Tanja MILOSHEVSKA

UDK: 007:004.056
Review article

DARK WEB – NEW TRANSNATIONAL SECURITY THREAT

Abstract

In latest years, the Dark web has converted to one of the most debated themes in cyber security circles. Recent academic analyses and media articles tend to focus how the anonymous nature of the Darknet is used to enable criminal activities. This article analyses and underlines the major roles played by the Dark Web as a market; as a communication platform; as an enabler of cybercrime; as an enabler of anonymous financial transactions and as a proxy to a surface web. Precisely, it draw attention to the 'black market' of the Internet–the dark web that represents such a hidden space, being the largest deployed anonymity network. This success is supported by numerous features that are imbedded in the high-tech structure of the Dark web, for instance, secrecy, anonymity and the usage of cryptocurrencies. The distinctive environment of Dark Net markets as extremely anonymous and secretive, as well as reliable, makes them an ultimate test case for the unrestrained online marketplace.

Keywords: *DARK WEB, CYBER SECURITY, SECURITY THREAT, ILLEGAL ACTIVITIES, ILLEGAL SERVICES*

Introduction

The digital universe is huge, and the internet and World Wide Web (WWW) are much bigger than what we see through our regular browsing. The internet and its users are rapidly growing due to emerging applications of information technology (IT), and it is expected to continue to grow. However, the rapid growth of internet has left it susceptible to misuse and abuse which becomes significant threat and challenge in cyberspace around the globe (Ozkaya, Islam, 2019).

Internet and network technologies have evolved dramatically in the last two decades, with rising users' demands to preserve their identities and privacy. Researchers have developed approaches to achieve users' demands, where the biggest part of the internet has formed, the Deep Web. However, as the Deep Web provides the resort for many benign users who desire to preserve their privacy, it also became the perfect floor for hosting illicit activities, which generated the Dark Web (AlKhatib, Basheer, 2018).

The so-called Dark Web has been in the focus of the media in recent years, regularly in a negative context. With the takedown of the 'Silk Road' website in October 2013 by the FBI, the Dark Web entered the awareness of large parts of the population. In February 2015, the FBI took the infamous Dark

Web site 'Playpen' offline, which hosted more than 23,000 child pornographic images and videos and had more than 215,000 users (Koch, 2019).

As part of the preparation for the terrorist attacks in Paris in November 2015, the communication was anonymized by using the software Tor; while the weapon used in the shooting rampage in Munich in July 2016 was also acquired over the Dark Web. Beside drugs, weapons, and child pornography, every kind of information is sold via marketplaces on the Dark Web: from credit cards to sensitive information captured during data leaks or hacking attacks. The latter can pose new challenges for the armed forces (Koch, 2019).

Terminology

Quite often, the terms Darknet, Deep Web and Dark Web are improperly mixed or used interchangeably. Due to insufficient separation and misuse of terms, data and evaluations can be incorrectly assigned and falsify the actual situation.

Deep Web. The Deep Web "refers to any Internet information or data that is inaccessible by a search engine and includes all websites, intranets, networks and online communities that are intentionally and/or unintentionally hidden, invisible or unreachable to search engine crawlers" (Janssen 2018). The term, Deep Web, "relates to deep sea/ocean environments that are virtually invisible and inaccessible" (Janssen 2018). These hidden parts of the internet are known as the Deep Web. The Deep Web is approximately 400-500 times more massive than the Surface Web. (Wilson Centre, 2015). Therefore, the Deep Web "contains data that is dynamically produced by an application, unlinked or standalone Web pages/websites, non-HTML content and data that is privately held and classified as confidential. Some estimate the size of the Deep Web as many times greater than the visible or Surface Web" (Janssen 2018).

Darknet. From a technical and historical point of view, the term 'Darknet' is used to describe the part of the IP address space which is routable, but not in use. This must be differentiated from addresses, which should not be routed by definition. One of the early uses of the term with regard to digital content can be found in an article about content protection. It described Darknets as a 'collection of networks and technologies used to share digital content' (Biddle at al, 2002). Nowadays, the term is mainly used for overlay networks providing anonymous network connectivity and services. An overlay network is a layer of virtual network topology on top of the physical layer, which directly interfaces with users (Zhang 2003). Tor is an example of an overlay network, and the biggest and most widely used anonymisation network; but there are numerous others, such as I2P, Freenet or ZeroNet. It is important to recognize that the term Darknet originally refers to the network itself, and therefore the technical base like the protocol and devices; but not the content which may be transported through the network, or can be found on its respective servers (Koch, 2019).

The Dark Web refers to the websites which are hosted within overlay networks, and are normally not accessible without special software like the Tor Browser. Nowadays, usage of the Tor network is easy and straightforward: the Tor Browser is a complete bundle ready to use without installation by providing a fully configured Firefox Browser. As in the case of the Deep Web, search engine crawlers are not able to index the websites of the Dark Web. But in contrast to it, its most important feature is that the users of a service stay anonymous – neither a provider of a website can identify the visitors, nor can a visitor identify the service provider. Given this, the respective services are also called 'hidden services'; more recently, 'onion services' (Koch, 2019).

The deepest layers of the Deep Web, a segment known as the Dark Net, contains con-tent that has been intentionally concealed including illegal and anti-social information. The Dark Net can be defined as the portion of the Deep Web that can only be accessed through specialized browsers (like the Tor browser). A recent study found that 57% of the Dark Net is occupied by illegal content like pornography, illicit finances, drug hubs, weapons traffick-ing, counterfeit currency, terrorist communication, and much more (Moore, Rid, 2016).

Illicit activities and services

The Dark Web has been cited as facilitating a wide variety of crimes. Illicit goods such as drugs, weapons, exotic animals, and stolen goods and information are all sold for profit. There are gambling sites, thieves and assassins for hire, and troves of child pornography (Chertoff, Simon, 2015). Data on the prevalence of these Dark Web sites, however, are lacking. Tor estimates that only about 1.5% of Tor users visit hidden services/Dark Web pages (Tor Project Blog, 2015).

Illicit online markets, both on the surface web and on the dark web, provide criminal vendors the opportunity to purvey all manner of illicit commodities, with those of a more serious nature typically found deeper, in the dark web. Many of these illicit goods and services, such as cybercrime toolkits or fake documents, are enablers for further criminality (EUROPOL, 2018).

Cybercriminals can victimize individuals and organizations alike, and they can do so without regard for borders. How criminals exploit borders is a perennial challenge for law enforcement, particularly as the concept of borders and boundaries has evolved (Finklea, 2017).

Such activities are drugs trading, weapons trading, child abuse, trading sensitive information, malwares and spywares, sharing Software Exploits information that hacktivists discover in computer systems, or renting a Botnet, which is a full-equipped network connected to the internet that hackers can operate to perform a wide range security breach. In addition to trading documents, fake IDs, stolen credit cards, patients' medical records, and any other Personally Identifiable Information (PII). It also includes financial fraudulence,

publicizing criminal ideologies, even employing hitmen, and a lot more. Dark Web Hidden Service stake place in the Dark Web as well, they are special services that host the security breach activities, and work as the hosting environment for malwares (Hawkins, 2016).

Broad Role	Specific Cases	Description
As a Market	Illicit drugs traded on markets	All ranges of drugs from marijuana to cocaine are being sold on eBay-like platforms, e.g. Silk Road 3.0. (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. (Armin et al., 2015).
	Credit card, identities, breached data made traded on markets	Stolen credit card info, medical profiles, personally identifying information (PII) allowing identify theft. (Denic, 2017)
	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 Playpen12. (Kirkpatrick, 2017).
	Weapons traded on markets	Guns for sale, especially in countries where banned (Rhumorbarbe et al., 2018).

Broad Role	Specific Cases	Description
As a Communication platform	Forums for discussion	Sharing ideas, knowledge, propaganda, recruitment, and training. Used by hackers, terrorists, journalists, citizens concerned about sensitive topics. (Sapienza et al., 2018).
	Chat for real-time communication	Instant Messaging/Chat facilitated by Tor, e.g. TorChat13, or end-to-end encrypted chat software, e.g. Telegram14 and Signal15, known to be in use for private communication in real-time. (Maddox et al., 2016).

Broad Role	Specific Cases	Description
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).
	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 conjunction with other roles	Recruitment, training, radicalisation, planning, fundraising for known terrorist organisations, e.g. ISIL (Broadhurst, 2017).

Broad Role	Specific Cases	Description
As a source of Threat Intelligence	Scanning Forums & Marketplaces for threat intelligence	Generating leads on the type of attacks that may be imminent based on exploits being sold and discussed. (Robertson et al., 2017).

Broad Role	Specific Cases	Description
As an enabler of anonymous Financial Transactions	Using Bitcoin over Tor for anonymity	Added layer of anonymity and precaution (DiPiero, 2017).
	Money Laundering of cryptocurrencies via tumbling services	Specific services to launder money, e.g. via bitcoin conversion (Dalins et al., 2017).

Broad Role	Specific Cases	Description
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).
	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. (Moore and Rid, 2016).

According to the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA, 2018) and Europol, Germany, the Netherlands and the United Kingdom were the most important countries with regards to the EU-based Darknet drug supply, in terms of sales revenue and volumes. Other research indicates that vendors of certain drugs commodities, such as cannabis and cocaine, are primarily located in a small number of highly active consumer

countries. This further suggests that most Darknet market vendors are 'local' retailers serving the 'last mile' for drug trafficking routes (Dittus, at al, 2018). This is supported by other research that Darknet markets are mostly used for mid or low-volume market sales or sales directly to consumers. Large-volume sales (wholesale) on Darknet markets are relatively uncommon (Europol, 2018).

However, since the commerce of illicit goods is one of the most predominant activities taking place in the Deep Web, it has become essential in the context of high anonymity, to be able to guarantee trust and reputation among sellers and buyers without having to rely on an external authority like a banking institution as in electronic commerce. We are foreseeing the rise of new, completely decentralized marketplaces that rely on the blockchain technology that Bitcoins and other cryptocurrencies already exploit for transport and storage. As such, the technology will be used to implement full-blown marketplaces without a single point of failure and that rely on particular aspects of game theory to guarantee safe transactions, escrow mechanisms, and trust between actors who may be shady in nature to begin with (Ciancaglini at al, 2015).

Terrorist use of online platforms

Terrorists have been active on various online platforms since the late 1990s (Weimann, 2016). The Surface Web, however, was revealed to be too risky for anonymity-seeking terrorists: they could be monitored, traced and found. Many of the terrorist websites and social media on the Surface Web are monitored by counter-terrorism agencies and are often shut down or hacked. In contrast, on the Dark Net, decentralized and anonymous net-works aid in evading arrest and the closure of these terrorist platforms. "ISIS's activities on the Surface Web are now being monitored closely, and the decision by a number of governments to take down or filter extremist content has forced the jihadists to look for new online safe havens," (Berton, 2015).

This has led to their migration to the dark web and made their conduct even more resilient to being disrupted (Denic, 2017). 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. 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).

Following the attacks in Paris in November 2015, ISIS has turned to the Dark Net to spread news and propaganda in an apparent attempt to protect the identities of the group's supporters and safeguard its content from hacktivists. The move comes after hundreds of websites associated with ISIS were taken down as part of the Operation Paris (OpParis) campaign launched by the

amorphous hacker collective Anonymous. ISIS's media outlet, Al-Hayat Media Center, posted a link and explanations on how to get to their new Dark Net site on a forum associated with ISIS (Weimann, 2017).

In April 2018 a report, entitled "Terror in the Dark", summarizes the findings of a study, revealing the growing use of the Dark Net by terrorist groups (Malik, 2018). The findings illustrate how terrorists and extremists are creating growing numbers of safe havens on the Dark Net to plot future attacks, raise funds and recruit new followers. This report highlights the following uses of the Dark Net for terrorist purposes:

1. Terrorists use the Dark Net to hide: The monitoring of the surface web by social media companies and security officials has resulted in a faster rate of removal of extremist content from social media platforms. Correlated with this is an increased use by terrorist networks of the Dark Net for communication, radicalization and planning attacks.

2. Terrorists use the Dark Net for recruitment: While initial contact can be made on surface web platforms, further instructions are often given on end-to-end encryption apps, such as Telegram, on how to access jihadist websites on the Dark Net.

3. Terrorists use the Dark Net as a reservoir of propaganda: The removal of extremist and terrorist content from the surface web increases the risk that material of terrorist organizations may be lost. Much of this material later re-surfaces on the Dark Net.

4. Terrorists use virtual currencies to evade detection and to fundraise: Terrorists, like criminals, use cryptocurrency, because it provides the same form of anonymity in the financial setting as encryption does for communication systems (Weimann, 2016).

Whereas the Dark Web is most well-known for hosting illicit economic trade, it has become clear that the Dark Web also holds some very serious national security implications that will affect most nations throughout the globe. The proliferation of cyber and kinetic weapons, the facilitation of terrorism, intelligence gathering, extortion, malicious services-for-hire à all of these illicit activities are occurring on the Dark Web, and the evidence put forth in this paper suggests that these activities may occur at increasing rates in the coming future (Rivera, Archy, 2019).

Conclusion

The Dark Web presents a serious security risk and clandenstine networks become a way to attain freedom in the Internet; while from another point of view these networks are nothing more than new channels to make their criminogenic desires explicit.

Findings from this paper would help to the progress of security technologies and practices to better manage some of the more unique characteris-

tics of the Darknet identified above. The Dark Web is not, eventually, a society where crime is the model or pattern. In fact, it is a technological platform that is used by different individuals for a variety of purposes.

References:

ALKHATIB, B. BASHEER, R. (2018). Crawling the Dark Web: A Conceptual Perspective, Challenges and Implementation. *Journal of Digital Information Management*. Syrian Virtual University. Syria.

ARMIN, J. AT AL. (2015). 0-day vulnerabilities and cybercrime, in: Availability, Reliability and Security (ARES), 10th *International Conference On.*

BERTON, B. (2015). "The dark side of the web: ISIL's one-stop shop?". Report of the European Union Insti-tute for Security Studies, June 2015. Available at: http://www.iss.europa.eu/uploads/media/Alert_30_The_-Dark_Web.pdf.[Accessed 17 February 2020].

BIDDLE, P. AT AL. (2002). The Darknet and the Future of Content Protection. In ACM Workshop on Digital Rights Management, Springer-Verlag Berlin Heidelberg.

BROADHURST, R. (2017). *Cyber Terrorism Research Review Cyber Terrorism*: Research Review Research Report of the Australian National University. Available at: https://doi.org/10.13140/RG.2.2.19282.96964. [Accessed 17 February 2020].

BRYNIELSSON, J. AT AL. (2013). Harvesting and analysis of weak signals for detecting lone wolf terrorists. *Secur. Inform*. 2, 11.

CHERTOFF, M., SIMON, T. (2015). *The Impact of the Dark Web on Internet Governance and Cyber Security,* Global Commission on Internet Governance, The Royal Institute od International Affairs, Centre for International Governance Innovation and Chatham House, No. 6. Available at: https://www.cigionline.org/sites/default/files/gcig_paper_-no6.pdf. [Accessed 17 February 2020].

CIANCANGLINI VINCENZO AT AL. (2015). *Below the Surface: Exploring the Deep Web* Trend Micro.

DALINS, J. AT AL. (2017). *Criminal motivation on the dark web: A categorisation model for law enforcement.* Digit. Investig.

DENIC, N. V. (2017). *Government Activities to Detect, Deter and Disrupt Threats Enumerating from the Dark Web,* thesis presented to the Faculty of the U.S. Army Command and General Staff College, Fort Leavenworth, Kansas.

DIPIERO, C. (2017). Deciphering Cryptocurrency: Shining a Light on the Deep Dark Web. U. *Ill. L. Rev*.1267.

DITTUS, M. AT AL. (2018). Platform Criminalism: The 'last-mile' geography of the darknet market supply chain, in WWW 2018, Lyon: France. European Monitoring Centre for Drugs and Drug Addiction (2018).

Available at: http://www.emcdda.europa.eu/drugs-library/emcdda-europol-working-arrangement-2018_en. [Accessed 16 February 2020].

EUROPOL. (2018). *Internet Organized Crime Threat Assessment*, European Union Agency for Law Enforcement Cooperation 2018.
Available at: www.europol.europa.eu. [Accessed 12 March 2020].

FINKLEA, K. (2017). *The Interplay of Borders, Turf, Cyberspace, and Jurisdiction: Issues Confronting U.S. Law Enforcement*, CRS Report R41927.

HAWKINS, B. (2016). Under The Ocean of the Internet - The Deep Web.
Available at: https:/ /www.sans.org/reading-room/whitepapers /covert/ oceaninternet-deepweb-37012. [Accessed 22 February 2020].

HUANG, K. AT AL. (2017). *Cybercrime-as-a-Service: Identifying Control Points to Disrupt*.

JANSSEN, D. (2018). Deep Web. Techopedia 2018.

KIRKPATRICK, K. (2017). Financing the Dark Web. *Commun*. ACM 60, 21–22.

KOCH, R. (2019). *Hidden in the Shadow: The Dark Web – A Growing Risk for Military Operations?*, NATO CCD COE Publications, Tallinn.

KREBS, B. (2015). "Tax Fraud Advice, Straight From the Scammers," *Krebs on Security*.

MADDOX, A. AT AL. (2016). Constructive activism in the dark web: cryptomarkets and illicit drugs in the digital 'demimonde.' *Inf. Commun. Soc*. 19, 111–126.
Available at: https://doi.org/10.1080/1369118X.2015.1093531 [Accessed 17 February 2020].

MALIK, N. (2018). "Terror in the Dark", a report by the the Henry Jackson Society, London.
Available at: http://henryjackson-society.org/wpcontent/uploads/2018/-04/Terror-in-the- Dark.pdf. [Accessed 17 February 2020].

MOORE, D., RID, T. (2016). Cryptopolitik and the Darknet. *Survival* (Lond). 58, 7–38.

OWEN, G. SAVAGE, N. (2016). Empirical analysis of Tor hidden services. IET *Inf. Secur.* 10, 113–118.

OZKAYA E, RAFIKUL, I. (2019*). Inside the Dark Web*, CRC Press, Taylor and Francis Group: USA.

RHUMORBARBE, D. AT ALL., (2018). Characterising the online weapons trafficking on cryptomarkets. *Forensic Sci. Int*. 283, 16–20.

RIVERA, J. ARCHY, W. (2019). The Role of the Dark Web in Future Cyber Wars to Come, *Small War Journal*.
Available at: https://smallwarsjournal.com/jrnl/art/role-dark-web-future-cyber-wars-com. [Accessed 1 February 2020].

ROBERTSON, J. AT AL. (2017). *Darkweb Cyber Threat Intelligence Mining*. Cambridge: University Press.

SAPIENZA, A. AT AL. (2018). Early Warnings of Cyber Threats in Online Discussions.arXiv Prepr. arXiv1801.09781.

TOR PROJECT BLOG. (December 30, 2014) *Tor: 80 Percent of ??? Percent of 1-2 Percent Abusive*.

TZANETAKIS, M. (2018). Comparing cryptomarkets for drugs. A characterization of sellers and buyers over time. *Int. J. Drug Policy*.

WEIMANN, G. (2016). "Going Dark: Terrorism on the Dark Web", *Studies in Conflict & Terrorism* 39, 195-206.
Available at: http://www.tandfonline.com/doi/abs/10.1080/1057610X.2015.1119546. [Accessed 12 February 2020].

WEIMANN, G. (2017). *Going Darker-The challenge of Dark Net Terrorism*, Wilson Center, Washington DC, USA.

WILSON CENTER REPORT. (2015). "The Deep Web and the Darknet: A Look Inside the Internet's Massive Black Box".
Available at: https://www.wilsoncenter.org/sites/default/files/deepweb-report_october_2015.pdf. [Accessed 12 April 2020].

ZHANG, X. (2003). System/Application Designs, Optimization and Implementations on Overlay Networks. High Performance Computing and Software Lab. Ohio State University.