THE INFLUENCE OF BLACK MARKET ACTIVITIES THROUGH DARK WEB ON THE ECONOMY: A SURVEY

Hilary Mazi
Department of Information Assurance
St. Cloud State University
St. Cloud, MN 56301, USA
hemazi@go.stcloudstate.edu

Foka Ngniteyo Arsene
Department of Information Assurance
St. Cloud State University
St. Cloud, MN 56301, USA
ngar1001@go.stcloudstate.edu

Akalanka Mailewa Dissanayaka
Department of Computer Science and IT
St. Cloud State University
St Cloud, MN 56301, USA
amailewa@stcloudstate.edu

Abstract

The economy of a country is driven in part by the variety of businesses that thrive in it. Competition among these businesses is encouraged as long as they follow specific rules set forth by the governments in which they operate. However, it becomes an entirely different story when the competitors play in a completely different environment and make their own rules. The black market has long provided such an environment but it used to be confined to a particular geographic area, and very few thrived outside of their geographic location, until the Dark Web was introduced. The Dark Web has provided to any black market business of any size to expand their business outside of their geographic location. The black market by itself already influences businesses with whom they share the same geographic location. But the Dark Web expands the black market's influence to a global scale. This paper first, looks into the influence of Black Market activities on the Dark Web. Then, it presents how both the Black Market and the Dark Web affect on the economy of individual countries and on the world's economy as a whole.

Keywords: GDP, Black Market, Dark Web, Deep Web, Network Security, Threats, Vulnerabilities, Hacking, Cybersecurity.

1. INTRODUCTION

According to a "Research and Development" (RAND) corporation study, the black market for hacking tools, services, and byproducts is continuing to expand. The black-market expanding causes bigger threats to businesses, governments and individuals [1][2]. It is clear to cybercriminals the value of the information they steal by hacking. Bank accounts, credit cards, and social security numbers mean life to average people. Those items are being traded for money in the cyber black market, in the favor of hackers [3]. As the Cybersecurity Ventures site posted, the cybercrime industry cost the world three trillion dollars in 2015. It is predicted to be doubled by 2021. The cost of cybercrimes includes damages to companies, investments in technology, upgrading security policies and ransoms paid to get back what got stolen [4]. "Hacking used to be ab activity that was mainly carried out by individuals working alone, but over the last 15 years the world of hacking has become more organized and reliable" said Lillian Ablon, the lead author of RAND's research [1]. That help us understand more how big the black market is these days.

Following a research conducted by Crowe UK [6] on how the United Kingdom's (UK) top brands have been attacked or damaged by the Dark Web, 23 of the 50 brands been researched were affected by the Dark Web.

Table 1: Business areas in the UK affected by the Dark Web [6]

Business Area	**Number of Businesses affected**
Banking and Finance	8
Telecommunication	6
Retail and Entertainment	4
Energy and Transportation	3

The attacks conducted on these companies did not only come from expert hackers, as the Dark Web has forums from where even the novice hacker could get advice and guidance on how to conduct attacks [6][7]. The same research pointed out that Invoice Fraud causes approximately nine million pound in losses per year to United Kingdom's Small and Medium Enterprises (SMEs). Furthermore, indirect attacks at business were another means for hackers to obtain valuable information from their victims. An example of this was the case where 16,600 Bank account numbers and sort codes were exposed after a telecommunication company, Talk Talk, was hacked in 2015 [6][8].

Rest of the paper organized such that, first, it presents the background of the Dark Web and Deep Web. Second, paper presents about the Dark Web and Black Market. Finally, it discusses in detail the effects of Black Market activities through Dark Web on the economy of individual countries and on the world's economy as a whole.

2. Dark Web vs Deep Web

Before talking about the Dark Web and how it is used in the Black Market, it is important to make the distinction between the Deep Web and the Dark Web, as they are often merged together. The stratified structure of the internet could be illustrated by an iceberg as depicted in Figure 1. The figure 1 shows how the internet strata involves the Surface Web, the Deep Web and the Dark Web [9].

The Surface Web refers to the potion of the internet that is the most commonly used by anyone. It typically contains sites that are easily indexed and reached by the common search engines such as: Bing, Google, Fire Fox, Internet Explorer, and Edge, just to name a few [10].

The Deep Web is the biggest portion of the internet. It is not commonly accessed directly by the everyday internet user. The Deep Web contains all the digital data or information that are not readily indexed by the common search engines. Some of the information that could be found in the Deep web are specific emails, documents, files, messages and more [11].

The Dark Web is much like the Surface Web, except it's not regulated by law and it also provides anonymity and secrecy to its users. As a result of this, sites that could not be reached via the Surface Web due to regulations in different countries, could be reached in the Dark Web. The Onion Router (Tor) is what is used to navigate the Dark Web [12]. Before the Dark Web in 2004, Tor was used and created by the United States Naval Research Laboratory (USNR Lab) a means of exchanging intelligence across the net in total anonymity and secrecy. The USNR Lab was able to create complete anonymity between to users through the use multiple virtual IPs that hide the true IP address of its users [13].

It is also important to note that though the Dark Web is most often connected to illegal and criminal activities, illegal activities account for about 50% of the Dark Web [14]. In addition to the commonly known illegal and criminal activities in the Dark Web, it is also used by people running away from Government surveillance or censorship. Some of these other users include but not limited to: Freedom Fighters, Whistleblowers, Discrimination and Abuse Victims, Corporations and Governments [15].

3. THE DARK WEB AND THE BLACK MARKET

In December 2013 a Target store got hacked, stealing about 40 million credit cards and 70 million users are accounts data. Then the stolen data was being sold on black market websites [16][17]. The cybercrime growth has been helped by specialized markets that deal for free in tools of cybercrimes. The markets provide tools like exploit kits (software can create, spread, and control attacks on systems), botnets (group of computers controlled remotely by a central authority, used to send spam websites), in addition to as-a-service models [1][18]. As the Armor Threat Resistance Unit (TRU) reported, U.S credit card numbers could sell for $7, and other types of data can be profitable as well [19]. Social media accounts, sites that store credit/debit cards info (Amazon), video games online services (PS Plus) can be used as products for cybercriminals to sell in the underground markets [3] [20].

Figure 1: Iceberg to illustrate the strata the make up the interne [9]

The cyber underground is just a market like any other regular market. It is controlled by the power of supply and demand. Customer services are available in the cyber underground, helping customers to get their product, and making sure that their customers are happy with their services [21][22]. The black market offers different products. However, the most profitable items are social media credentials, reward points, and fake ID's and passports. Prices vary depending on the item you want or the purpose you need the item for. Fake documents can range between US $10 and US $2000 [23]. Few data, such as date of birth and address, can be used to create all types

of fake documents. Green cards, insurance, passports, driver's licenses, and even social security number are the most searched for in the black market [24]. Such documents can be the base for creating a new life for wanted people maybe [6].

Hotel and airline reward points range between $34.99 to $198.88. These stolen points and make it easier to hide someone's travel plan. The stolen rewards point should be used by legitimate customers, who spent money to get discounts. However, the black market is selling these points for cheaper prices than a one-night hotel reservation or average flight ticket [6]. Buyers are paying for travel and hotel packages; therefore, cybercriminals are stealing and selling the requested information. Prices may vary depending on the airline, country, and the amount of rewards points [25].

Many accounts are being compromised by credential-stealing malware or phishing attacks, where victims are tricked to enter their usernames and passwords. Attacks can have several stages, starting with drive by downloading malware, aiming at a specified victim or company [17][26]. Once an account is compromised, attackers can analyze and monitor the account to identify the importance of the data. When they find an account that is not used often or has useful data, the account becomes the number one target for an account takeover (ATO). The attackers then will immediately change the communication details associated with the wanted account, so the owner has no chance to receive any notification about the attackers' action. At this point, attackers can use the stolen account to make other attacks toward other accounts. One type of account takeover, is the Business Email compromise (BEC) scams, is where attackers access business used accounts using malware or phishing. The attackers will use the account to request payments or wire transfers to bank accounts they control [6][27].

The black market offers ransomware service, just like any other legal software people can get from programmers. The dark web market provides updates, technical support, and access to C&C servers, as well as payment plans for buyers' subscription. A good example of ransomware packages would be Ranion. Ranion offers different payment model based on monthly or annual subscriptions. They charge $120 for monthly subscriptions and $900 for one-year access, which can reach $1900 if the buyer wishes to add more features. Cybercriminals use another way to sell their ransomware with offering the malware and C&C infrastructure for free, but they take a cut of any payment received from victims [4][28]

There are different services provided by the black-market offering access to servers around the global, using remote desktop protocol (RDP). The prices of these services vary between $8 and $15 per server, and the buyer can search by country, by operating system, or by which payment sites users visited using that server. After having such access, a cybercriminal could use it to launch ransomware or install a malware. Some

cybercriminals who develop botnets, or networks of compromised computer, give their computing power for rent. For instance, a denial of service attacks prices vary according to how long an attack would last. Also, there are young teens and adults who offer to rent their small botnets. These botnets are mostly used to attack servers used by online games. These cybercriminals promote themselves using social networks and they are not concerned about being anonymous [4] [29]

Usually cybercriminals do not risk it with using successfully stolen PayPal or credit card accounts by themselves. Instead, they sell it to other cybercriminals because it is safer for them and more profitable. Cybercriminals usually charge around %10 of the total balance available in the stolen account. We can understand that cybercriminals, who are hidden by their tools, have built together a big criminal and profitable industry. That industry which provides customer services, updates, and user manual is now comparable with any other legal industry [4][30]. "The malware industry has stopped being disruptive and now has characteristics similar to those of a software company" said Tony Anscombe the ESET's Global Security Evangelist. Figure 2 (Bank accounts being sold) shows an example of accounts being sold after stealing them [31][32].

RAND researchers have done more than 12 interviews with cybersecurity experts, including academics and security researchers [1]. The research focused on the characteristics of the black markets considering botnets and their role in the cyber underground. The research stated that, the "Dark Net" will stay active with even more participants, higher usage of crypto currencies (Bitcoin), and higher ability of anonymity in malware [1][33]. In addition, the research predicted that the technology of cyber-attacks would advance faster than the defending technologies. Therefore, more actions should be taken to improve privacy policies and defending technologies [17][34].

Internal UID	Balance	Account type	Card	Country	Our Price	Add to cart
BGKGQFTL	2.023 USD	Premier	Yes (confirmed)	United States	$ 212	LOCKED
KUYATDLH	684 USD	Premier	Yes (confirmed)	United States	$ 78	LOCKED
QTEKVNUB	2.028 EUR	Personal	Yes (confirmed)	Italy	$ 253	Buy this!
HFQZEKOF	1.816 USD	Personal	No confirmed card	United States	$ 181	Buy this!

Figure 2: An example of accounts being sold after being stolen [31]

4. BLACK MARKET AGAINST THE ECONOMY

To understand the impacts the Black Market has on the economy of a country, it is important to first know how it is related to a country's economy. The way used to assess the impact of the black market in a country's economy is through the country's Gross Domestic Product (GDP) [35]. However, it is hard to find a country that calculates their GDP while factoring in the black market in their country. Part of the problem is, no real study has been done on the black-market as a whole, mainly due to its shadowy aspect and that it is not being reported as it is the case in the normal market. As a result of the black market's activities not being reported it is hard to estimate the actual impact it has on a country's economy. The use of the Dark Web and bit coins to carry out transactions, makes it even harder to trace transactions. Nevertheless, most of the assessments collected here are from assessment done on the part of the black market that is partially or completely out of the Dark Web. With this assessment, though estimates, will provide an idea of how the entire black market, including the portion in the Dark Web, could impact the economy of a country.

In the late 1990s, during the former Soviet Union, the black market was estimated to account for 64% of Georgia's GDP [36]. It would be interesting to know what the percentages are today. However, with the lack of sufficient studies in the domain, it is hard to get a proper estimate, especially with the Dark Web being involved. Based on an indirect study conducted by the Institute for Applied Economic Research at the University of Tübingen in Germany (IAW), the following chart in Figure 5(Country's with shadow economies) was obtained. The chart shows the percentage the black market contributes to a country's GDP. Based on estimates from Economic Analysts, the black market could account for 10% of a developed country's economy and a third of a developing country. Similar studies carried out in 2011 stipulate that, if the black market was appropriately taxed in the United States, it would have brought $400 billion to $500 billion to the country's economy [37]. According to a study carried out by Havoscope researching company around 2012, the revenue of the global black market is estimated at $1.8 trillion. The estimate includes 50 sectors of the black market not including trafficking of cultural artifacts. The studies also broke down the estimates by country as follows: United States is the biggest with $626 billion; China is next with $261 billion; Mexico with $126 billion; Spain with $124 billion; Italy with $111 billion; and Japan with $108 billion. Canada, India, United Kingdom, and Russia have less than $100 billion each of estimated black-market revenue [38]. Similar studies carried out by Global Financial Integrity, the revenue made by the top ten sectors in the Black market in 2012 were estimated as follows [39]:

1. **Counterfeiting: $1.13 trillion.**
2. **Drug Trafficking: $652 billion.**

3. **Illegal Logging: $157 billion.**
4. **Illegal Mining: $48 billion.**
5. **Illegal Fishing: $36.4 billion.**
6. **Illegal Wildlife Trade: $23 billion.**
7. **Crude Oil Theft: $11.9 billion.**
8. **Light Weapons Trafficking: $3.5 billion.**
9. **Organ Trafficking: $1.7 billion.**
10. **Trafficking in Cultural Property: $1.6 billion.**

Which all amounts to an estimated total of 2.2 trillion when human trafficking is added to it. As mentioned earlier, the Government loses a lot of tax money to the black market. According to the International Monetary Fund (IMF), United State's GDP could increase by 14% to 15% when adding the black market to the GDP calculation. These percentages jump to 35% or even 44% in emerging countries.

In spite these numbers, and the government of certain countries trying to fight back against the black market, these same governments are the once promoting the black market. With stringent rules and policies implemented in certain countries such as in Greece and the chaotic economic and political systems in other countries such as in Venezuela, the black market has been a means for people I these countries to obtain the goods and services they need or even legitimate business owners to still survive or even flourish, all through the dark web.

The black market does not benefit a community or country directly. As the black market fills the pockets of its business men and women, it increases the purchase power of the latter in addition to giving them an employment. As the purchase power increases for these black-market traders, they become able to purchase thigs much more easily in the real market, where they have to pay taxes and fees. Through this taxes and fees in the real market the communities benefit from this, which in turn benefits the country.

Especially after the Silk Road co-founder Ross Ulbricht was caught and sentenced to life imprisonment, many law enforcement and intelligence agencies have intensified their watch on the Dark Web [40]. As a result of this intensive monitoring, traders in the Dark web have only gotten more ingenious in their ways of carrying out their business(es) in that environment. This has equally made research on the black market and the Dark Web much harder. For some Black Market Entrepreneurs, they look at their business, whether in the Dark Web or not, as a means to put their children to school, feed their family, or even helping their community by employing others and through the provision of some of the basic needs of the people in their community [41].

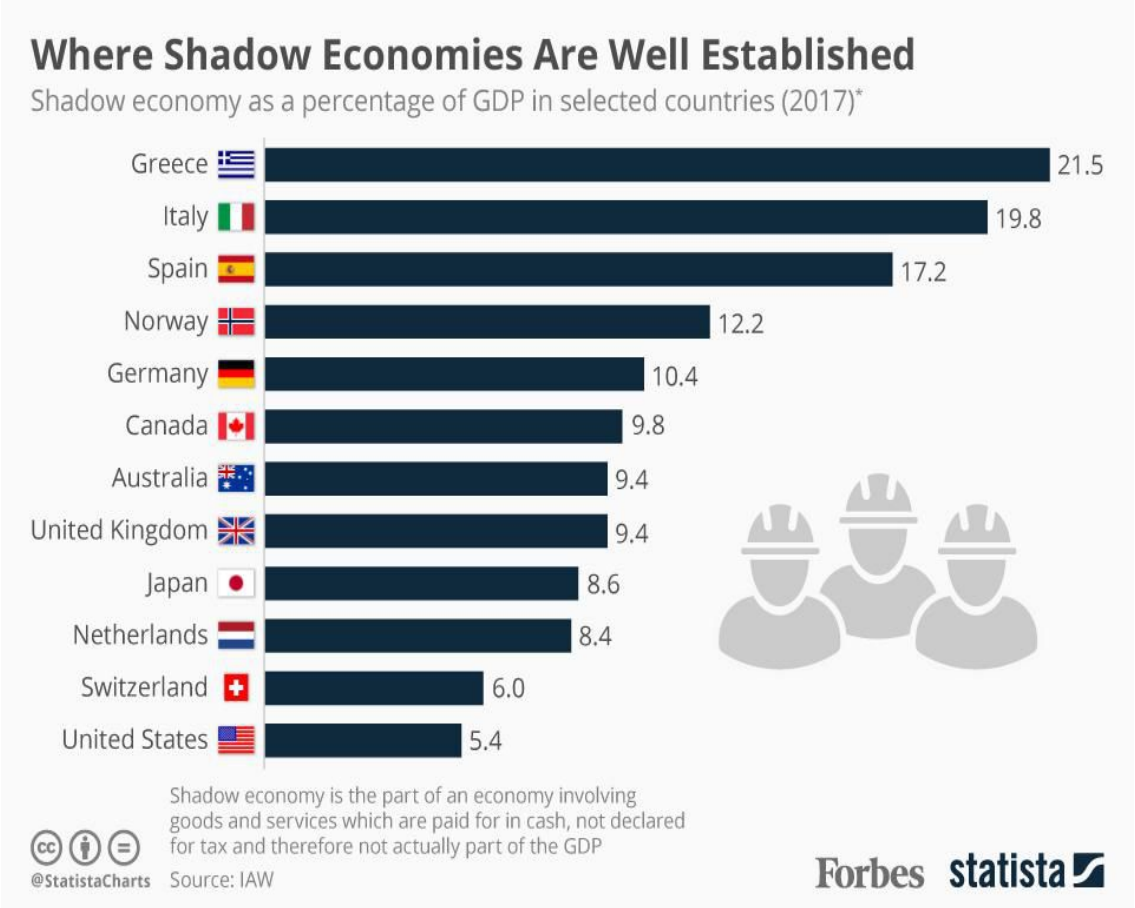

Figure 3: Picture depicting GDP of Countries with Their Shadow Economy

5. CONCLUSION

In order to restrict some black market activities via dark web, it is very important to harden all the web based software systems such as data analytic frameworks [42]. People who work within the black market are affecting societies financially. They are making a lot of money but causing more damages. The black market is running as any other usual market. Customer services, user manual, and different services are offered. Governments around the global need to take actions against the cyber underground. The hacking and stealing industry must be destroyed, in order to protect people's privacy. The advent of the Dark Web and bitcoin has brought the black market into the digital world. With both the Dark Web and the bitcoin, the black market can thrive globally in almost complete anonymity of its actors and traceability of their financial transactions.

REFERENCES

[1] L. Ablon, 25 March 2014. [Online]. Available: https://www.rand.org/news/press/2014/03/25.html.

[2] Akintaro, Mojolaoluwa, Teddy Pare, and Akalanka Mailewa Dissanayaka. "DARKNET AND BLACK MARKET ACTIVITIES AGAINST THE CYBERSECURITY: A SURVEY." In The Midwest Instruction and Computing Symposium. (MICS), North Dakota State University, Fargo, ND, April 5-6 2019.

[3] C. Milligan, 16 August 2018. [Online]. Available: https://www.armor.com/blog/cyber-black-market-hackers-want/.

[4] M. Porolli, 31 Jan 2019. [Online]. Available: https://www.welivesecurity.com/2019/01/31/cybercrime-black-markets-dark-web-services-and-prices/.

[5] [17] Simkhada, Emerald, Elisha Shrestha, Sujan Pandit, Upasana Sherchand, and Akalanka Mailewa Dissanayaka. "SECURITY THREATS/ATTACKS VIA BOTNETS AND BOTNET DETECTION & PREVENTION TECHNIQUES IN COMPUTER NETWORKS: A REVIEW, In The Midwest Instruction and Computing Symposium. (MICS), North Dakota State University, Fargo, ND, April 5-6 2019.

[6] V. Wang and E. Joseph, "The Dark Web Bad for business Research into the planning and monetisation of fraud and cybercrime against organisations on the Dark Web," 2017. [Online]. Available: https://doi.org/10.13140/RG.2.2.17198.36164. [Accessed 20 Sep 2019].

[7] Yang, Ying, Lina Yang, Meihong Yang, Huanhuan Yu, Guichun Zhu, Zhenya Chen, and Lijuan Chen. "Dark web forum correlation analysis research." In 2019 IEEE 8th Joint International Information Technology and Artificial Intelligence Conference (ITAIC), pp. 1216-1220. IEEE, 2019.

[8] Page, Joanna, Madison Kaur, and Emma Waters. "Directors' liability survey: Cyber attacks and data loss—a growing concern." Journal of Data Protection & Privacy 1, no. 2 (2017): 173-182.

[9] Lederman, Abe. "Google Just Gets to the Tip of the Iceberg: How to Get to the Gems in the Deep Web." Refer 32, no. 2 (2016): 16.

[10] Hardy, Robert Augustus, and Julia R. Norgaard. "Reputation in the Internet black market: an empirical and theoretical analysis of the Deep Web." Journal of Institutional Economics 12, no. 3 (2016): 515-539.

[11] Minnaar, Anthony. "Online'underground'marketplaces for illicit drugs: the prototype case of the dark web website'Silk Road." Acta Criminologica: Southern African Journal of Criminology 30, no. 1 (2017): 23-47.

[12] Sejfuli-Ramadani, Nexhibe, Florim Idrizi, and Florinda Imeri. "THE INFLUENCE OF THE DARK WEB." Journal of Natural Sciences and Mathematics of UT 4, no. 7-8 (2019): 95-98.

[13] Sharma, Shweta, Parvesh Sharma, and Gyanendra Singh. "Dark Web and Trading of Illegal Drugs." J Forensic Science & Criminal Investigation 9, no. 4 (2018): 555766.

[14] "How the Dark Web Impacts Business," IT Solution, 2019. [Online]. Available: https://www.itsolutions-inc.com/news-and-training/article/how-the-dark-web-impacts-business/. [Accessed 20 Sep 20].

[15] M. Lewis, "What Is the Dark Web – Who Uses It, Dangers & Precautions to Take," Money Crashers, 2017. [Online]. Available: https://www.moneycrashers.com/dark-web/. [Accessed 20 Sep 2019].

[16] Pigni, Federico, Marcin Bartosiak, Gabriele Piccoli, and Blake Ives. "Targeting Target with a 100 million dollar data breach." Journal of Information Technology Teaching Cases 8, no. 1 (2018): 9-23.

[17] Akalanka Mailewa Dissanayaka, Roshan Ramprasad Shetty, Samip Kothari, Susan Mengel, Lisa Gittner, and Ravi Vadapalli. 2017. A Review of MongoDB and Singularity Container Security in regards to HIPAA Regulations. In Companion Proceedings of the10th International Conference on Utility and Cloud Computing (UCC '17 Companion). ACM, New York, NY, USA, 91-97.

[18] Mailewa, Akalanka and Jayantha Herath. “Operating Systems Learning Environment with VMware." In The Midwest Instruction and Computing Symposium. (MICS), Verona, WI, April 25-26 2014.

[19] Romanosky, Sasha. "Examining the costs and causes of cyber incidents." Journal of Cybersecurity 2, no. 2 (2016): 121-135.

[20] Portnoff, Rebecca S., Sadia Afroz, Greg Durrett, Jonathan K. Kummerfeld, Taylor Berg-Kirkpatrick, Damon McCoy, Kirill Levchenko, and Vern Paxson. "Tools for automated analysis of cybercriminal markets." In Proceedings of the 26th International Conference on World Wide Web, pp. 657-666. 2017.

[21] Huang, Keman, Michael Siegel, and Stuart Madnick. "Systematically understanding the cyber attack business: A survey." ACM Computing Surveys (CSUR) 51, no. 4 (2018): 1-36.

[22] Mailewa, Akalanka, Jayantha Herath, and Susantha Herath. "A Survey of Effective and Efficient Software Testing." In The Midwest Instruction and Computing Symposium. (MICS), Grand Forks, ND, April 10-11 2015.

[23] Evangelista, Andrea, L. Allodi, and M. Cremonini. "Darknet Markets: Competitive Strategies in the Underground of Illicit Goods." Eindhoven University of Technology 13 (2018): 14.

[24] Hong, Sunghyuck. "Survey on Analysis and Countermeasure for Hacking Attacks to Cryptocurrency Exchange." Journal of the Korea Convergence Society 10, no. 10 (2019): 1-6.

[25] Park, Andrew J., Richard Frank, Alexander Mikhaylov, and Myf Thomson. "Hackers Hedging Bets: A Cross-Community Analysis of Three Online Hacking Forums." In 2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), pp. 798-805. IEEE, 2018.

[26] Roshan Ramprasad Shetty, Akalanka Mailewa Dissanayaka, Susan Mengel, Lisa Gittner, Ravi Vadapalli, and Hafiz Khan. 2017. Secure NoSQL Based Medical Data Processing and Retrieval: The Exposome Project. In Companion Proceedings of the10th International Conference on Utility and Cloud Computing (UCC '17 Companion). ACM, New York, NY, USA, 99-105.

[27] Hasegawa, Ayako Akiyama, Takuya Watanabe, Eitaro Shioji, and Mitsuaki Akiyama. "I know what you did last login: inconsistent messages tell existence of a target's account to insiders." In Proceedings of the 35th Annual Computer Security Applications Conference, pp. 732-746. 2019.

[28] Kamat, Pooja, and Apurv Singh Gautam. "Recent trends in the era of cybercrime and the measures to control them." In Handbook of e-business security, pp. 243-258. Auerbach Publications, 2018.

[29] Paquet-Clouston, Masarah, Bernhard Haslhofer, and Benoit Dupont. "Ransomware payments in the bitcoin ecosystem." Journal of Cybersecurity 5, no. 1 (2019): tyz003.

[30] Shanmugam, Bharanidharan, Sami Azam, Kheng Cher Yeo, Jithin Jose, and Krishnan Kannoorpatti. "A critical review of Bitcoins usage by cybercriminals." In 2017 International Conference on Computer Communication and Informatics (ICCCI), pp. 1-7. IEEE, 2017.

[31] Akalanka Mailewa Dissanayaka, Susan Mengel, Lisa Gittner, and Hafiz Khan. Dynamic & portable vulnerability assessment testbed with Linux containers to ensure the security of MongoDB in Singularity LXCs. In Companion Conference of the Supercomputing-2018 (SC18).

[32] Buhalis, Dimitrios, Tracy Harwood, Vanja Bogicevic, Giampaolo Viglia, Srikanth Beldona, and Charles Hofacker. "Technological disruptions in services: lessons from tourism and hospitality." Journal of Service Management (2019).

[33] Kethineni, Sesha, Ying Cao, and Cassandra Dodge. "Use of bitcoin in darknet markets: Examining facilitative factors on bitcoin-related crimes." American Journal of Criminal Justice 43, no. 2 (2018): 141-157.

[34] Song, Wenjie, and Hao Li. "Research on Android Application Security Protection in China." DEStech Transactions on Computer Science and Engineering csae (2017).

[35] Cai, Junning, Hui Huang, and PingSun Leung. "Understanding and measuring the contribution of aquaculture and fisheries to gross domestic product (GDP)." FAO Fisheries and Aquaculture Technical Paper 606 (2019): I-69.

[36] N. McCarthy, "The Countries With The Largest Shadow Economies [Infographic]," 9 Feb 2017. [Online]. Available: https://www.forbes.com/sites/niallmccarthy/2017/02/09/where-the-worlds-shadow-economies-are-firmly-established-infographic/#a35af0e742cc. [Accessed 20 Sep 2019].

[37] A. Bloomenthal, "How the Underground Economy Affects GDP," 29 Jul 2019. [Online]. Available: https://www.investopedia.com/articles/markets-economy/062216/how-underground-economy-affects-gdp.asp. [Accessed 20 Sep 2019].

[38] Jang, Jae Im, and Ho Jung Choo. "Consumption of Counterfeit Luxury Fashion Products Based on the Theory of Planned Behavior." Journal of the Korean Society of Clothing and Textiles 39, no. 3 (2015): 433-445.

[39] Kar, Dev, and Joseph Spanjers. Illicit financial flows from developing countries: 2003-2012. Vol. 20. Washington, DC: Global Financial Integrity, 2014.

[40] Trautman, Lawrence J. "Virtual currencies; Bitcoin & what now after Liberty Reserve, Silk Road, and Mt. Gox?." Richmond Journal of Law and Technology 20, no. 4 (2014).

[41] R. Capps, "Why Black Market Entrepreneurs Matter to the World Economy," 16 Dec 2011. [Online]. Available: https://www.wired.com/2011/12/mf-neuwirth-qa/. [Accessed 20 Sep 2019].

[42] Akalanka Mailewa Dissanayaka, Susan Mengel, Lisa Gittner, and Hafiz Khan. Vulnerability Prioritization, Root Cause Analysis, and Mitigation of Secure Data Analytic Framework Implemented with MongoDB on Singularity Linux Containers. In The 4th International Conference on Compute and Data Analysis -2020 (ICCDA-2020). San Jose, CA.