Secur J (2019) 32:102–118
https://doi.org/10.1057/s41284-018-0150-5

ORIGINAL ARTICLE

The not so dark side of the darknet: a qualitative study

Mihnea Mirea[1] · Victoria Wang[1] · Jeyong Jung[1,2]

Published online: 7 August 2018

Abstract In recent years, the Darknet has become one of the most discussed topics in cyber security circles. Current academic studies and media reports tend to highlight how the anonymous nature of the Darknet is used to facilitate criminal activities. This paper reports on a recent research in four Darknet forums that reveals a different aspect of the Darknet. Drawing on our qualitative findings, we suggest that many users of the Darknet might not perceive it as intrinsically criminogenic, despite their acknowledgement of various kinds of criminal activity in this network. Further, our research participants emphasised on the achievement of constructive socio-political values through the use of the Darknet. This achievement is enabled by various characteristics that are rooted in the Darknet's technological structure, such as anonymity, privacy, and the use of cryptocurrencies. These characteristics provide a wide range of opportunities for good as well as for evil.

Keywords Darknet · Criminogenic · Anonymity · Privacy · Cryptocurrencies

✉ Victoria Wang
victoria.wang@port.ac.uk

Mihnea Mirea
mihneam.mirea@gmail.com

Jeyong Jung
jeyong.jung@port.ac.uk

[1] Institute of Criminal Justice Studies (ICJS), University of Portsmouth, Portsmouth, UK

[2] Korean National Police, Seoul, Korea

Introduction

The Darknet has become, in the last few years, one of the most discussed topics in cyber security circles. To some, the hidden networks in the Internet are a means to achieve freedom; while to others these networks are no more than new outlets to express their criminogenic desires. In general, the Darknet tends to be portrayed by various news media as an environment wherein criminal activities flourish naturally, even to the extent of being criminogenic. Many news media outlets highlight that the Darknet and its Tor browser are overwhelmingly used for criminal activities (Chandran 2015; Farrell 2017; McGoogan 2016; Moloney 2016; Samson 2017; Weissman 2015). Two example newspapers headlines are 'Dark Net may pose 'disruptive risk' to internet sector' (Samson 2017) and 'Dark web browser Tor is overwhelmingly used for crime, says study' (McGoogan 2016). This negative perception of the Darknet is also taken by governments and ordinary citizens at large, which may drive unnecessary moral panics and misguided policies (Murray 2014). The previous head of the UK GCHQ, for example, has likened the Dark Net to the Wild West, claiming that it needs to be controlled (Omand 2016).

In academic circles, previous criminological research appears to have heightened the perception that the Darknet drives criminality—depicting it as a safe haven for criminals to undertake a range of criminal activities, such as the anonymous trading of illegal goods (e.g. drugs) via cryptocurrencies (e.g. Bitcoin) (Buxton and Bingham 2015; UNODC 2014). The trading of illegal drugs, in fact, is the most prevalent activity on the Darknet (Dolliver 2015; Owen and Savage 2015). In January 2016 alone, the total drug revenues, excluding prescription drugs, on the Darknet crypto-drug markets were estimated to be between $12 and $21.1 million (Kruithof et al. 2016). These crypto-drug markets are of serious concern to law enforcement agencies around the world (Horton-Eddison and Di Cristofaro 2017). Other illegal transactions on these markets include the trading of weapons, credit card and other personal information, and exotic animals (BBC 2017; Chertoff and Simon 2015; Holm 2017). The growth of the Darknet markets is enabled by various technological characteristics of the network, such as anonymity, privacy, and the use of cryptocurrencies. Holm (2017), for example, claims that the anonymous nature of the Darknet amplifies threats of identity theft. Further, general risk and threats from the Darknet have not been thoroughly investigated either (e.g. Byrne and Kimball 2017). Most research projects on the Darknet were focused on criminal activities and their technical aspects (e.g. Qiang et al. 2014; Wright 2008; Zheng et al. 2013). Only a few very recent projects tried to assess the sociological and psychological dimensions of the Darknet (Everett 2015; Lacson and Jones 2016; Van Hout and Bingham 2013).

This paper reports on a small-scale research project that was carried out on the Darknet. The overall aim of the research was to identify whether the Darknet is inherently criminogenic, and thus constitutes a fundamental threat to individuals, organisations, and societies. Based on a qualitative research conducted in four Darknet forums, we were able to identify five main themes from our findings,

which together present an alternative view of the Darknet. The Darknet might not be intrinsically criminogenic—it does not naturally increase criminal activities; rather it might just be another tool that is used by some individuals to carry out illicit activities. Some key characteristics of the Darknet, including its anonymous nature, virtual markets, and cryptocurrencies have, of course, simply made it easier for these activities to be carried out.

The Darknet in a nutshell

Technological structure

Although the term Darknet was initially coined in the 1970s, to refer to networks isolated from The Advanced Research Projects Agency Network (ARPANET) (Pace 2017), only recently has the public become aware of it. Simply put, it is the only network on the Internet (a set of interconnected networks), wherein all network traffic is hidden. Thus, anyone can carry out any activity without leaving traces that could be tracked by commonplace technical tools—a place where perfect anonymity might, as a result, be possible.

The Darknet or Dark Web is a subset of the Deep Web, which is approximately 400–500 times larger than the Surface Web also known as the Internet that we usually use (Rudesill et al. 2015). Websites that reside on the Surface Web/Internet are stored on servers waiting to be retrieved. These websites are mostly HTML files with fixed content available in the same format to anyone who makes requests. Unlike the Surface Web, connections in the Deep Web are only made between trusted peers that are required to be part of the hidden network. Thus, websites are dynamic and mostly in a continuous change of servers, meaning that one link might lead to something at a particular time, and at another time it might lead to something else or nothing (Moore and Rid 2016). The hidden websites that reside on these private networks can only be accessed by specific software, configurations, or authorizations, such as Freenet, I2P, and Tor (Byrne and Kimball 2017). For example, Tor is a very popular browser, with an estimated over 4,000,000 users in January 2018 (The Tor Project n.d.). Thousands of volunteers around the world run relays and nodes that enable the running of anonymous network traffic. If anyone gains access to a node, then the person can see the traffic that runs through it but cannot see where it comes from and where it goes to next. The anonymous nature of the Darknet and its virtual market is protected using cryptocurrencies, e.g. Bitcoin (Buxton and Bingham 2015; Hardy and Norgaard 2016).

Social activities on the Darknet

The Darknet is used for a wide range of social activities (Moore and Rid 2016). These range from being clearly morally acceptable, across to being considered as illicit by some people, or to being clearly criminal based on national and/or international legislative frameworks. These activities could be grouped into three main

categories: (i) activism, journalism, and whistle-blowing; (ii) criminal activities in virtual markets; and (iii) cyber security threats including botnets, malware, and ransomware.

First, online anonymity provided by the Darknet is used for social and political purposes (Moore and Rid 2016). Individuals can openly share their social and political beliefs; and their disagreements with, or expectations of, their governments without fear of retribution. This sharing is especially necessary in countries with strong state censorship and surveillance against political activists, freedom fighters, and journalists (Jardine 2015). Journalists, activists, and whistle-blowers in these countries could use the Darknet to communicate with the outside world, encourage social change, and political reform, without disclosing their identities (Chertoff and Simon 2015). Nearly all types of organisations intend to keep their electronic information exchanges in safe places (Wall 2013). This is also the case with journalists, activists, and whistle-blowers. In fact, the use of Tor is recommended by 'Reports Without Borders' as one of its 'survival kits' for journalists and activists working in repressive countries (Murray 2014). During the Egyptian riots, for example, journalists and activists from around the world bypassed government censorship through Tor. They thus successfully informed the world about what was happening in Egypt (Stacey 2017). Whistle-blowing is the act of leaking governments' or companies' private information to the public. Some argue that the public have the right to be informed about the activities of both their governments and large companies (Greenwald et al. 2013). Regardless of that in some countries, leaking private information from governmental files is considered to be treasonable, e.g. the UK. Moreover, leaking information from companies is illegal in some countries, e.g. the US Edward Snowden, the most infamous whistle-blower, has leaked sensitive information from the United States government, most of this information involved the NSA and the US army (Brown 2014; Macaskill and Dance 2013) and was charged under the 1917 Espionage Act (Finn and Horwitz 2013). He has allegedly used the Tor network to send secret information about the surveillance program PRISM to a number of journalists (Paganini 2013).

Second, a large number of virtual markets on the Darknet specialise in the trading of illegal drugs (Duxbury and Haynie 2017). Stolen identities, credit card information, weapons, and contract killing are also popular 'goods and services' on this network (Chertoff and Simon 2015; Holm 2017). One of the most famous Darknet markets—the Silk Road—was said to promote decentralisation of governments and socio-political movements against law enforcement agencies (Greenberg 2013; Robinson 2012). Since 2011 when the Silk Road dominated the Darknet's marketplace, its anonymous ecosystem has evolved significantly (Soska and Christin 2015). The business model is similar with the online market place eBay. Users could leave, for example, feedback on products, and a system called 'escrow' was set up to protect the sellers and the buyers, and to resolve any possible disputes (Afilipoaie and Shortis 2015). Due to its high profile, law enforcement agencies soon started to take down the Silk Road (Rushe 2014). After the original Silk Road was shut down in October 2013, the 2nd version—Silk Road 2.0—came online under different managements. Later, a 3rd version—Silk Road Reloaded—was created after the closure of Silk Road 2.0 (BBC 2015; Olson 2013). Soon, other markets including 'Black

Market Reloaded' and 'Sheep Marketplace'—with websites, forums, or even discovery services—emerged to take Silk Road's place (Van Buskirk et al. 2014). A couple of years ago, Soska and Christin (2015) estimated that the entire Darknet marketplace ecosystem generated between $150 and $180 million in revenue annually. The rise of the Darknet markets demonstrates the degree of resilience of these anonymous online ecosystems. It also questions whether law enforcement agencies can effectively regulate these markets.

Third, the Darknet is a hot bed for cyber security threats and risks. Hacking tools that could directly or indirectly be used to attack companies or other individuals are traded on some Darknet markets (Van Buskirk et al. 2016). Malware authors have been using the Darknet to communicate and exchange ideas. The Mevade Botnet saw an increase to 5 million daily users after incorporating a Tor anonymity network. The ChewBacca malware uses the Tor infrastructure to obtain its victims' IP addresses and record their keyboard strokes; while the i2Ninja malware is known to maintain secure communications between the infected devices, and command and control server through the I2P hidden network (Maor 2013, 2015; Novitski 2014; Preuss 2013). Ransomware instals viruses on infected computers, scramble and encrypt all data these can access, and then demand payments in the form of Bitcoin to release the data. The Tor network has become indispensable to the prevalence of ransomware applications (Wyke and Ajjan 2015). Certainly, the Darknet, along with the invention of Bitcoins has provided profitable businesses for criminals (Edwards 2016).

Methods

Given that there are continuous debates over what the key characteristics of cybercrime and cyber criminals are (e.g. Williams and Levi 2015), a study on the Darknet ought to be challenging, and thus ought to merit recognition. Previous research on the Darknet has tended to be technical in nature. Researchers primarily used technical skills, such as traffic analysis (Biryukov et al. 2014) and web-crawling (Dolliver and Kenney 2016; Moore and Rid 2016; Soska and Christin 2015) to understand the hidden websites. In the largest study related to Tor hidden services, at the time of the research, for example, Owen and Savage (2016) collected approximately 80,000 hidden services, using 40 onion relays over a period of 6 months. These approaches were used to identify the nature and characteristics of the websites and their users' activities on the Darknet. They could not, however, provide any understandings of perceptions and thoughts of users of the Darknet. As our study intended to examine the sociological dimensions of the Darknet, we took a different approach.

Here, we explore the two overarching research questions below:

- Is the Darknet a natural environment within which criminal activity can flourish?
- If so, could the Darknet be described, in fact, as criminogenic?

Our research provides some insights into whether individuals predominantly use the Darknet to take advantage of its technological features to conduct a range of criminal

activities. It aims to identify whether the Darknet is inherently criminogenic, and thus constitutes a fundamental threat to individuals, organisations, and societies. A qualitative approach provided the basis for our empirical research. By way of qualitative interviews carried out in the style of an online survey, the empirical work took the participants through a series of 10 questions on four different Darknet forums. We would, of course, have preferred standard semi-structured face-to-face interviews. However, the option was ruled out since we needed to respect various ethical considerations raised by our ethics committee, and the anonymous culture of the Darknet. Thus, we formulated 10 interview questions and transposed these into an online survey using the Bristol Online Survey (BOS) tool (https://www.onlinesurveys.ac.uk).

The link to the survey was imbedded in an invitation letter, which was posted in four forums that reside on the Darknet—The Hub (thehub7gqe43miyc.onion); Intel Exchange (rrcc5uuudhh4oz3c.onion); Darknet Central (2u7kil26qazmrmb6.onion); and DarknetM Avengers (avengerfxkkmt2a6.onion). These forums were selected because these were platforms for general everyday discussions and were not dedicated to specific purposes. Subjected to an anonymous registration process, these forums are free for anyone to use, and provide a sample that closely reflects Darknet users coming from diverse backgrounds, and also, having disparate reasons behind their use of the Darknet. Forum users who wished to participate in this research could simply click on the live link and answer these 10 questions via the BOS tool. They could withdraw at any time and had the option to not submit their answers.

Although the Darknet is a vast place, with more and more experimental search engines created daily, the forums that were used to conduct this research were not easy to locate. First, there is no unique public database that stores all the Darknet websites. The process to search for suitable forums can be a dangerous task, as some databases (both on the Surface and Deep Web) that contain Darknet websites are known to publish links that lead to malicious websites. Secondly, for various ethical reasons, not all forums on the Darknet could be used to conduct this research. Each forum on the Darknet has its internal regulations, e.g. prohibiting any research activities. Furthermore, some forums required rigorous vetting processes prior to participating in any activities, e.g. posting. Overcoming these difficulties, we managed to identify four suitable forums that allowed for our research to take place.

Convenience sampling is our chosen sampling method for two main reason. Those are i) to accommodate to the anonymous culture and the constantly changing membership of the Darknet; and ii) to obtain a sensible approximation of ordinary users' views on the Darknet. Furthermore, to respect the culture of the Darknet, we guaranteed total anonymity and did not ask for any personal information. To avoid being accused of spamming, we only posted the invitation note in these four forums once. We analysed 17 completed responses, to the 10 questions, from 17 users of these four forums. These responses provided valuable information on the nature of the Darknet, and some possible security threats it could generate. The data collected were analysed using thematic analysis, which is useful when investigating uncovered areas or under-researched subjects (Braun and Clarke 2006). This approach was appropriate because the Darknet was a recent phenomenon, and therefore its users were not very well understood. We wished to achieve an understanding of subjective experience by gaining insights into

individuals' motivations and actions. Of course, these individuals' views were determined by a range of factors, such as the forums, in which they resided. These forums were platforms for general everyday discussions. Thus, individuals participated in the forums would be those who were more willing to engage with the general social purposes of the Darknet. They might also be individuals who had long been concerned with the predominant image of the Darknet being a natural ground of crime, and thus, had long been eager to express their views. Therefore, our research is only designed to offer an alternative view of the Darknet.

Main findings and discussions

Findings from our empirical research are presented and analysed under five main themes that were identified during the thematic analysis.

Darknet is not underground

First, the participants were asked where they heard about the Darknet. When people talk about the Darknet, they often portray the dark side of the Internet (Farrell 2017; McGoogan 2016; Samson 2017). The Darknet can be considered as having an 'underground' element, and thus it is natural to assume that those who use it have discovered it in other underground environments. However, some of our participants clearly stated that they found out about the Darknet from conventional open sources, including schools, news media, and other Surface Web discussion forums. Today, a simple Google search offers numerous websites with tutorials on how to get on the Darknet (Egan 2016; Kumar 2014). Over three quarter of our participants (13 out of 17) claimed that they use the Darknet every day while the remaining participants (4 out of 17) mentioned that they visit the Darknet occasionally. The participants do not consider the Darknet as an underground phenomenon. For some examples, see the two extracts below:

> R10: 'When I was a teenager, our information teacher told us about a strange thing called "Darknet" and at the same time, he talked about some actual whistle blowers who used the Darknet for their activities, I found it interesting, so I decided to look it up on google Every day'.
>
> R11: 'I learned about the darknet through reading an article on Gizmodo about it. It was a pretty neutral article explaining indexing, the tor browser etc. I use it a few times a week'.
>
> Extracts from responses on online forums, May 2016

Darknet's anonymity provided freedom of expression

Next, we asked our participants why they participated in the Darknet and what the most interesting/appealing feature of this environment was. A simple online

search on the key words of 'Darknet' and 'Dark Web' would display results that put the Darknet in a negative light by repeatedly associating words including, 'illicit', 'shady', 'disruptive', 'creepiest', or 'infamous' with it (e.g. Farrell 2017; Fox-Brewster 2017; Samson 2017; Weissman 2015). Some search engines, for example Google, were accused of manipulating search results to fit dominant political agendas (Chmielewski and Bergen 2016). Google has, however, openly denied the accusations, and claimed that if many searched for negative things about one subject then the search index would automatically favour those results (Leswing 2016).

According to labelling theories, individuals might be influenced by terms that are used to describe them. Thus by stereotyping and defining someone to be something, the person might start to behave according to the label put on him or her (Lee et al. 2014; Meier 1976). Our findings show that most of our participants were aware of the deviant label attached to Darknet users. However, they do not appear to behave according to their labels—over two-thirds of the participants (12 out of 17) have explicitly stated that 'anonymity' and 'freedom' are the two main reasons behind their initial and continued use of the Darknet. For some examples, see the three extracts below:

> R1: 'I have a strong interest in online privacy and anonymity. I am extremely concerned by the shift in global politics that seeks to demonise any dissent or alternative views to those held by the ruling elites who own self-serving interests are not those of the people they purport to represent. I find the Darknet community fascinating and enjoyable to engage with. I feel it is a human right to be able to have an exchange of views without fear of reprisals or being labelled as a subversive'.
>
> R4: 'The most appealing feature is the ability to speak freely, without repercussions; one can express unpopular opinions, without attracting undue attention to oneself. In some quarters, e.g. Saudi Arabia, even a hint as to a lack of faith can lead to charges of apostasy, with deadly consequences'.
>
> R12: 'I do think that anonymity attracts criminals and that the Darknet enforces that. However, there are many more honest people on the Darknet without criminal intentions. Anonymity is a universal human right'.
>
> Extracts from responses on online forums, May 2016

Some of the participants mentioned that they initially used the Darknet for drug-related activities, but subsequently their activities have shifted to those of a more conventional, even positive nature. For two examples:

> R6: 'Originally as a mechanism to buy high quality, low cost weed and other drugs but over time the priority has changed, now more engaged in harm reduction and OPSEC awareness'.
>
> R3: 'Originally to buy drugs but now to participate in forums/the community'.
>
> Extracts from responses on online forums, May 2016

Darknet is not a society on its own

For some, the Darknet is gradually becoming a society of its own based on diverse ideologies, such as freedom, anonymity, and lack of regulations and central authorities (Bartlett 2014; Simons 2014; Viney 2016). As a result, it might threaten social norms and conventions of our off-line societies. The consensus from our participants is that the Darknet is not a society on its own. Moreover, even if it becomes one, it would not threaten fundamental values of our off-line societies, partly because it lacks a solid infrastructure.

Most of our participants (14 out of 17) indicated that communities on the Darknet are detached from various real-world societies. Some of our participants (7 out of 17) explained that this detachment is because the Darknet communities are mainly sustained by technological structures not human bonds. For two examples:

> R1: 'I think the Darknet community has actually disbanded to a greater extent. Back in the days of the Silk Road forums there was a huge and lively community who congregated to discuss a large range of issues. I also think this is one of the reasons the US went after it so hard. Communities like the Hub are but a mere shadow of the former community. But as you have seen there are those of us who come here for shared values but there are too few of us to pose any real threat to the standard societal model'.
>
> R3: 'There are many communities of good people on there, but I don't think they hold the power to make large scale changes in everyday society. The Internet is not real life'.
>
> Extracts from responses on online forums, May 2016

However, the participant below prefers the Darknet to real world societies, and thinks it has some forms of rules of its own:

> R12: ''The 'standard societal model' is not the real thing. People are desperately trying to fit in but often get frustrated because they don't. The Darknet-society is liberating in that sense. The interesting thing is that the Darknet regulates itself, it is not out of control, there are rules as well, just different rules. I like the Darknet better than the society authorities created. I love the diversity'.
>
> An extract from responses on online forums, May 2016

Supporting the participant above, another participant claimed that the Darknet generates constructive socio-political values, which in turn influence off-line societies. His/her argument is clearly based on the assumption that off-line societies in some countries are dominated by certain privileged classes/individuals. For him/her, the Darknet could decentralise authoritarian powers and provide venues for democratic participation:

> R16: 'Somebody has to make sure the government does not abuse its power but in reality we have some institutions that are controlling everybody but they

> are not being controlled by any other instance itself. Someone has to control the people who have control over other people.'
>
> An extract from responses on online forums, May 2016

The Darknet marketplace Silk Road

Silk Road was one of the biggest black markets on the Darknet. As a result, it received a lot of media attention, especially attention concerning the trading of illegal drugs on the Silk Road. More than half of our participants (11 out of 17) argued that the mainstream media was prejudiced against the virtual markets on the Darknet, deliberately altering the information to suit the real-world agenda of 'war on drugs'. This coincides with Helms et al.'s (2012) view that media publicity generally generates fear of cyber-attacks. The participants further claimed that the media did not depict these markets in a balanced point of view. In fact, their way of portrayal was designed to infuse the public with fear. Two of our participants wrote:

> R1: 'The mainstream news media is nothing but a propaganda machine. It always misrepresents the facts in either sensationalist or deliberately misrepresentative ways to suit an agenda. I am therefore totally unsurprised that the media misrepresented what Silk Road was about or stood for…'
>
> R11: 'Well, it is understandable when the most famous page form the Darknet is a black market, selling drugs, weapons and other illegal things. And that the media will latch on to this is expected. It's classic fear mongering. But in the ends, it's like blaming a platform for what some users are doing, it's like saying Facebook is for bullying, because some selected people use it for bullying'.
>
> Extracts from responses on online forums, May 2016

Some argued that by creating an online market with user feedback, Silk Road managed, in a way, to promote 'safer' drugs; and to also reduce the level of drugs on the streets and drug-related street violence (Afilipoaie and Shortis 2015; Buxton and Bingham 2015). Three of our participants asserted that Silk Road in fact offered safer drugs and less street-related violence. These positive aspects were provided by promoting quality through the feedback system and by moving the exchange of drugs online. Two of them wrote:

> R1: 'Silk Road for the first time introduced accountability into the drug trade for the end user. No longer could drug dealers get away with simply selling dangerous and adulterated products, if they tried they were outed quickly and driven from the market. Purchasing online also reduces the risk of harm by eliminating the need to associate with people who have traditionally been associated with using violence. The combination of these factors of course promotes 'safer' purchasing of drugs and only someone invested in making their money or deriving power and influence from enforcing the war on drugs could disagree with those facts'.

R4: 'There have been numerous reports to that effect. If people don't have to do business with dealers on the street, the prospect for violence is eliminated.

Extracts from responses on online forums, May 2016

The Darknet does not intrinsically breed criminal activities

Some media outlets, academic papers, and law enforcement agencies appear to depict the primary purpose of the Darknet as being a place for criminals to conduct their businesses (Décary-Hétu and Giommoni 2017; Fox-Brewster 2017; Horsman 2017; Jeffray and Feakin 2015; McGoogan 2016; Moloney 2016; Weimann 2016). The Darknet has indeed offered new opportunities for criminal activities to flourish. However, it is not fundamentally different from any other means of technologies and tools. For example, when the social platform—Twitter—was designed, the creators had no intention to promote terrorist activities, however, there are now known terrorist cells that seek to recruit people through Twitter (Yadron 2016). The Tor browser, the most popular browser used to access the Darknet, was created as a collaborative project between the US Naval Research Laboratory and the non-profit organisation Free Haven Project (Moore and Rid 2016).

Considering the negative image of the Darknet, the security industry, however, ought to be concerned and ought to investigate whether the Darknet can be used to harm the assets that they are protecting. The companies of Ashley Madison and Sony have been previously hacked, and the stolen private data were stored on the Darknet (Boorstin 2015; Lamont 2016). Although the hacking groups involved in these two hacks never mentioned whether the existence of Darknet had facilitated their activities, governments consider the Darknet as a threat to their security, and thus fear both the network and its users (Buxton and Bingham 2015; Décary-Hétu and Giommoni 2017; Jeffray and Feakin 2015). There have not been, however, a concrete study evidencing that the Darknet increases levels of criminality, and without the Darknet, governments and companies are less likely to be attacked. Consequently, the Darknet is considered by most of our research participants (13 out of 17) as just another tool that can be used by criminals. For example, four of our participants wrote:

R4: '…any tool or technology that could be turned to evil purpose. Steak knives can be used to cut your steak or murder your wife. Car can be used to kidnap children. It would be insane to think that anonymity and privacy tools are going to be any different. There are always going to be people who are going to commit crimes, and they are going to use *any* tools at their disposal…'.

R1: 'It may have given new opportunities to some, but you could use that argument for any innovation. Criminals often are the earliest adopters of new technology, you don't hear people blaming Google for child porn, do you? In any society there will be those who exploit certain technology, should we therefore ban all future technological advancement in case it gets misused? Of course not, that would be ridiculous just like blaming the small number of people of

use the Darknet for nefarious reasons as a reason to taint everyone who uses it'.

R6: 'Not exclusively. By demonizing the Darknet they are forgetting that there are many other attack vectors, some more viable than TOR itself, by which a determined attacker can compromise their security, information and operations. Companies should assume threats to their information and computing infrastructure can come from ANY attack vector and plan their strategy accordingly.

R4: 'The Sony and Ashley Madison leaks were the end-result of poor security planning and implementation on the part of the companies involved. With Sony, the department responsible for security was poorly-staffed, and even more poorly-funded… Requests for resources, manpower, etc. are routinely ignored'.

Extracts from responses on online forums, May 2016

Less than a third of participants (5 out of 17) recognised that the Darknet can be a dangerous place, but they rejected the claim that it is inherently criminogenic. They emphasised that the Darknet is a neutral place and it is the users that determine the criminality of the network. Further, they indicated that the Darknet was labelled as criminal in order to justify law enforce activities and government control. More than two-thirds of participants (12 out of 17) made it clear that everyone should have freedom over their actions without fear of reprisals. For three examples:

R16: 'If you don't explicitly search for child pornography you won't find it. One has to differentiate. The Darknet can always be used and abused'.

R8: 'The Darknet is not inherently criminal, just as the clear net is not inherently criminal either. I'm sure that both have illegal content such as child porn or what have you. Albeit, there are also legal uses for both. The government creating an image that the Darknet is criminal is simply them trying to take away the human rights to privacy without legally doing so'.

R12: 'This actually made me laugh. What a nonsense! You really have to put in a lot of effort to hurt yourself or others through the Darknet. No such thing can happen accidently. The Darknet is not a threat to society, not more than the clear net anyway! I indeed think law enforcement exaggerated it all, just because they don't like admitting that they will never have everything under control'.

Extracts from responses on online forums, May 2016

Conclusion

In conclusion, this research is a small-scale exercise. To achieve a holistic understanding of the Darknet, much larger research projects that focus on its sociological dimensions would need to be undertaken. Our findings, however, have provided an alternative view of the Darknet in contrast to its current 'dark' image, which is constructed by the existing literature.

The Darknet can be viewed by some as the dark side of the Internet for valid reasons, which include its anonymous nature, virtual markets, and cryptocurrencies. However, most of our participants learned about it from conventional open sources. Once they start using the Darknet, freedom of expression becomes the main attraction sustaining their regular use of this network for many everyday activities. Despite the regular use, they do not, however, consider this network as a society. Without a solid and stable physical infrastructure that enables a sense of belonging, the Darknet is, and will always remain, a tool.

Even though many criminal activities take place on this network, the Darknet is not criminogenic. Many of these activities can also exist outside of it. Considering the virtual markets on the Darknet, most of our participants believe that the most famous one—the Silk Road—was used by governments and law enforcement agencies as a propaganda tool to discredit the freedom that the Darknet could offer. Certainly, we cannot deny that the illegal trading of drugs is a predominant activity in many Darknet markets. However, there are some positives associated with this activity, such as better-quality drugs and less stress and violence.

We cannot, of course, deny that the Darknet presents a serious security risk. Because of its unique characteristics, such as anonymity, virtual markets, and the use of cryptocurrencies, a range of criminal activities could be performed in this network with ease. As a result, the Darknet ought to be investigated more seriously. Yet, it should be noted that its inherent purpose is not to harm individuals, organisations, and societies. Instead of labelling an environment as criminogenic and its users as 'deviant others', a more holistic sociological understanding of the Darknet's social characteristics and technological infrastructures is now needed. Findings from such research would help to improve security technologies and practices to better cope with some of the more unique characteristics of the Darknet identified above. The Darknet is not, ultimately, a society where crime is the norm. In fact, it is a technological platform that is used by different individuals for a variety of purposes.

References

Afilipoaie, A. and Shortis, P. 2015. *From Dealer to Doorstep–How Drugs are Sold on the Dark Net.* Global Drug Policy Observatory, Situation Analysis.

Bartlett, J. 2014. Dark Net Markets: The eBay of Drug Dealing. *The Guardian*, 5 October. http://www.theguardian.com/society/2014/oct/05/dark-net-markets-drugs-dealing-ebay.

BBC. 2015. Silk Road Drug Website Founder Ross Ulbricht Jailed. *BBC News*, 30 May. http://www.bbc.co.uk/news/world-us-canada-32941060

BBC. 2017. Dark Net Guns Shipped in Old Printers. *BBC News*, 20 July. Retrieved from http://www.bbc.co.uk/news/technology-40668749.

Biryukov, A., Pustogarov, I., Thill, F. and Weinmann, R.P. 2014. Content and Popularity Analysis of Tor Hidden Services. In *Distributed Computing Systems Workshops (ICDCSW), IEEE 34th International Conference*; 30 June–3 July, Madrid, Spain: IEEE.

Boorstin, J. 2015. The Sony Hack: One Year Later. *CNBC*, 24 November. http://www.cnbc.com/2015/11/24/the-sony-hack-one-year-later.html.

Braun, V., and V. Clarke. 2006. Using Thematic Analysis in Psychology. *Qualitative Research in Psychology* 3 (2): 77–101.

Brown, M. 2014. Edward Snowden: The True Story Behind His NSA Leaks. *The Telegraph*, 24 October. http://www.telegraph.co.uk/culture/film/11185627/Edward-Snowden-the-true-story-behind-his-NSA-leaks.html.

Buxton, J. and Bingham, T. 2015. *The Rise and Challenge of Dark Net Drug Markets*. Global Drug Policy Observatory. Policy Brief No. 7.

Byrne, J.M., and K.A. Kimball. 2017. Inside the Darknet: Techno-Crime and Criminal Opportunity. In *Criminal Justice Technology in the 21st Century*, 3rd ed, ed. L.J. Moriarty, 206–232. Illinois: Charles C. Thomas Publisher.

Chandran, N. 2015. From Drugs to Killers: Exploring the Deep Web. *CNBC*, 23 June. http://www.cnbc.com/2015/06/23/from-drugs-to-killers-exploring-the-deep-web.html.

Chertoff, M. and Simon, T. 2015. *The Impact of the Dark Web on Internet Governance and Cyber Security*. Global Commission on Internet Governance. Paper Series No. 6.

Chmielewski, D. and Bergen, M. 2016. Google Better Get Used to Conspiracy Theories About Search Results This Election Year. *Recode*, 10 June. http://www.recode.net/2016/6/10/11905822/google-conspiracy-theory-search-election-2016-hillary-clinton.

Décary-Hétu, D., and L. Giommoni. 2017. Do Police Crackdowns Disrupt Drug Cryptomarkets? A Longitudinal Analysis of the Effects of Operation Onymous. *Crime, Law and Social Change* 67 (1): 55–75.

Dolliver, D.S. 2015. Evaluating Drug Trafficking on the Tor Network: Silk Road 2, the Sequel. *International Journal of Drug Policy* 26 (11): 1113–1123.

Dolliver, D.S., and J.L. Kenney. 2016. Characteristics of Drug Vendors on the Tor Network: A Cryptomarket Comparison. *Victims & Offenders* 11 (4): 600–620.

Duxbury, S.W., and D.L. Haynie. 2017. The Network Structure of Opioid Distribution on a Darknet Cryptomarket. *Journal of Quantitative Criminology*. https://doi.org/10.1007/s10940-017-9359-4.

Edwards, H. S. 2016. A Devastating Type of Hack is Costing People Big Money. *Time*, 21 April. http://time.com/4303129/hackers-computer-ransom-ransomware/.

Egan, M. 2016. What is the Dark Web? How to Access the Dark Web. What's the Difference Between the Dark Web and the Deep Web? *PC Advisor*, 28 April. http://www.pcadvisor.co.uk/how-to/internet/what-is-dark-web-how-access-dark-web-deep-joc-beautfiulpeople-3593569/.

Everett, C. 2015. Should the Dark Net be Taken Out? *Network Security* 2015 (3): 10–13.

Farrell, P. 2017. Inside the Darknet: Where Australians Buy and Sell Illegal Goods. *The Guardian*, 4 July. https://www.theguardian.com/technology/2017/jul/04/inside-the-darknet-where-australians-buy-and-sell-illegal-goods.

Finn, P. and Horwitz, S. 2013. U.S. Charges Snowden with Espionage. *The Washington Post*, 21 June. https://www.washingtonpost.com/world/national-security/us-charges-snowden-with-espionage/2013/06/21/507497d8-dab1-11e2-a016-92547bf094cc_story.html?utm_term=.fb2f6647d1a8.

Fox-Brewster, T. 2017. Forget Silk Road, Cops Just Scored Their Biggest Victory Against The Dark Web Drug Trade. *Forbes*, 20 July. https://www.forbes.com/sites/thomasbrewster/2017/07/20/alphabay-hansa-dark-web-markets-taken-down-in-massive-drug-bust-operation/#6abef9535b4b.

Greenberg, A. 2013. An Interview with A Digital Drug Lord: The Silk Road's Dread Pirate Roberts. *Forbes*, 8 August. http://www.forbes.com/sites/andygreenberg/2013/08/14/an-interview-with-a-digital-drug-lord-the-silk-roads-dread-pirate-roberts-qa/.

Greenwald, G., MacAskill, E. and Poitras, L. 2013. Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations. *The Guardian,* 10 June. http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.

Hardy, R.A., and J.R. Norgaard. 2016. Reputation in the Internet Black Market: An Empirical and Theoretical Analysis of the Deep Web. *Journal of Institutional Economics* 12 (3): 515–539.

Helms, R., S.E. Costanza, and N. Johnson. 2012. Crouching Tiger or Phantom Dragon: Examining the Discourse on Global Cyber-Terror. *Security Journal* 25 (1): 57–75.

Holm, E. 2017. The Darknet: A New Passageway to Identity Theft. *International Journal of Information Security and Cybercrime* 6 (1): 41–50.

Horsman, G. 2017. Can We Continue to Effectively Police Digital Crime? *Science & Justice* 57 (6): 448–454.

Horton-Eddison, M., and M. Di Cristofaro. 2017. *Hard Interventions and Innovation in Crypto-Drug Markets: The Escrow Example*, 11. Policy Brief: Global Drub Policy Observatory.

Jardine, E. 2015. *The Dark Web Dilemma: Tor, Anonymity and Online Policing*. Global Commission on Internet Governance. Paper Series No. 21.

Jeffray, C. and Feakin, T. 2015. *Underground Web The Cybercrime Challenge*. Australian Strategic Policy Institute, Special Report. https://www.aspi.org.au/report/underground-web-cybercrime-challenge.

Kruithof, K., J. Aldridge, D. Décary-Hétu, M. Sim, E. Dujso, and S. Hoorens. 2016. *Internet-Facilitated Drugs Trade—An Analysis of the Size, Scope and the Role of the Netherlands*. Santa Monica, CA: RAND EUROPE.

Kumar, A. 2014. DarkNet or DeepNet: What is It and How to Access It? *The Windows Club*, 1 October. http://www.thewindowsclub.com/darknet-deepnet.

Lacson, W., and B. Jones. 2016. The 21st Century DarkNet Market: Lessons from the Fall of Silk Road. *International Journal of Cyber Criminology* 10 (1): 40–61.

Lamont, T. 2016. Life After the Ashley Madison Affair. *The Guardian*, 28 February. https://www.theguardian.com/technology/2016/feb/28/what-happened-after-ashley-madison-was-hacked.

Lee, J., S. Menard, and L.A. Bouffard. 2014. Extending Interactional Theory: The Labeling Dimension. *Deviant Behavior* 35 (1): 1–19.

Leswing, K. 2016. Google Says Charges of Altering Search Results to Help Hillary Clinton are 'simply False'. *Business Insider UK*, 10 June. http://uk.businessinsider.com/google-says-no-altered-hillary-clinton-search-results-2016-6?r=USandIR=T.

Macaskill, E. and Dance, G. 2013. NSA Files: Decoded. *The Guardian*, 1 November. http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1.

Maor, E. 2013. Out of the Shadows: i2Ninja Malware Exposed. *Security Intelligence,* 20 November. https://securityintelligence.com/shadows-i2ninja-malware-exposed/.

Maor, E. 2015. The Darknet Isn't Just for Dark Deals. *Security Intelligence*, 17 February. https://securityintelligence.com/the-darknet-isnt-just-for-dark-deals/.

McGoogan, C. 2016. Dark Web Browser Tor is Overwhelmingly Used for Crime, Says Study. *The Telegraph*, 2 February. http://www.telegraph.co.uk/technology/2016/02/02/dark-web-browser-tor-is-overwhelmingly-used-for-crime-says-study/.

Meier, R.F. 1976. The New Criminology: Continuity in Criminological Theory. *Journal of Criminal Law & Criminology* 67 (4): 461–469.

Moloney, P. 2016. Dark Net Drug Marketplace Begin to Emulate Organised Street Crime. *The Sidney Morning Herald,* 15 January. http://www.smh.com.au/technology/technology-news/dark-net-drug-marketplaces-begin-to-emulate-organised-street-crime-20160111-gm3k1i.html.

Moore, D., and T. Rid. 2016. Cryptopolitik and the Darknet. *Survival* 58 (1): 7–38.

Murray, A. 2014. The Dark Web is not Just for Paedophiles, Drug Dealers and Terrorists, *The Independent*, 18 August. http://www.independent.co.uk/voices/comment/the-dark-web-is-not-just-for-paedophiles-drug-dealers-and-terrorists-9920667.html.

Novitski, N. 2014. The Cyber Threat Industry: Into the Darknet. *American Center for Democracy*, 2 May. Retrieved from http://acdemocracy.org/the-cyber-threat-industry-into-the-darknet/.

Olson, O. 2013. The Man Behind Silk Road—the Internet's Biggest Market for Illegal Drugs. *The Guardian*, 10 November. https://www.theguardian.com/technology/2013/nov/10/silk-road-internet-market-illegal-drugs-ross-ulbricht.

Omand, D. 2016. The Dark Net: Policing the internet's Underworld: World Policy: Winter 2015/2016. http://www.worldpolicy.org/journal/winter2015/dark-net.

Owen, G., and N. Savage. 2015. *The tor dark net*, 20. Paper Series no: Global Commission on Internet Governance.

Owen, G., and N. Savage. 2016. Empirical Analysis of Tor Hidden Services. *IET Information Security* 10 (3): 113–118.

Pace, J. 2017. Exchange Relations on the Dark Web. *Critical Studies in Media Communication* 34 (1): 1–13.

Paganini, P. 2013. How Edward Snowden Protected Information … and His Life. *Infosec Institute*, 25 July. http://resources.infosecinstitute.com/how-edward-snowden-protected-information-and-his-life/#gref.

Preuss, M. 2013. ChewBacca—a New Episode of Tor-based Malware. *Securelist*, 17 December. https://securelist.com/blog/incidents/58192/chewbacca-a-new-episode-of-tor-based-malware/.

Qiang, B., R. Zhang, Y. Wang, Q. He, W. Li, and S. Wang. 2014. Research on Deep Web Query Interface Clustering Based on Hadoop. *Journal of Software* 9 (12): 3057–3062.

Robinson, M. 2012. The eBay for Drugs: 'Silk Road' Website Allows UK Drug Users to Buy Cocaine and Heroin by Mail Order from all Over the World. *Daily Mail*, 19 November. http://www.dailymail.co.uk/news/article-2235199/The-eBay-drugs-Silk-Road-website-allows-drug-users-buy-heroin-cannabismail-order-world.html.

Rudesill, D.S., Caverlee, J. and Sui, D. 2015. *The Deep Web and the Darknet: A Look Inside the Internet's Massive Black Box.* Ohio State Public Law Working Paper No. 314.

Rushe, D. 2014. Silk Road 2.0's Alleged Owner Arrested as Drugs Website Shuttered by FBI. *The Guardian*, 6 November. http://www.theguardian.com/technology/2014/nov/06/silk-road-20-owner-arrested-drugs-website-fbi.

Samson, A. 2017. Dark Net May Pose 'Disruptive Risk' to Internet Sector—Goldman. *Financial Times*, 13 July. https://www.ft.com/content/d045b27e-0842-3686-800e-080d8ca883ae.

Simons, J. W. 2014. Guns, Drugs and Freedom: The Great Dark Net Debate. *The Telegraph*, 17 September. http://www.telegraph.co.uk/culture/books/11093317/Guns-drugs-and-freedom-the-great-dark-net-debate.html.

Soska, K. and Christin, N. 2015. Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem. *Proceedings of the 24th Usenix Security Symposium*; 12–14 August 2015, Washington, D.C: Advanced Computing Systems Association.

Stacey, E. 2017. *Combating Internet-Enabled Terrorism: Emerging Research and Opportunities: Emerging Research and Opportunities*. Hershey, PA: IGI Global.

The Tor Project. n.d. *Users*. https://metrics.torproject.org/userstats-relay-country.html. Accessed 3 February 2018.

UNODC. 2014. *World Drug Report 2014*. https://www.unodc.org/wdr2014/.

Van Buskirk, J., Naicker, S., Bruno, R.B., Breen, C. and Roxburgh, A. 2016. *Drugs and the Internet*. Issue 7. Australia: National Drug & Alcohol Research Centre.

Van Buskirk, J., A. Roxburgh, M. Farrell, and L. Burns. 2014. The Closure of the Silk Road: What has This Meant for Online Drug Trading? *Addiction* 109 (4): 517–518.

Van Hout, M.C., and T. Bingham. 2013. 'Silk Road', the Virtual Drug Marketplace: A Single Case Study of User Experiences. *International Journal of Drug Policy* 24 (5): 385–391.

Viney, S. 2016. What is the Dark Net, and How will it Shape the Future of the Digital Age? *ABC News*, 27 January. http://www.abc.net.au/news/2016-01-27/explainer-what-is-the-dark-net/7038878.

Wall, D.S. 2013. Enemies Within: Redefining the Insider Threat in organizational security Policy. *Security Journal* 26 (2): 107–124.

Weimann, G. 2016. Going Dark: Terrorism on the Dark Web. *Studies in Conflict & Terrorism* 39 (3): 195–206.

Weissman, C.G. 2015. The Creepiest and Most Bizarre Stories Told by People Who Explored the Internet's Hidden Websites. *Business Insider UK*, 30 June. http://uk.businessinsider.com/creepy-and-weird-deep-web-stories-from-reddit-2015-6?r=USandIR=T.

Williams, M., and M. Levi. 2015. Perceptions of the eCrime Controllers: Modelling the Influence of Cooperation and Data Source Factors. *Security Journal* 28 (3): 252–271.

Wright, A. 2008. Searching the Deep Web. *Communications of the ACM* 51 (10): 14–15.

Wyke, J. and Ajjan, A. 2015. The Current State of Ransomware. SOPHOS. A SophosLabs Technical Paper.

Yadron, D. 2016. Twitter Deletes 125,000 ISIS Accounts and Expands Anti-Terror Teams. *The Guardian*, 5 February. https://www.theguardian.com/technology/2016/feb/05/twitter-deletes-isis-accounts-terrorism-online.

Zheng, Q., Z. Wu, X. Cheng, L. Jiang, and J. Liu. 2013. Learning to Crawl Deep Web. *Information Systems* 38 (6): 801–819.