available for use as a service and hosted as Tor Hidden Services (Huang et al., 2017; Nunes et al., 2016; Tsakalidis and Vergidis, 2017)
	Command-and-Control (C2) servers deployed as hidden services	Botnets are being controlled by C2 services hosted as Tor Hidden Services (Owen and Savage, 2016)
	Terrorism Operations conducted in	Recruitment, training, radicalisation, planning, fundraising for known terrorist organisations, e.g. ISIL

[12] https://www.rt.com/news/387317-pedophile-ring-arrested-playpen
[13] https://github.com/prof7bit/TorChat
[14] https://telegram.org
[15] https://signal.org

	conjunction with other roles	(Broadhurst, 2017b; Brynielsson et al., 2013; Denic, 2017; Scanlon and Gerber, 2014; Tsakalidis and Vergidis, 2017; Weimann, 2016a, 2016b)
As a source of Threat Intelligence	*Scanning Forums & Marketplaces* for threat intel	Generating leads on the type of attacks that may be imminent based on exploits being sold and discussed (Nunes et al., 2016; Robertson et al., 2017; Samtani et al., 2017; Skopik, 2017)
As an enabler of anonymous Financial Transactions	Using *Bitcoin over Tor* for anonymity	Added layer of anonymity and precaution (Biryukov and Pustogarov, 2015; DiPiero, 2017)
	Money Laundering of cryptocurrencies via tumbling services	Specific services to launder money, e.g. via bitcoin conversion (Dalins et al., 2017; Denic, 2017; DiPiero, 2017; Kellermann, 2017; Moore and Rid, 2016; Sabillon et al., 2016)
As a Proxy to the Surface Web	*Avoid censorship* by circumventing blocks	Civilians engaging in ethical behaviour while protecting privacy, e.g. bypassing China's firewall (Chertoff and Simon, 2015; Denic, 2017)
	Protection from persecution by local authorities due to browsing anonymity	Journalists writing about sensitive topics pertaining to a country which is known for an oppressive regime (Chertoff and Simon, 2015; Denic, 2017; Moore and Rid, 2016; Owen and Savage, 2016)

Relationships between various actors participating on the Tor dark web are shown below in *Figure* 5 (Denic, 2017).

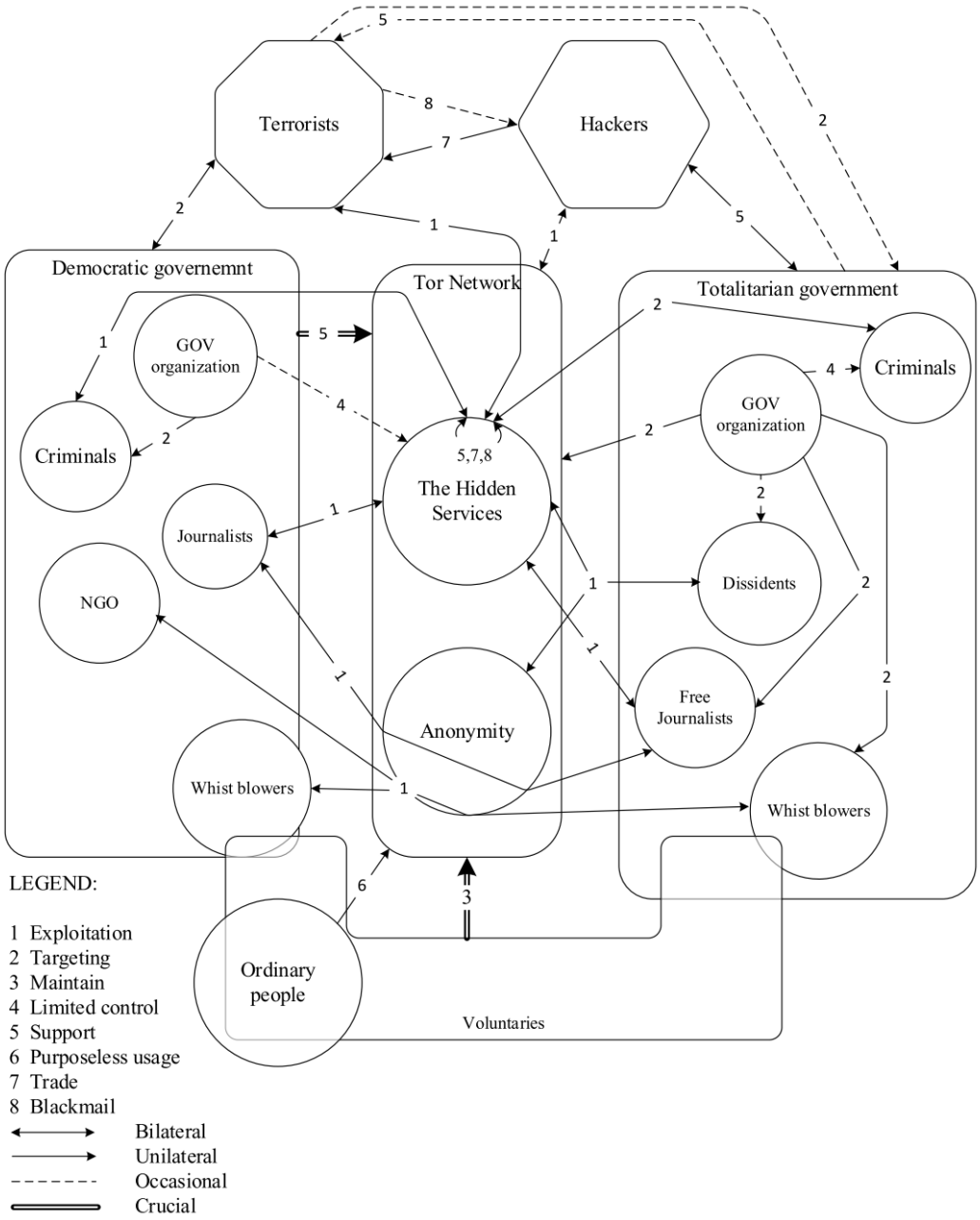

Figure 5: Relationship, Actors, Functions and Tensions (RAFT) diagram of Tor

3.6 Concerns about Accountability & Visibility

There is a significant amount of research being conducted into finding vulnerabilities in the Tor protocol and network. There is value primarily for law enforcement in being able to deanonymize users of Tor, or at least disrupt communications making the system unusable (Vogt, 2017). The US government has, at the least, created a search engine - *Memex*[16] - which indexes websites on the darknet with one of its objectives as uncovering all kinds of illegal activities (Cuthbertson, 2015).

[16] https://memex.jpl.nasa.gov

Multiple trade markets have been shut down by LE over the years, including the biggest-ever - *Silk Road* - in 2013 that brought the dark web to public attention, and *AlphaBay* and *Hansa* in 2017 (Tzanetakis, 2018). Such darknet marketplaces continue to be taken offline as law enforcement tries its best to crack down on servers hosting these services. While the network itself is decentralised and even distributed to an extent, the content is still served on a traditional client-server model. This means the server is an operational bottleneck and thus a central point of failure. This is used by law enforcement to prosecute owners of these servers and website content. LE continues to collaborate on a global scale to bring these marketplaces down but it does not take long for these marketplaces to return to a functional form; a new version of Silk Road – currently in its third iteration - continues to exist despite takedowns (Maddox et al., 2016). Furthermore, fully distributed marketplaces – one without a need for servers to host the platform – are becoming mature in recent years, e.g. OpenBazaar which has no central server but instead relies on files distributed across the network of users being downloaded when the service is requested. Combined with a distributed currency system like Bitcoin and the Tor protocol such market systems can afford near anonymity to its users and their engagements (Deep Dot Web, 2017).

To achieve deanonymisation, there are passive methods that work by passively fingerprinting the circuits set up in Tor connections (Kwon et al., 2015), analysing traffic within middle relays (Jansen et al., 2017) or by correlating traffic between the entry and exit nodes (Overlier and Syverson, 2006). If the adversaries operate at the nation-state level and are able to influence entire autonomous systems (AS) (Sun et al., 2015) or even a higher authority like an Internet Exchange Point (IXP) they may be able to deanonymize nearly 100% of Tor traffic within months of engagement (Johnson et al., 2013). Users may also be deanonymized by having their identities linked across multiple hidden services by analysing their writing style – also known as *stylometry* (Ho and Ng, 2016).

Denial of Service is also explored as a method of discouraging use or supplementing deanonymization efforts above by forcing users to connect to relays under the attacker's control (Jansen et al., 2014).

Deanonymization is not aimed only at clients or 'users' of the system to determine who is accessing a hidden service. It is also applied to the publishers of hidden services themselves as shutting down a hidden service would be more effective in curtailing questionable behaviour rather than attempting to prohibit individuals from participating. For this purpose, research exists on how to measure the popularity of hidden services, effect a denial of service towards them or even reveal their IP address given enough time (Biryukov et al., 2013).

The attempts at revealing hidden services are not limited to traffic analysis: the amount of throughput through an exit node affects its CPU usage, thus affecting its heat output which in turn affects the

clock skew rate. The latter can be measured via timestamps and may aid in linking pseudonyms of hidden services to their real identities (Murdoch, 2006).

Despite LE being persistent, developers and maintainers of Tor are continually upgrading the protocol and software to fix vulnerabilities and introduce new functionality to make the system even safer to use (Greenberg, 2017; Winter, 2017). Alternatively, other similar networks also have the potential to come to the rescue and become widely adopted, e.g. the P2P technology behind Freenet is known to be more secure than Tor (Duddu and Samanta, 2018). It remains to be seen whether alternatives to Tor, like Freenet, will ever reach critical mass for wide-scale adoption.

3.7 Growth of the Tor Dark Web

Regardless of LE's attempts to control and curb the growth of Tor, it remains the biggest anonymising network and has had at least 2 million active users connecting directly to the service, with bursts of up to 4 million (*Figure* 6 below, (The Tor Project, 2018a)) over the last year.

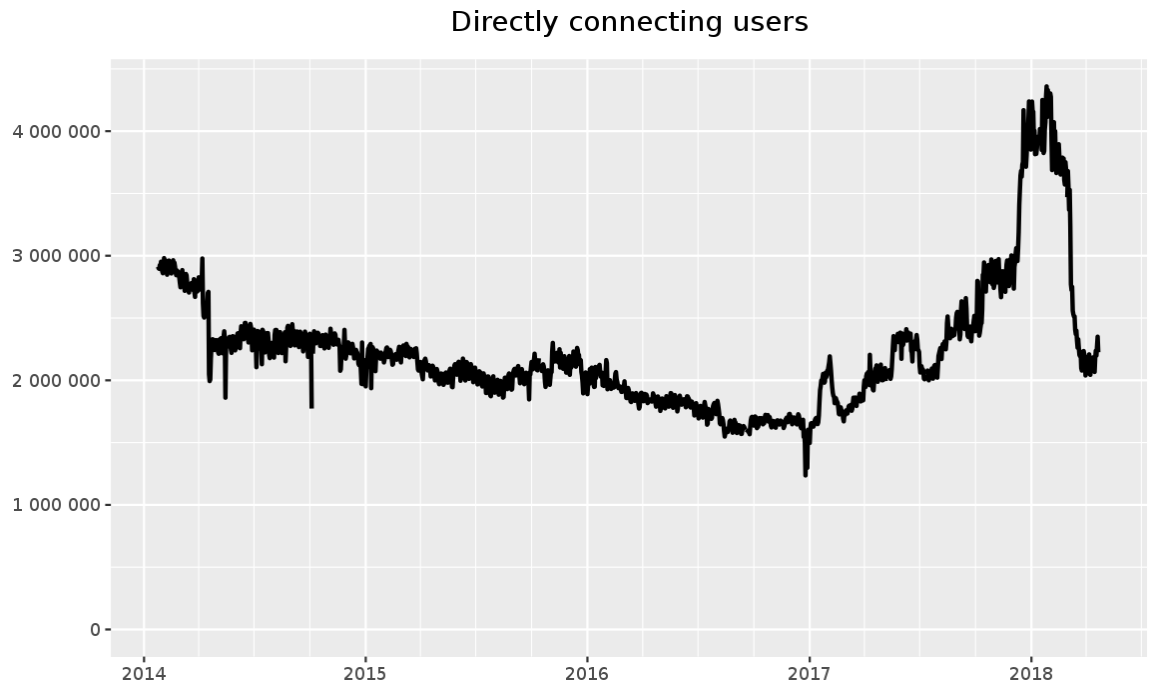

Figure 6: Number of users directly connected to Tor (last four years)

The network has also been steadily increasing in its bandwidth capacity where it increased six-fold from nearly 50 Gbit/s in 2014 to over 300 Gbit/s in 2018 (*Figure* 7 below, (The Tor Project, 2018a)). The usage lags at less than half the capacity.

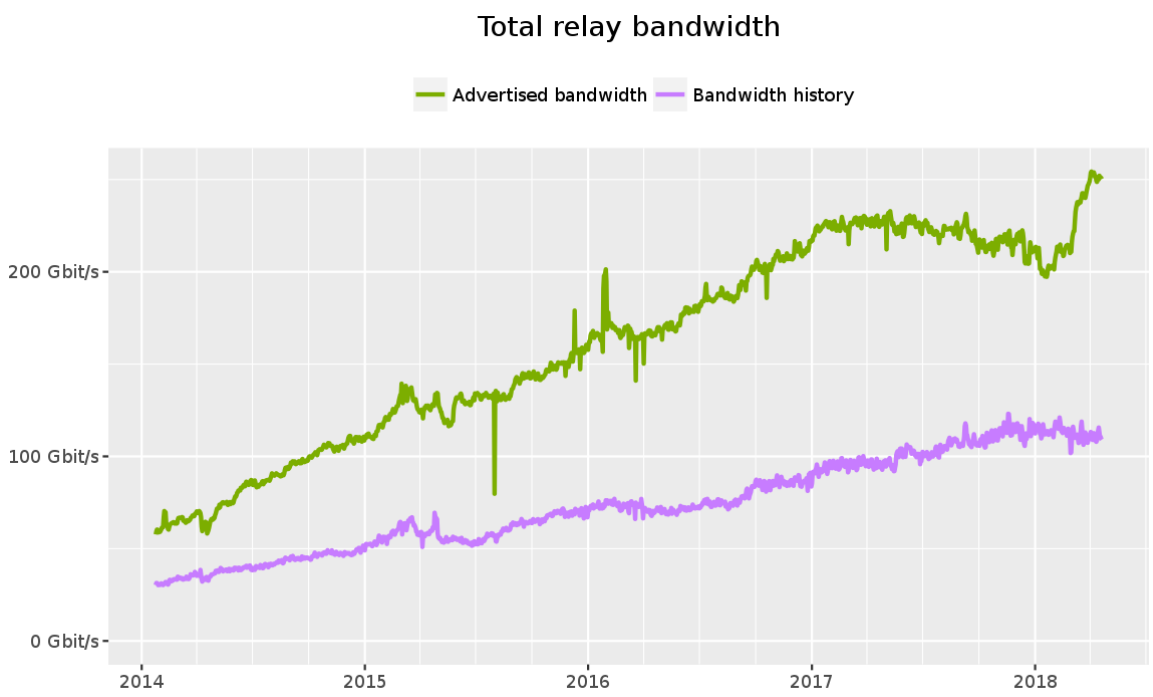

Figure 7: Total bandwidth available and in use within Tor (last four years)

The number of unique '.onion' addresses, i.e. addresses of Tor Hidden Services which can only be visited by users of the Tor network, have nearly tripled in the last four years from less than 30 000 in 2014 to 80 000 in 2018. Of these 80 000 hidden services, around 45 000 are available at any given point in time (The Tor Project, 2018a). Looking at the growing number of Tor dark web users, participating nodes in the infrastructure, unique hidden services, and search popularity of "dark web", it is observed that this ecosystem is expanding over time and the phenomenon can thus be said to be increasing in its reach.

Some have even proposed the development of Tor to discontinue (Guitton, 2013) because as per 'deindividuation theory' anonymous users are bound to engage in unethical behaviour – evident in the analysis of dark web's uses.

4. Model for Future Research / Gaps Identified

Having looked at the literature on the topic of dark web/darknets/tor hidden services, the following research gaps have been identified and proposed.

4.1 Enabling Cybercrime: Criminals' Dependence on the Dark Web

Cybercriminals have benefitted from hidden services by way of being able to buy exploits – including zero-day – from marketplaces, engage with other criminals on forums, host command-and-control (C2) servers for botnets & exfiltration malware, and hire professional criminals or their skills 'as-a-service' (Chertoff and Simon, 2015; Sabillon et al., 2016; Vogt, 2017). The anonymity attribute the dark web confers to its users makes these activities possible and enables cybercriminals to conduct their affairs.

There are various types of cybercrimes and actors present, from the amateur 'script-kiddies' using readily-available tools and exploits to target highly vulnerable systems aka the "low-hanging fruit", to the highly focused and skilled Advanced Persistent Threats (APT) known to be behind significant cases of espionage against large organisations and nation states. The APT phenomenon is known to use zero-day exploits as one of the ways of gaining privileged access to target systems (Ask et al., 2013; Tankard, 2011). The creative tactics of APTs poses a significant challenge to even the most mature incident response teams (Ahmad et al., 2015, 2012). However, there was no significant literature found explicitly exploring a link between the dark web and APT phenomena, and if investigated it can potentially be exploited in curbing or better defending against cyber-attacks from APTs in the future.

Research questions:

4.1.1 *Given one of the enabling features of the APT phenomenon is their use of zero-day exploits, and that dark web marketplaces allow trading of said exploits, how significant a role does the dark web phenomenon play in condoning the APT phenomenon?*

4.1.2 *To what extent is the dark web crucial to the success of APT attacks?*

4.2 Distributed Hidden Services (non-Client-Server model) & Dark Web Scalability

Hidden services on the dark web, e.g. *'.onion'* sites part of, and accessible through, the Tor network make use of the anonymity feature of Tor to keep their location and address private but yet are reachable by interested parties. This strength of theirs makes it challenging for law enforcement to shut them down as their hosting provider and geographical location is hidden. However, as seen in recent cases of darknet marketplaces like Silk Road, Hansa and AlphaBay being shut down they are not impervious to regulation (Bhaskar et al., 2017; Broadhurst, 2017a; Huang et al., 2017; Tzanetakis, 2018). As a result, marketplace operators, and interested traders, are exploring ways of removing the bottleneck associated with having a centralised marketplace web platform. In these situations when

anonymity is not enough, a more distributed implementation is potentially the answer and can be seen in its early stages in the form of multiple new decentralised markets either built on Tor (Deep Dot Web, 2017; Fraser, 2015) or the blockchain technology (Silkos, 2017). There is scope to utilise the significantly distributed nature of the internet to continue expanding upon the phenomenon. Dark web markets which work on a more distributed model as opposed to a client-server one would become even more resistant to being shut down – OpenBazaar being a recent example.

Research can also be conducted into the scalability of the dark web over time: whether the current internet infrastructure continues to support this phenomenon or become a limiting factor in its usage. Moreover, given that some methods for deanonymization of clients or services rely on controlling sufficient nodes on the Tor network (Biryukov et al., 2013; Jansen et al., 2014; Johnson et al., 2013; Kwon et al., 2015), further investigation can be conducted into what level of growth, or user adoption, of Tor is required before these methods become economically infeasible to exploit. This research could help law enforcement reprioritise its approaches for monitoring the dark web.

Research questions:

4.2.1 What trends can be observed about existing web infrastructure – especially hidden services – moving in the direction of being more decentralised?

4.2.2 What technological, and other, factors currently affect this transition and how will this affect the scalability and observability of the dark web?

4.3 Role & Capability of Law Enforcement

As the medium of communication between people becomes more and more decentralised and thus harder to regulate, it is possible that unethical (and illegal) content will proliferate in a direction that will keep it away from the watchful eye of the law.

Part of current law enforcement operations' focus is on deanonymization of hidden services, of marketplace operators, of site administrators and anyone else involved in the facilitation of a relatively centralised (but anonymous) infrastructure used to conduct illegal activity on the dark web. As technology advances, these elements may become increasingly difficult to track, identify and shut down especially as they cease to exist in their current form (Deep Dot Web, 2017; Moore and Rid, 2016).

Research questions:

4.3.1 What strategies can the law enforcement use to exercise control over the dark web? Are there merits to focus on targeting users, servers or the protocol, e.g. Tor itself?

4.3.2 How can we, as a society, reduce unethical behaviour, e.g. child sexual abuse, in the presence of a market demand that seems to be forever present combined with markets that are difficult to shut down?

Furthermore, the question of what *can* be done is separate from what *should* be done about the technology from a regulatory perspective. The two ideas seem mutually exclusive in their pure forms as promoting the full extent of civil liberties by way of allowing unrestricted and unmonitored access to internet technologies mean illicit activities will likely flourish (Chertoff, 2017). However, civil liberties may suffer when policies restricting the use of the surface, or dark, web are brought into existence.

Research question:

4.3.3 *Where on the spectrum of allowing civil liberties vs clamping down on unethical behaviour should the law position itself at?*

It is argued that our efforts need to be refocused on initiatives elsewhere in the process, e.g. prosecuting the traders as opposed to facilitators of the marketplace – as this becomes more and more difficult to do with technological advancements. DiPiero (2017) suggests increasing the number of sting operations and focusing on bringing down the source of drugs rather than the marketplace itself as the phenomenon grows over time.

4.4 Dark Web Phenomenon Growth vs Regulatory Growth

Private spaces for people to interact with each other have almost always existed, be they in one's private property, or in a dark alleyway on a quiet night. Most research on the topic of the dark web focuses on deanonymization attempts or utilising it for some form of threat intelligence. There is potential for looking at this topic as a manifestation of a much more significant phenomenon of civilians looking for private spaces to conduct their affairs. Seeing the dark web through this lens could allow for better speculation of its growth in the future and thus help stakeholders such as law enforcement make better decisions in the investment of their efforts.

We make the argument that the dark web – potentially a phenomenon – has increasingly become bigger as regulations have increased (Dolan, 2018; Goodman, 2013; Henderson, 2010; Whitehouse, 2017) and individual liberties have decreased (Shor et al., 2018). Proponents of the dark web claim (Maddox et al., 2016) that if the current political landscape was aligned with a more libertarian ideology, trade between individuals would not be subject to regulations and thus there would likely not exist a need for an underground black market, e.g. for recreational drugs. Spikes in Tor usage have

been noticed with many major political events enforcing censorship as deemed important by the government of a country (The Tor Project, 2018a).

Moreover, given that cybercriminals make extensive use of the dark web to facilitate their operations, an improved law enforcement capability on the surface web could lead to an increase in the technological investment, and thus advancement, in the dark web phenomenon. This is similar to the drug cartels in Mexico over time having become increasingly technologically creative and improved the scale and quality of their operations (Ramirez and Bunker, 2014; Smith and Nieto-Gomez, 2016). Clamping down on illegal activity has become the driver for technological innovation and growth in the direction suited for illegal activity, especially when the economic return from said activities is able to support this investment.

There is potential for research into whether the phenomenon of the dark web - and investment in technology which enables it – is increasing over time and if this increase is correlated with a reduction in personal liberties/stricter regulations. Establishing this correlation can lead to a discussion on the effects of policy concerning civil liberties on the dark web phenomenon, and a desired outcome in the latter could be affected by manipulating the former.

Research questions:

4.4.1 How does the growth of the dark web – and investment in technology supporting it - correlate with an increase in regulations surrounding personal, civic and economic liberties in a society?

4.4.2 In the case that regulations positively correlate with growth of the dark web, how can the correlating factors in this relationship allow for control of the dark web by controlling the regulatory landscape?

5 Conclusions

The internet can be classified into three different areas – surface, deep and dark – based on their identifiability and accessibility aspect. One of those areas, the dark web (aka darknets), is defined as being that part of the internet which affords anonymity to its users and hosted web services (hidden services). From a technical viewpoint, the dark web is a distributed system and an overlay network which can be accessed via the use of special software. A literature review was conducted into the roles the dark web plays in modern digital society, its enablement of cybercrime and its relationship with law enforcement. Conducting a literature review on this topic was challenging as information available and research conducted on the topic is relatively limited due to its 'secretive' and generic/non-identifying nature. Many hidden services rely on word-of-mouth popularity and certain communities are invite-only with restricted access not just due to payment but reputation in certain communities.

The first research question required investigation of the roles the dark web currently serves. It was revealed that it plays a plethora of roles, more than may seem on the surface. While online marketplaces for illicit drugs are still a major one, they remain one of many; marketplaces for trade of software exploits, forums for discussion amongst special interest groups, cybercriminal infrastructure, extremist recruitment, financial transactions and money laundering are some of the other significant uses. It is also seen to be growing its user base as evidenced by increasing bandwidth and nodes on the network, much of which is to support anonymous browsing of the surface web.

The second research question involved looking at the significance of the dark web to cybercriminal activities and operations. This was found to one of the roles the dark web plays, especially in the case of providing zero-day vulnerabilities thus enabling the APT phenomenon. There is evidence to show that it serves as a training ground for cybercriminals, e.g. APT actors, via discussion boards, hosts infrastructure used to conduct, support and commodify cybercriminal operations in the form of exploit trade, exploit-as-a-service business model, hosting command-and-control servers as Tor Hidden Services, and providing anonymity to escape legal prosecution for online activity. However, the criticality of this role remains questionable as it may be considered to only lower the barrier to entry into the world of cybercrime. More established and well-resourced actors are purported to use their own private infrastructure, e.g. botnet proxies to anonymise their actions, discovering their own zero-day vulnerabilities and using other means to finance their operations.

Finally, the third research question was about law enforcement curbing illegal activity on the dark web. It was found that law enforcement continues its attempts to close markets responsible for the sale of illicit items, especially recreational drugs. However, the infrastructure reacts to these incidents and attempts to mitigate the vulnerabilities exploited – technical and otherwise – by the authorities. In

response, the Tor protocol is continually updated to fix protocol vulnerabilities, the market operators improve their operational security, the financial backbone – cryptocurrencies – introduces newer and more anonymous variants alongside an increase in money laundering ('tumbling') services, hidden services become more distributed and without a central server that can be seized, and escrow functions are evolving to be based not just on trust but also on cryptographic improvements.

Looking at the evolution of dark web and the increasing user base of Tor, this phenomenon of people congregating together away from interference – legal and otherwise – and judgement to share content, opinions and to trade is likely going to continue developing. People are innovating to come up with even more resilient systems to ensure a 'safe space' for their actions, especially if it is deemed illegal – socially acceptable or not. In the debate on privacy versus security that developed countries are having with their citizens, the technology factor is weighing in stronger than before as it becomes not just a matter of legality but of technical capability to monitor and conduct surveillance on people. It is possible that in the future this debate would be over as technology advances to the point where privacy is not at the mercy of governments but in the hands of users and private corporations. The discussion on this topic then no longer remains in the domain of technology but is one that needs an interdisciplinary contemplation by experts in areas of psychology, sociology, law, and others.

In order to continue investigation in this area, and having conducted a review, some research gaps have been identified. These are outlined in the table below.

Ref	Topic	Questions
4.1	APT Phenomenon's Dependence on Dark Web	*4.1.1* Given one of the enabling features of the APT phenomenon is their use of zero-day exploits, and that dark web marketplaces allow trading of said exploits, how significant a role does the dark web phenomenon play in condoning the APT phenomenon? *4.1.2* To what extent is the dark web crucial to the success of APT attacks?
4.2	Distributed Hidden Services & Scalability	*4.2.1* What trends can be observed about existing web infrastructure – especially hidden services – moving in the direction of being more decentralised? *4.2.2* What technological, and other, factors currently affect this transition and how will this affect the scalability and observability of the dark web?

4.3	Role & Capability of Law Enforcement	*4.3.1* What strategies can the law enforcement use to exercise control over the dark web? Are there merits to focus on targeting users, servers or the protocol, e.g. Tor itself? *4.3.2* How can we, as a society, reduce unethical behaviour, e.g. child sexual abuse, in the presence of a market demand that seems to be forever present combined with markets that are difficult to shut down? *4.3.3* Where on the spectrum of allowing civil liberties vs clamping down on unethical behaviour should the law position itself at?
4.4	Dark Web vs Regulatory Growth	*4.4.1* How does the growth of the dark web – and investment in technology supporting it - correlate with an increase in regulations surrounding personal, civic and economic liberties in a society? *4.4.2* In the case that regulations positively correlate with growth of the dark web, how can the correlating factors in this relationship allow for control of the dark web by controlling the regulatory landscape?

6 Appendix

6.1 PAFM Elicitation

Table 2: PAFMRQ analysis of current work

Component	**Definition**	**Specific**
Real-world Problem (**P**)	*The problem setting represents people's concerns in a real-world problematic situation*	The Dark Web is a component of the Web that is notorious for illicit and anonymous activity, particularly drug trade. The nature of the dark web is surrounded by secrecy. Is the dark web a one-off occurrence in response to something in the real world or is it a manifestation of a broader phenomenon? If it is the latter, it is important to identify characteristics and predict its future if law enforcement wants to keep up.
Area of Concern (**A**)	*The area of concern represents some body of knowledge in the literature that relates to P.*	- Anonymous overlay networks ('Dark Web') and its documented uses - Information security and its affiliation with the Dark Web
Framework (**F**)	*The conceptual framing helps structure collection and analyses of data from P to answer RQ; FA draws on concepts from A, whereas FI draws on concepts independent of A.*	- dark web as a phenomenon, not just a haven for drug-buyers - dark web as an unregulated free market, an online version of the black market - dark web as a private space for individuals to engage with others
Methodology (**M**)	*The method details the approach to empirical inquiry, specifically to data collection and analysis.*	Literature review on 'Dark Web', 'Darknets' and 'Tor hidden services' via Google Scholar and EBSCOHost. A

		concept-centred approach to analysing the literature.
Research Question (**RQ**)	*The research question relates to P, opens for research into A, and helps ensure the research design is coherent and consistent.*	- What is the dark web used for? - What activities does the dark web harbour other than trade of illicit drugs? - How is the dark web dealing with the law enforcement being an adversary? - Can the Dark Web be considered a phenomenon and if so what projections can be made about its future?
Contributions (**C**)	*Contributions influence P and A, and possibly also F and M.*	Ca: identify gaps in research and propose a research agenda to improve knowledge about the nature, future and control of the dark web.

7 References

Abbasi, A., 2007. Affect intensity analysis of dark web forums, in: Intelligence and Security Informatics, 2007 IEEE. pp. 282–288.

Ablon, L., Libicki, M.C., Golay, A.A., 2014. Markets for cybercrime tools and stolen data: Hackers' bazaar. Rand Corporation.

ACPHIS, 2018. IS Journal Ranking [WWW Document]. Aust. Counc. Profr. Heads Inf. Syst. URL http://www.acphis.org.au/v2wp/rank-order/ (accessed 4.13.18).

Ahmad, A., 2010. Tactics of Attack and Defense in Physical and Digital Environments: An Asymmetric Warfare Approach. J. Inf. Warf. 9, 46–57.

Ahmad, A., Hadgkiss, J., Ruighaver, A.B., 2012. Incident Response Teams - Challenges in Supporting the Organisational Security Function. Comput. Secur. https://doi.org/10.1016/j.cose.2012.04.001

Ahmad, A., Maynard, S.B., Shanks, G., 2015. A Case Analysis of Information Systems and Security Incident Responses. Int. J. Inf. Manage. 35, 717–723. https://doi.org/10.1016/j.ijinfomgt.2015.08.001

Almukaynizi, M., Nunes, E., Dharaiya, K., Senguttuvan, M., Shakarian, J., Shakarian, P., 2017. Proactive identification of exploits in the wild through vulnerability mentions online, in: Cyber Conflict (CyCon US), 2017 International Conference On. pp. 82–88.

Anonymous, 2016. Anonymous Launches OnionIRC, Specifically for "Training the Next Generation of Hackers" [WWW Document]. ANONHQ.COM. URL http://anonhq.com/anonymous-launches-onionirc-specifically-training-next-generation-hackers/ (accessed 4.19.18).

Armin, J., Foti, P., Cremonini, M., 2015. 0-day vulnerabilities and cybercrime, in: Availability, Reliability and Security (ARES), 2015 10th International Conference On. pp. 711–718.

Ask, M., Bondarenko, P., Rekdal, J.E., Nordbø, A., Bloemerus, P., Piatkivskyi, D., 2013. Advanced persistent threat (APT) beyond the hype. Proj. Rep. IMT4582 Netw. Secur. Gjøvik Univ. Coll. Springer.

Balakrishnan, H., Kaashoek, M.F., Karger, D., Morris, R., Stoica, I., 2003. Looking up data in P2P systems. Commun. ACM 46, 43–48.

Bernstein, M.S., Monroy-Hernández, A., Harry, D., André, P., Panovich, K., Vargas, G.G., 2011. 4chan

and/b: An Analysis of Anonymity and Ephemerality in a Large Online Community., in: ICWSM. pp. 50–57.

Bhaskar, V., Linacre, R., Machin, S., 2017. Dark web: The economics of online drugs markets. LSE Bus. Rev. Blog.

Bilge, L., Dumitras, T., 2012. Before we knew it: an empirical study of zero-day attacks in the real world, in: Proceedings of the 2012 ACM Conference on Computer and Communications Security. pp. 833–844.

Biryukov, A., Pustogarov, I., 2015. Bitcoin over Tor isn't a good idea, in: Security and Privacy (SP), 2015 IEEE Symposium On. pp. 122–134.

Biryukov, A., Pustogarov, I., Thill, F., Weinmann, R.-P., 2014. Content and popularity analysis of Tor hidden services, in: Distributed Computing Systems Workshops (ICDCSW), 2014 IEEE 34th International Conference On. pp. 188–193.

Biryukov, A., Pustogarov, I., Weinmann, R.-P., 2013. Trawling for tor hidden services: Detection, measurement, deanonymization, in: Security and Privacy (SP), 2013 IEEE Symposium On. pp. 80–94.

Bradley, S., 2018. How to use a VPN on an iPhone or iPad [WWW Document]. Tech Advis. URL https://www.techadvisor.co.uk/how-to/apple/how-use-vpn-on-iphone-ipad-3674019/ (accessed 5.20.18).

Broadhurst, R., 2017a. Cybercrime: Thieves, Swindlers, Bandits and Privateers in Cyberspace. SSRN.

Broadhurst, R., 2017b. Cyber Terrorism Research Review Cyber Terrorism : Research Review Research Report of the Australian National University. https://doi.org/10.13140/RG.2.2.19282.96964

Broadhurst, R., Woodford-Smith, H., Maxim, D., Sabol, B., Orlando, S., Chapman-Schmidt, B., Alazab, M., 2017. Cyber Terrorism: Research Review: Research Report of the Australian National University Cybercrime Observatory for the Korean Institute of Criminology.

Brynielsson, J., Horndahl, A., Johansson, F., Kaati, L., Mårtenson, C., Svenson, P., 2013. Harvesting and analysis of weak signals for detecting lone wolf terrorists. Secur. Inform. 2, 11.

Bugge, A., 2017. Dark web drug market growing rapidly in Europe: report. Reuters.

Cambia Research, 2016. Surface Web, Deep Web, Dark Web -- What's the Difference? [WWW Document]. Cambia Res. URL https://www.cambiaresearch.com/articles/85/surface-web-deep-

web-dark-web----whats-the-difference (accessed 5.20.18).

Chen, H., Chung, W., Qin, J., Reid, E., Sageman, M., Weimann, G., 2008. Uncovering the dark Web: A case study of Jihad on the Web. J. Assoc. Inf. Sci. Technol. 59, 1347–1359.

Chertoff, M., 2017. A public policy perspective of the Dark Web. J. Cyber Policy 2, 26–38.

Chertoff, M., Simon, T., 2015. The Impact of the Dark Web on Internet Governance and Cyber Security, Global Commission on Internet Governance.

Christin, N., 2013. Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace, in: Proceedings of the 22nd International Conference on World Wide Web. pp. 213–224.

Chu, H., 2017. Inside Monero.

CORE, 2018. Journal Portal [WWW Document]. Comput. Res. Educ. URL http://portal.core.edu.au/jnl-ranks/ (accessed 4.13.18).

Crawley, A., 2016. Hiring hackers. Netw. Secur. 2016, 13–15.

Cuthbertson, A., 2015. Death of the Dark Web? DARPA's Memex search engine allows Tor tracking [WWW Document]. Int. Bus. Times. URL https://www.ibtimes.co.uk/death-dark-web-darpas-memex-search-engine-allows-tor-tracking-1488124 (accessed 4.3.18).

Dalins, J., Wilson, C., Carman, M., 2017. Criminal motivation on the dark web: A categorisation model for law enforcement. Digit. Investig.

Deep Dot Web, 2017. Decentralized Darknet Markets Have Arrived: OpenBazaar 2.0 beta launches with support for TOR [WWW Document]. Deep Dot Web. URL https://www.deepdotweb.com/2017/09/23/decentralized-darknet-markets-arrived-openbazaar-2-0-beta-launches-support-tor/ (accessed 4.19.18).

Denic, N. V, 2017. Government Activities to Detect, Deter and Disrupt Threats Enumerating from the Dark Web.

Dewey, C., 2014. Absolutely everything you need to know to understand 4chan, the Internet's own bogeyman [WWW Document]. Washington Post. URL https://www.washingtonpost.com/news/the-intersect/wp/2014/09/25/absolutely-everything-you-need-to-know-to-understand-4chan-the-internets-own-bogeyman/ (accessed 4.19.18).

DiPiero, C., 2017. Deciphering Cryptocurrency: Shining a Light on the Deep Dark Web. U. Ill. L. Rev.

1267.

Dolan, E., 2018. Is Overregulation Really Holding Back the U.S. Economy? [WWW Document]. Harv. Bus. Rev. URL https://hbr.org/2018/01/is-overregulation-really-holding-back-the-u-s-economy (accessed 5.20.18).

Duddu, V., Samanta, D., 2018. Network and Security Analysis of Anonymous Communication Networks. arXiv Prepr. arXiv1803.11377.

Franklin, J., Perrig, A., Paxson, V., Savage, S., 2007. An inquiry into the nature and causes of the wealth of internet miscreants., in: ACM Conference on Computer and Communications Security. pp. 375–388.

Fraser, J., 2015. 4 reasons why decentralized marketplaces are inevitable [WWW Document]. Medium. URL https://medium.com/originprotocol/4-reasons-why-decentralized-marketplaces-are-inevitable-25b842565e48 (accessed 5.20.18).

Ghappour, A., 2017. Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web. Stanford Law Rev.

Goodman, J., 2013. Regulations Are Very Expensive, But Their Economic Value Is Negative [WWW Document]. Forbes. URL https://www.forbes.com/sites/johngoodman/2013/03/29/regulations-are-very-expensive-but-their-economic-value-is-negative/#4e8948ec230d (accessed 5.20.18).

Greenberg, A., 2017. IT'S ABOUT TO GET EVEN EASIER TO HIDE ON THE DARK WEB [WWW Document]. Wired. URL https://www.wired.com/2017/01/get-even-easier-hide-dark-web/ (accessed 5.4.18).

Guitton, C., 2013. A review of the available content on Tor hidden services: The case against further development. Comput. Human Behav. 29, 2805–2815.

Henderson, D., 2010. The Decline in Civil Liberties [WWW Document]. Found. Econ. Free. URL https://fee.org/articles/the-decline-in-civil-liberties/

Ho, T.N., Ng, W.K., 2016. Application of Stylometry to DarkWeb Forum User Identification, in: International Conference on Information and Communications Security. pp. 173–183.

Hoffman, D., Rimo, P.A., 2017. It Takes Data to Protect Data.

Hotspot Shield, 2018. Tor vs VPN [WWW Document]. URL https://www.hotspotshield.com/resources/tor-vs-vpn/ (accessed 5.20.18).

Huang, K., Siegel, M., Madnick, S., 2017. Cybercrime-as-a-Service: Identifying Control Points to Disrupt.

Hughes, D., Walkerdine, J., Coulson, G., Gibson, S., 2006. Peer-to-peer: Is deviant behavior the norm on p2p file-sharing networks? IEEE Distrib. Syst. online 7.

Jansen, R., Juarez, M., Gálvez, R., Elahi, T., Diaz, C., 2017. Inside Job: Applying Traffic Analysis to Measure Tor from Within, in: Network and Distributed System Security Symposium.

Jansen, R., Tschorsch, F., Johnson, A., Scheuermann, B., 2014. The sniper attack: Anonymously deanonymizing and disabling the Tor network.

Johnson, A., Wacek, C., Jansen, R., Sherr, M., Syverson, P., 2013. Users get routed: Traffic correlation on Tor by realistic adversaries, in: Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security. pp. 337–348.

Kellermann, T., 2017. Follow the Money: Civilizing the Darkweb Economy.

Kirkpatrick, K., 2017. Financing the Dark Web. Commun. ACM 60, 21–22.

Krebs, B., 2018. Deleted Facebook Cybercrime Groups Had 300,000 Members [WWW Document]. KrebsOnSecurity. URL https://krebsonsecurity.com/2018/04/deleted-facebook-cybercrime-groups-had-300000-members/ (accessed 4.26.18).

Kwon, A., AlSabah, M., Lazar, D., Dacier, M., Devadas, S., 2015. Circuit fingerprinting attacks: Passive deanonymization of tor hidden services, in: 24th USENIX Security Symposium (USENIX Security 15).

Lexie, 2016. 9 must-see .onion sites from the depths of the dark web [WWW Document]. ExpressVPN Blog. URL https://www.expressvpn.com/blog/best-onion-sites-on-dark-web/

Lotan, G., Graeff, E., Ananny, M., Gaffney, D., Pearce, I., others, 2011. The Arab Spring| the revolutions were tweeted: Information flows during the 2011 Tunisian and Egyptian revolutions. Int. J. Commun. 5, 31.

Maddox, A., Barratt, M.J., Allen, M., Lenton, S., 2016. Constructive activism in the dark web: cryptomarkets and illicit drugs in the digital 'demimonde.' Inf. Commun. Soc. 19, 111–126. https://doi.org/10.1080/1369118X.2015.1093531

Mathiassen, L., 2017. Designing Engaged Scholarship: From Real-World Problems to Research Publications. Engag. Manag. Rev. 1, 2.

Mathiassen, L., Saarinen, T., Tuunanen, T., Rossi, M., 2007. A contigency model for requirements development. J. Assoc. Inf. Syst. 8, 569.

McCallister, E., Grance, T., Scarfone, K.A., 2010. Guide to protecting the confidentiality of personally identifiable information (PII).

Moore, D., Rid, T., 2016. Cryptopolitik and the Darknet. Survival (Lond). 58, 7–38.

Murdoch, S.J., 2006. Hot or not: Revealing hidden services by their clock skew, in: Proceedings of the 13th ACM Conference on Computer and Communications Security. pp. 27–36.

Nakamoto, S., 2008. Bitcoin: A peer-to-peer electronic cash system.

Nunes, E., Diab, A., Gunn, A., Marin, E., Mishra, V., Paliath, V., Robertson, J., Shakarian, J., Thart, A., Shakarian, P., 2016. Darknet and deepnet mining for proactive cybersecurity threat intelligence, in: Intelligence and Security Informatics (ISI), 2016 IEEE Conference On. pp. 7–12.

Nye Jr, J.S., 2017. Deterrence and dissuasion in cyberspace. Int. Secur. 41, 44–71.

Overlier, L., Syverson, P., 2006. Locating hidden servers, in: Security and Privacy, 2006 IEEE Symposium On. p. 15--pp.

Owen, G., Savage, N., 2016. Empirical analysis of Tor hidden services. IET Inf. Secur. 10, 113–118.

Phelps, A., Watt, A., 2014. I shop online--recreationally! Internet anonymity and Silk Road enabling drug use in Australia. Digit. Investig. 11, 261–272.

Ramirez, B., Bunker, R.J., 2014. Narco-Submarines: Drug Cartels' Innovative Technology. Cent. Int. Marit. Secur.

Rhumorbarbe, D., Werner, D., Gilliéron, Q., Staehli, L., Broséus, J., Rossy, Q., 2018. Characterising the online weapons trafficking on cryptomarkets. Forensic Sci. Int. 283, 16–20.

Robertson, J., Diab, A., Marin, E., Nunes, E., Paliath, V., Shakarian, J., Shakarian, P., 2017. Darkweb Cyber Threat Intelligence Mining. Cambridge University Press.

Sabillon, R., Cano, J., Cavaller, V., Serra, J., 2016. Cybercrime and cybercriminals: a comprehensive study. Int. J. Comput. networks Commun. Secur. 4, 165–176.

Samtani, S., Chinn, R., Chen, H., Nunamaker Jr, J.F., 2017. Exploring Emerging Hacker Assets and Key Hackers for Proactive Cyber Threat Intelligence. J. Manag. Inf. Syst. 34, 1023–1053.

Sapienza, A., Bessi, A., Damodaran, S., Shakarian, P., Lerman, K., Ferrara, E., 2018. Early Warnings of

Cyber Threats in Online Discussions. arXiv Prepr. arXiv1801.09781.

Scanlon, J.R., Gerber, M.S., 2014. Automatic detection of cyber-recruitment by violent extremists. Secur. Inform. 3, 5. https://doi.org/10.1186/s13388-014-0005-5

Shor, E., Baccini, L., Tsai, C.-T., Lin, T.-H., Chen, T.C., 2018. Counterterrorist Legislation and Respect for Civil Liberties: An Inevitable Collision? Stud. Confl. Terror. 41, 339–364.

Silkos, 2017. Silkos (SLK) Technical White Paper.

Skopik, F., 2017. Collaborative Cyber Threat Intelligence: Detecting and Responding to Advanced Cyber Attacks at the National Level. CRC Press.

Smith, R., Nieto-Gomez, R., 2016. How Drug Cartels Operate Like Silicon Valley Startups.

Spitters, M., Verbruggen, S., van Staalduinen, M., 2014. Towards a comprehensive insight into the thematic organization of the tor hidden services, in: Intelligence and Security Informatics Conference (JISIC), 2014 IEEE Joint. pp. 220–223.

Springer, P.J., 2017. Encyclopedia of Cyber Warfare. ABC-CLIO.

Stoddart, K., 2016. UK cyber security and critical national infrastructure protection. Int. Aff. 92, 1079–1105.

Sun, Y., Edmundson, A., Vanbever, L., Li, O., Rexford, J., Chiang, M., Mittal, P., 2015. RAPTOR: Routing Attacks on Privacy in Tor., in: USENIX Security Symposium. pp. 271–286.

Tanenbaum, A.S., Van Steen, M., 2007. Distributed systems: principles and paradigms. Prentice-Hall.

Tankard, C., 2011. Advanced Persistent Threats and How to Monitor and Deter Them. Netw. Secur. 2011, 16–19.

The Smoking Gun, 2011. Feds Raid Boy's Home Over 4chan Child Porn Post [WWW Document]. Smok. Gun. URL http://www.thesmokinggun.com/documents/internet/feds-raid-boys-home-over-4chan-child-porn-post

The Tor Project, 2018a. Tor Metrics [WWW Document]. Tor Proj. URL https://metrics.torproject.org/ (accessed 4.24.18).

The Tor Project, 2018b. Tor Project [WWW Document]. URL https://www.torproject.org/

Tsakalidis, G., Vergidis, K., 2017. A Systematic Approach Toward Description and Classification of Cybercrime Incidents. IEEE Trans. Syst. Man, Cybern. Syst.

Tzanetakis, M., 2018. Comparing cryptomarkets for drugs. A characterisation of sellers and buyers over time. Int. J. Drug Policy.

Van Buskirk, J., Roxburgh, A., Farrell, M., Burns, L., 2014. The closure of the Silk Road: What has this meant for online drug trading? Addiction 109, 517–518.

Vogt, S.D., 2017. The Digital Underworld: Combating Crime on the Dark Web in the Modern Era. St. Cl. J. Int'l L. 15, 104.

Webb, J., Ahmad, A., Maynard, S.B., Shanks, G., 2014. A situation awareness model for information security risk management. Comput. Secur. 44, 1–15.

Webster, J., Watson, R.T., 2002. Analyzing the past to prepare for the future: Writing a literature review. MIS Q. xiii--xxiii.

Weimann, G., 2016a. Going Dark: Terrorism on the Dark Web. Stud. Confl. Terror. 39, 195–206.

Weimann, G., 2016b. Terrorist migration to the dark web. Perspect. Terror. 10.

Whitehouse, 2017. How Deregulation Can Increase Economic Growth [WWW Document]. Econ. Jobs. URL https://www.whitehouse.gov/articles/deregulation-can-increase-economic-growth/ (accessed 5.20.18).

Winkler, I., Gomes, A.T., 2016. Advanced Persistent Security: A Cyberwarfare Approach to Implementing Adaptive Enterprise Protection, Detection, and Reaction Strategies. Syngress.

Winter, P., 2017. Tor upgrades to make anonymous publishing safer [WWW Document]. Conversat. URL https://theconversation.com/tor-upgrades-to-make-anonymous-publishing-safer-73641 (accessed 5.4.18).