Kriminalističke teme
Zbornik radova
Godina XIX, Broj 5, 2019.
ISSN 1512-5505

DARK WEB AS A CONTEMPORARY CHALLENGE TO CYBER SECURITY

Pregledni naučni rad

Tanja MILOSHEVSKA, PhD[87]

ABSTRACT

Inspiration for work:
This paper looks specifically at the dark net which has become notorious in the media for being a hidden part of the web where all manner of illegal activities take place. 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.
Goals of paper:
This article analyzes and highlights 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.
Methodology/Concept:
The paper is managed by looking at current literature in academic journal databases and own research in dark web. The motivation behind this literature review is to estimate the current state and development of the dark web in relation to the roles it plays and explore how the dark web enables cybercrime.
Limits of the research/work:
It contributes to the space of the dark web by assisting as a citation document and by suggesting a research agenda to renew study on this phenomenon and allow for better projections on how it may reveal over time and as technology expands.
Results/Conclusions:
Criminality on the dark web spans multiple areas and involves a wide range of criminal commodities. An effective countermeasure will therefore require a suitably coordinated, cross-cutting response, involving investigators with equally diverse expertise. This will likely require additional capacity building and training of officers not involved in computer crime. And while though this awareness may not necessarily stop national security threats from the Dark Web, it can certainly shine a spotlight on the issue and facilitate a larger conversation on how the global community can address these emerging threats.
Accontability of the research:
The unique nature of Dark Net markets as highly anonymous and secretive, as well as loyal and intelligent, makes them an ideal test case for the unrestrained online marketplace. There is a need for a global strategy and accountabilty to address the abuse of

[87] Ss. Cyril and Methodius University – Skopje, Faculty of Philosophy, Institute of Security, defense and peace, E-mail: tanja@fzf.ukim.edu.mk

the dark web and other emerging platforms for illicit trade.

Key words
dark web, cyber crime, cyber security, networks, illegal activities

Introduction

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 interet – the dark web - represents such a hidden space.

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 (Vogt, 2017).

The Dark Web began with ARPANET, the Internet's progenitor that was developed by the Pentagon in 1969. As the inter-computer interaction began to grow, "a number of isolated, secretive networks started to appear alongside ARPANET" (McCormick, 2013). These networks eventually became the medium of choice for the U.S. Naval Research Laboratory, which introduced a browser called The Onion Router. Tor, as it is called now, "conceals the location and IP addresses of users who download the software" (McCormick, 2013) in order to protect overseas American operatives and dissidents. However, the software became available for public consumption in 2004, and Tor domains dedicated to drug dealing, child pornography, and terrorism began cropping up.

The Dark Web encompasses a vast amount of information on the Internet, the majority of which is inaccessible to the average user. Tor, the most popular Dark Web browser, which was initially created as a security measure by the U.S. Navy, is now the medium of choice for illegal sites ranging from drug dealing to assassination and terrorism (Lascon and Jones, 2016).

Last year, law enforcement dealt online criminal markets on the dark web a significant blow when two major operations, led by the FBI, the US Drug Enforcement Agency (DEA) and the Dutch National Police, with the support of Europol and a number of other law enforcement agency partners, dismantled two of the largest Darknet markets: AlphaBay

and Hansa. Until that point, along with the Russian Anonymous Marketplace (RAMP), these three markets had accounted for 87% of all Darknet market activity (Chainnalysis, 2018).

Providing easy access to a wide range of illicit commodities and services, these markets are key enablers for other crimes.

Darknet/hidden services

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.

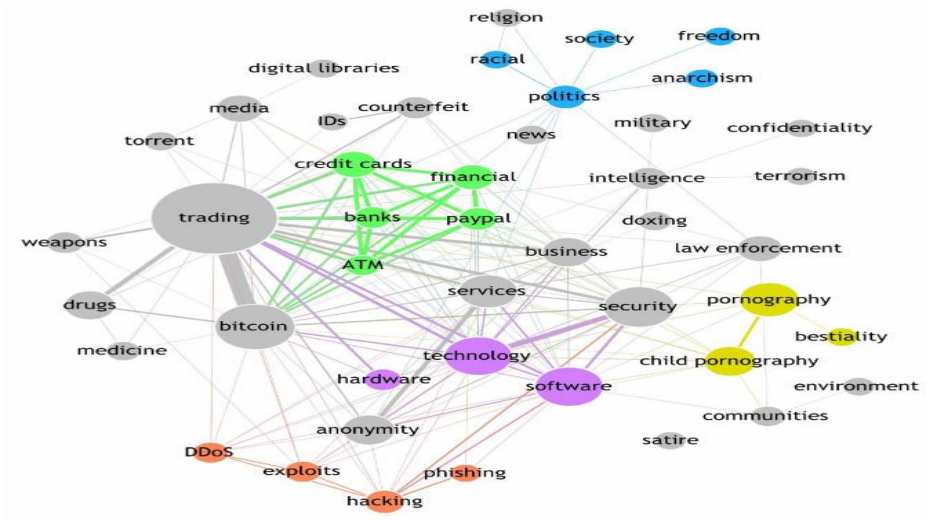

Figure 1: A topic taxonomy of Tor hidden services (Spitter at all, 2014)

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 and 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).

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).

Physical Borders. For law enforcement purposes, jurisdictional boundaries have been drawn between nations, states, and other localities. Within these territories, various enforcement agencies are designated authority to administer justice. When crimes cross boundaries, a given entity may no longer have sole responsibility for criminal enforcement, and the laws across jurisdictions may not be consistent (Richman, 2000). Criminals have long understood these phenomena—and exploited them.

Physical–Cyber Borders. The relatively clear borders within the physical world are not always replicated in the virtual realm. High-speed Internet communication has not only facilitated the growth of legitimate business, but it has bolstered criminals' abilities to operate in an environment where they can broaden their pool of potential targets and rapidly exploit their victims. Frauds and schemes that were once conducted face-to-face can now be carried out remotely from across the country or even across the world. For instance, criminals can rely upon botnets to target victims across the globe without crossing a single border themselves.

Cyber Borders. While cyberspace crosses physical borders, boundaries within cyberspace—both jurisdictional and technological—still exist. Some web addresses, for instance, are country-specific, and the administration of those websites is controlled by particular nations. Another barrier in cyberspace involves the lines between the Surface Web and the Deep Web. Crossing these boundaries may involve subscriptions or fee-based access to particular website content. Certain businesses—news sites, journals, file-sharing sites, and others—may require paid access. Other sites may only be accessed through an invitation.

The Dark Web can play a number of *roles* in malicious activity. As noted, it can serve as a forum—through chat rooms and communication services—for planning and coordinating crimes. For instance, there have been reports that some of those engaged in tax-refund fraud discussed techniques on the Dark Web (Krebs, 2015).

Roles played by the Dark Web

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.

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. (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, 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, Wright and Graham, 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).

The closure of any market will inevitably lead to the migration of customers and vendors to new or existing markets. Prior to the official announcement of the joint market seizures, Alphabay had been offline for several weeks. This had already resulted in a 25% increase in the number of listings appearing on Hansa, as it presumably absorbed the business from its chief competitor. Three months after Alphabay went offline and following the closure of Hansa and RAMP, several of the remaining markets had similarly displayed considerable growth in the number of listings they advertised. Dream Market, the largest remaining English language market, had grown by 20%, while several of the smaller markets such as Wall Street, TradeRoute and T-Chka/P-int had grown by 290%, 475% and 840% respectively (Europol, 2018). However, even collectively these markets did not meet the former scale of Alphabay, suggesting an overall decrease in dark web activity. Industry reporting supports this by highlighting that the value of Bitcoin transactions to Darknet markets fell by two thirds in the aftermath of the takedown operations (Chainalysis, 2018).

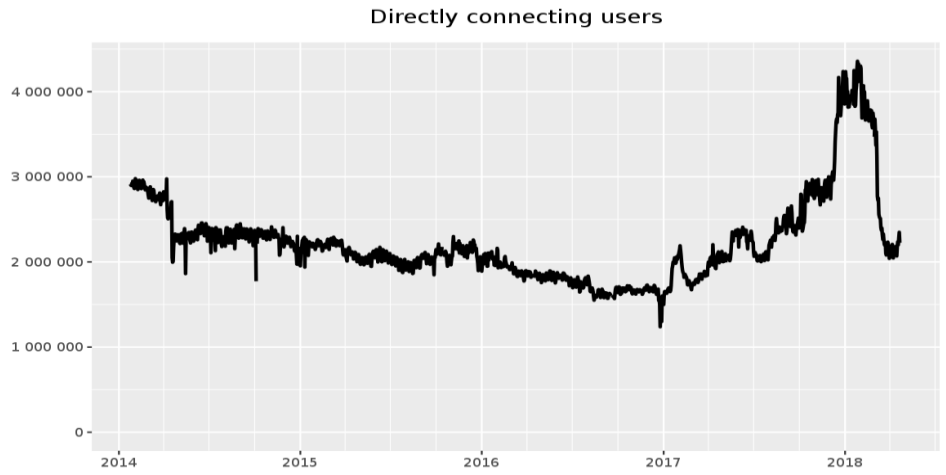

Figure 2*:* Number of users directly connected to Tor (last four years) (Top Project, 2018).

Regardless of 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 2 above) over the last year.

Compromised data - key commodity on Darknet markets

Compromised personal, medical and financial data is a key commodity for the commission of cyber-dependent crime, but even more so for cyber-enabled crime. It plays a crucial role in activities such as frauds, phishing, identity theft and account takeovers. The prominence of data on Darknet markets reflects this. Data is often the second or third largest category of commodity listed and one of the more common commodities highlighted by law enforcement.

In last year's Europol report (2018), was described the large number of automated credit card shops on the surface web. These are online stores which sell large quantities of compromised payment card data using a fairly standardised automated shopping interface. While a large number of these sites still exist on the surface web, there are a growing number of reports of such sites migrating to the dark web.

Emerging Trends Pertaining to National Security

Whereas the last section of this paper discussed observations so far, this section of the paper will delve into the possibilities of how the Dark Web may evolve to affect national security in years to come. Rather than listing a series of discrete possibilities (as the possibilities are literally endless), we will instead put forth a categorical framework that covers the types of Dark Web national security threats that defense professionals are likely to encounter. Before diving in, we want to make it very clear that no framework is infallible. It is very likely that there are categories of Dark Web threats and possible trends that we did not cover in this framework. We are aware that the threat landscape could change in the blink of an eye as emerging technologies such as quantum computing, digital currency, and 3-D printing continue to evolve. Given these caveats, our understanding of the historical threat landscape, and our research into emerging Dark Web trends, the following is our proposed framework:

Proliferation - Kinetic Weapons

The anonymity facilitated through the Dark Web fosters an ideal trading ground for would-be buyers and sellers of dangerous weapons. This is more than just theoretical – it is a fact that has been proven through observation time and time again. Uranium, dangerous chemical compounds, military grade firearms à these are sample subset of the types of weapons that have been listed on the Dark Web. In response to these listings, the global law enforcement community has been aggressively pursuing would be buyers and sellers of weapons on the Dark Web – and in many cases they have been successful in thwarting potential attacks. In 2016, the U.S. Federal Bureau of Investigation (FBI) collaborated with Irish law enforcement authorities to stop an Irish Republic Army (IRA)

militant from procuring handguns, grenades, and plastic explosives from a Dark Web marketplace (Aliens, 2018). And while the national security community can claim minor victories with these types of preventative operations, those interested in anonymously buying and selling kinetic weapons have begun to shift their methodology.

Over the coming years, we assess that there will be two major evolutions to the ways that kinetic weapons are traded on the Dark Web. The first is that buyers and sellers of Dark Web weapons will likely move their business away from some of the more popular open-access marketplaces (such as Dream Market) and over to other marketplaces that require a higher degree of vetting to enter (such as Demon Forum and OG-Users Forums). This is likely to happen for two primary reasons. The first is that the individuals who engage in the weapons trade are becoming more wary of undercover law enforcement presence and the possibility that they are being lured into a trap. The second is that the major marketplaces are likely becoming less tolerant of the risk they incur by allowing weapons listings on their marketplaces. Weapons listings have historically attracted the attention of the global law enforcement community, which has resulted in undercover officers perusing markets looking for leads. Beyond the increased risk, the marketplace profit margin for the weapons trade is relatively low when compared to the profit margins of other high-volume illicit goods such as drugs and fraud. According to two studies conducted by RAND (2016), global drug sales on the Dark Web were estimated to be between $12-$21.1 million per month in 2016, while the global arms trade was $80k per month in 2017. (RAND, 2017). Below is an image from the Dark Web listing some of the locations where threat actors can still purchase weapons:

Weapons / Оружие	
Guns	Guns and Ammo / Пистолеты и боеприпасы
Pistols	Your european arms dealers / Поставка европейского оружия
Weapons	Guns,Pharmacy,Counterfeits / Оружие, наркотики, подделки валют
Guns Store	Verified marketplace for Guns and other weapons, worldwide shipping / Склад оружия,доставка по всему миру
Lucky47	Weapons from Ukraine / Оружие с Украины
GG Club	Stocks every type of rifle to meet your needs / Оружие и боеприпасы для ваших нужд
Darkseid guns shop	Rifles, Handguns, Silencers, Body Armour / Винтовки, пистолеты, глушители, бронежилеты

Image 5: Examples of Limited Access Dark Web Marketplaces (Rivera and Arcy, 2019)

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.

Reflections

Criminality on the dark web spans multiple areas and involves a wide range of criminal commodities. An effective countermeasure will therefore require a suitably coordinated, cross-cutting response, involving investigators with equally diverse expertise. This will

likely require additional capacity building and training of officers not involved in computer crime. And while though this awareness may not necessarily stop national security threats from the Dark Web, it can certainly shine a spotlight on the issue and facilitate a larger conversation on how the global community can address these emerging threats.

However, even with all three top markets sensationally being taken offline by police in the space of a few months, the will or desire to migrate from the familiar territory of Tor to another, potentially safer digital environment still does not appear to be there. It therefore seems unlikely that this will come to pass in the foreseeable future.

The almost inevitable closure of large, global Darknet marketplaces has led to an increase in the number of smaller vendor shops and secondary markets catering to specific language groups or nationalities.

The unique nature of Dark Net markets as highly anonymous and secretive, as well as loyal and intelligent, makes them an ideal test case for the unrestrained online marketplace.

There is a need for a global strategy to address the abuse of the dark web and other emerging platforms for illicit trade.

References

- Armin, J., Foti, P., Cremonini, M. (2015). 0-day vulnerabilities and cybercrime, in: Availability, Reliability and Security (ARES), 10th International Conference On.
- Broadhurst, R. (2017). Cyber Terrorism Research Review Cyber Terrorism: Research Review Research Report of the Australian National University. doi: https://doi.org/10.13140/RG.2.2.19282.96964
- C. Aliens. (2018). "More Details Revealed In The Dublin Explosives Case", Deep Dot Web. doi: https://www.deepdotweb.com/2018/08/05/more-details-revealed-in-the-dublin-explosives-case/.
- Chainalysis. (2018). The changing nature of cryptocrime, Chainalysis: Darknet Market Activity Nearly Doubled Throughout 2018, Crypto Crime Report. doi: https://e-cryptonews.com/chainalysis-darknet-market-activity-nearly-doubled-throughout-2018/.
- 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. doi: https://www.cigionline.org/sites/default/files/gcig_paper_no6.pdf.
- Dalins, J., Wilson, C., Carman, M. (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., Wright, J., Graham, M.. (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). doi: http://www.emcdda.europa.eu/drugs-library/emcdda-europol-working-arrangement-2018_en.
- Finklea, K. (2017). The Interplay of Borders, Turf, Cyberspace, and Jurisdiction: Issues Confronting U.S. Law Enforcement, CRS Report R41927.
- Huang, K., Siegel, M., Madnick, S. (2017). Cybercrime-as-a-Service: Identifying Control Points to Disrupt.
- Internet Organized Crime Threat Assessment (2018), Europol, European Union Agency for Law Enforcement Cooperation 2018. doi: www.europol.europa.eu.
- "International arms trade on the dark web". (2017). RAND Corporation. doi: https://www.rand.org/randeurope/research/projects/international-arms-trade-on-the-hidden-web.html.
- Kirkpatrick, K. (2017). Financing the Dark Web. Commun. ACM 60, 21–22.
- Krebs, B. (2015). "Tax Fraud Advice, Straight From the Scammers," Krebs on Security.

- 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. doi: https://doi.org/10.1080/1369118X.2015.1093531
- McCormick, T. (2013). The Darknet. Foreign Policy, (203), 22-24.
- 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.
- Rhumorbarbe, D, at all., (2018). Characterising the online weapons trafficking on cryptomarkets. Forensic Sci. Int. 283, 16–20.
- Richman, D. (2000). "The Changing Boundaries Between Federal and Local Law Enforcement," Boundary Changes in Criminal Justice Organizations, pp. 81-111, http://www.ncjrs.gov/criminal_justice2000/vol_2/02d2.pdf.
- Rivera, J., Archy, W. (2019). The Role of the Dark Web in Future Cyber Wars to Come, Small War Journal. doi: https://smallwarsjournal.com/jrnl/art/role-dark-web-future-cyber-wars-com.
- Robertson, J., at all. (2017). Darkweb Cyber Threat Intelligence Mining. Cambridge: University Press.
- Sapienza, A. at all, (2018). Early Warnings of Cyber Threats in Online Discussions. arXiv Prepr. arXiv1801.09781.
- 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.
- "Taking Stock of the Online Drugs Trade". (2016). RAND Corporation. doi: https://www.rand.org/randeurope/research/projects/online-drugs-trade-trafficking.html.
- The Tor Project. (2018a). Tor Metrics [WWW Document]. Tor Proj. doi: https://metrics.torproject.org/
- The Tor Project. (2018b). Tor Project [WWW Document]. doi: https://www.torproject.org/
- Tor Project Blog. (December 30, 2014) Tor: 80 Percent of ??? Percent of 1-2 Percent Abusive.
- Tzanetakis, M. (2018). Comparing cryptomarkets for drugs. A characterisation of sellers and buyers over time. Int. J. Drug Policy.
- Vogt, S.D. (2017). The Digital Underworld: Combating Crime on the Dark Web in the Modern Era. St. Cl. J. Int'l L. 15.
- Wesley L., Jones, B. (2016). The 21st Century DarkNet Market: Lessons from the Fall of Silk Road, International Journal of Cyber Criminology (IJCC).