Digital Forensics: Crimes and Challenges in Online Social Networks Forensics

Bandr Fakiha

Umm Al Qura University, Al Qunfudah, Saudi Arabia

bfageeha@hotmail.com

Abstract

The growth in online social networks (OSNs) has opened up communication and interaction between people and businesses across the globe. This open communication has improved international trade, but it has simultaneously created a channel for perpetrating cybercrimes such as cyberbullying and harassment, cyberstalking, slander spreading, copyright infringement and identity theft, and cyber-extremism. Despite the many cybercrimes on OSNs, challenges exist in investigating and prosecuting criminals behind these crimes. The perpetrators of these crimes use sophisticated anti-forensic techniques, legal challenges, and resource-based challenges to prevent prosecution. They limit forensic investigations making it challenging to obtain a conviction. The challenges in conducting OSNs forensics point to a grey area regarding combating crime and the online safety of global citizens. This article examines the different cybercrimes on OSNs and the challenges encountered in conducting digital forensics on OSNs. It forms a basis for motivating consistent and unified support across the globe to combat cybercrimes committed through OSNs.

***Keywords**: Anti-forensic Techniques, Cybercrimes, Online Social Networks, Digital Forensics*

1. Introduction

In this paper, the researcher investigates the current state of the open social networks[1] (OSN) and their impact on the lives of the individuals in specific and society in general. The researcher also discusses the misuse of OSNs in committing cybercrimes ranging from financial crimes cyber bullying, and spreading of fake news, to the recruitment of extremists. In addition, the researcher investigates the period that cybercriminals will take to protect their identities and then makes recommendations for effectively litigating cybercrime cases, where the offense is committed through OSNs.

Figure 1: Penetration of digital around the world (Kemp, 2019).

Figure 1 shows the global penetration of digital around the world (Kemp, 2019). The 2019 Global Social Media Research Summary by Smart Insights confirms the data presented by (Kemp, 2019) that global social media penetration is 45% of the total world's population (3.484 billion people). The 3.484 billion users represent the 9% growth in the number of users since last year. This growth is a clear indicator of the persistent growth in the use of online social networks (OSNs) since their inception a decade ago.

[1] IGI Global (https://www.igi-global.com/dictionary/constructing-community-higher-education-regardless/21064) defines a online social network as "An online service or site to facilitate social interaction to help individuals find others of a common interest, establish a forum for discussion, and exchange information."

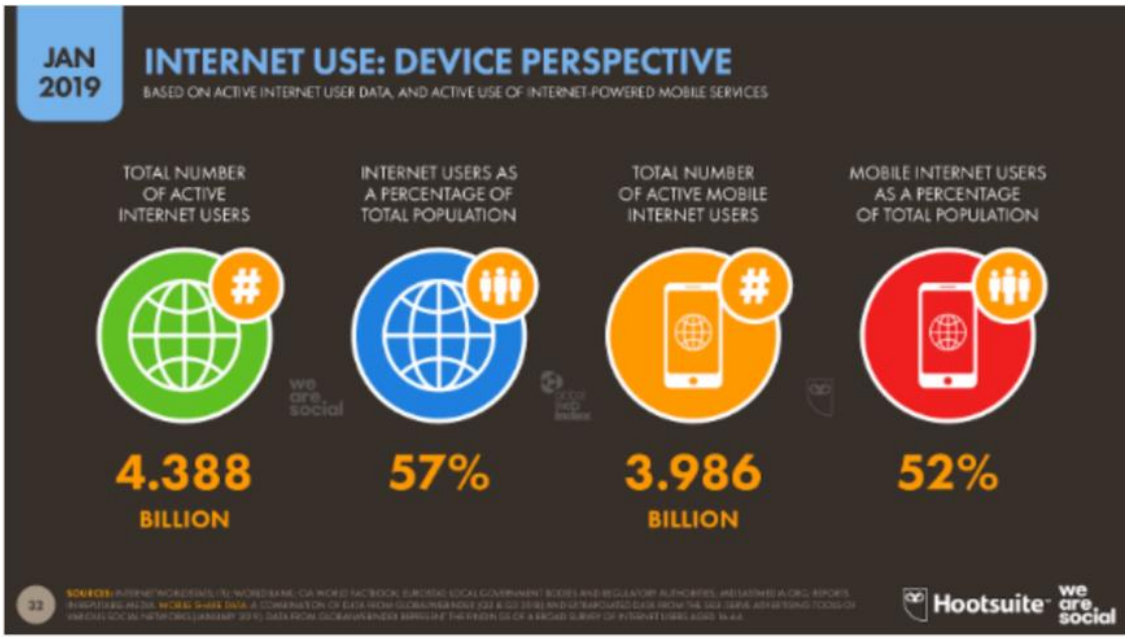

Figure 2: Internet use by device(Kemp, 2019).

Figure 2 shows internet use by a device (Kemp, 2019). It is noted that more than half of internet users are accessing the internet using a mobile device.

The core of this paper's interest is OSNs for their extensive usage and influence. Thus, Figure 3 shows the ranking of the most popular OSNs (Kemp, 2019). More specifically, as of April 2019, Facebook has been ranked as the most popular OSNs with 2.3 billion users , followed by YouTube and WhatsApp with 1.9 and 1.6 billion users, respectively (Statista, 2019). This superiority of OSNs is attributed to their fulfillment of the users' needs like entertainment and fun, networking with people from different cultures across the world, information discovery and obtaining real-time news, self-expression, and opening up business opportunities (Myhre, Mehl, &Glisky, 2017; Zheng, Cheung, Lee, & Liang, 2015).

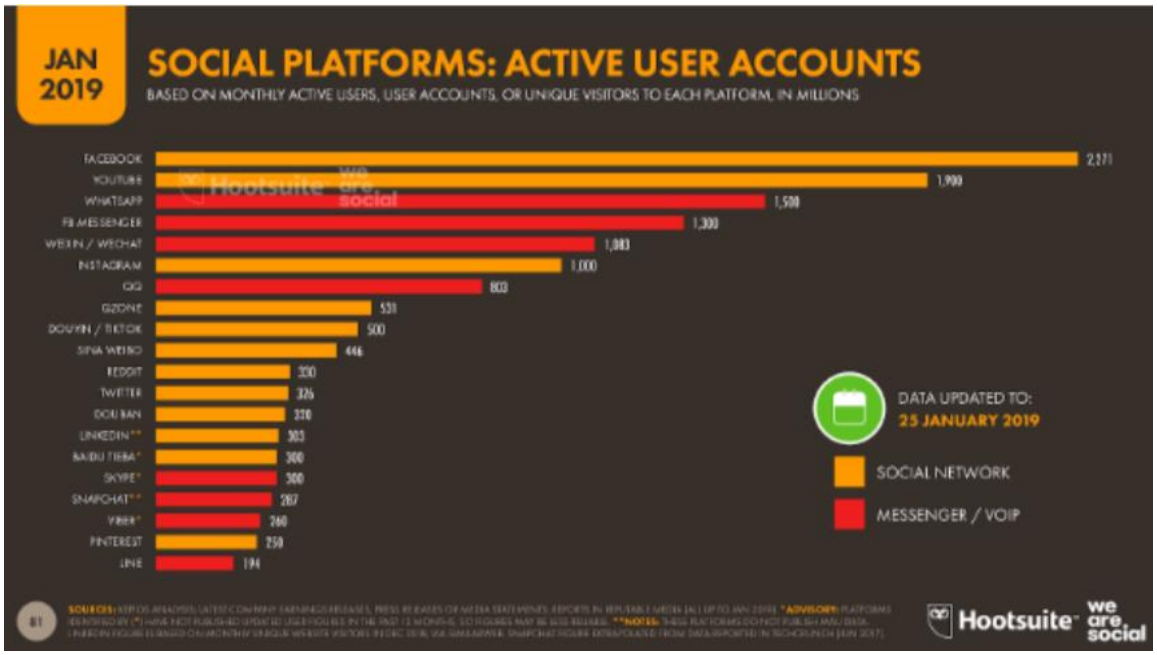

Figure 3: The number of active users by OSN(Kemp, 2019).

However, despite these great benefits to people and businesses, the OSNs are targeted by cybercrimes[2], thus posing considerable threats to the users and the global populace at large (Awan, 2017; Yusoff, Dehghantanha, &Mahmod, 2017). An example of the impact of cybercrime on a country is the UK, where cybercrime accounts for more than 50% of all crimes that are reported (Zaharia, 2019). One of the reasons for this increase in cybercrimes is that hackers attack on average once every 39 seconds (Zaharia, 2019).

[2] Technophobia (https://www.techopedia.com/definition/2387/cybercrime) defines a cybercrime as "Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes). Cybercriminals may use computer technology to access personal information, business trade secrets or use the internet for exploitative or malicious purposes."

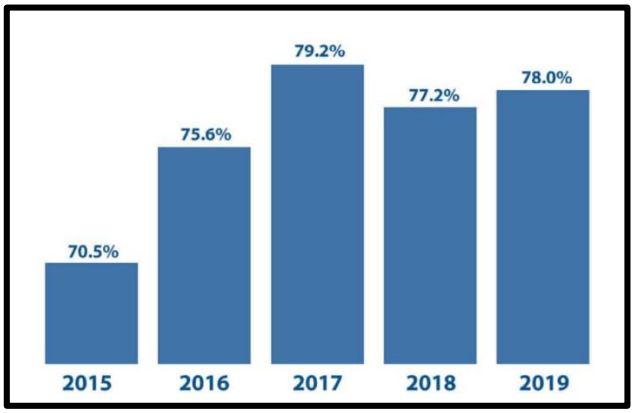

Figure 4: Frequency of successful attacks per year (Zaharia, 2019).

In this article, the researcher is interested in the link between the growth of OSNs and the increase in cybercrimes (Zaharia, 2019).

Due to the advancement in technology, the criminals engaged in the cybercrimes are devising mechanisms to hide their criminal activities. They are also developing ways of distracting or blocking forensic investigators from obtaining the critical information needed to complete investigations (Lillis, Becker, O'Sullivan, & Scanlon, 2016). The challenges facing digital forensic[3] experts (DFEs) are providing reliable evidence to indict the culprits or spotting crimes before they occur. This article examines the different cybercrimes on OSNs and the challenges encountered in conducting digital forensics on OSNs as a basis for rallying for consistent and unified support across the globe to combat the crimes perpetrated on OSNs.

2. The rationale for the study

The rationale for this study comes from the fact that Saudi Arabia has the second highest percentage of cyber attacks in the world (91.5%), after Spain (93.7%) (Zaharia, 2019). In addition to the number of cyber attacks experienced by Saudi Arabia, the country also experienced the highest number of ransomware attacks in the world in 2019 (Zaharia, 2019). The statistics mentioned above are shown in Figures 5 and 6 below.

[3] Technophobia (https://www.techopedia.com/definition/27805/digital-forensicsdefinesdefines digital forensics as "Digital forensics is the process of uncovering and interpreting electronic data. The goal of the process is to preserve any evidence in its most original form while performing a structured investigation by collecting, identifying and validating the digital information for the purpose of reconstructing past events.."

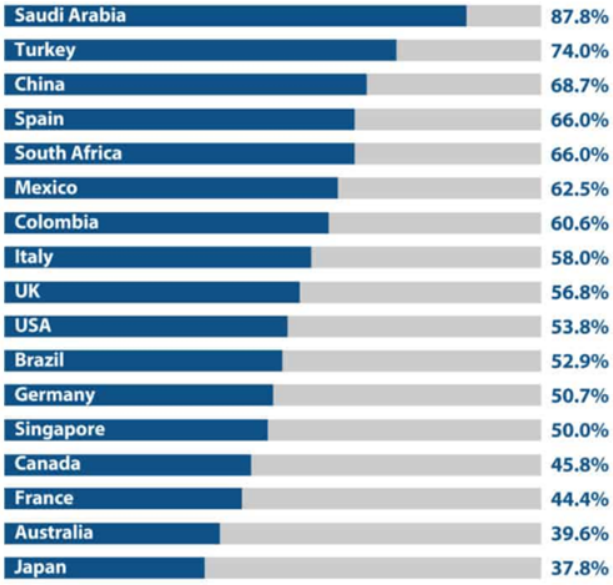

Figure 5: A graph showing the percentage of ransomware attacks by country (Zaharia, 2019).

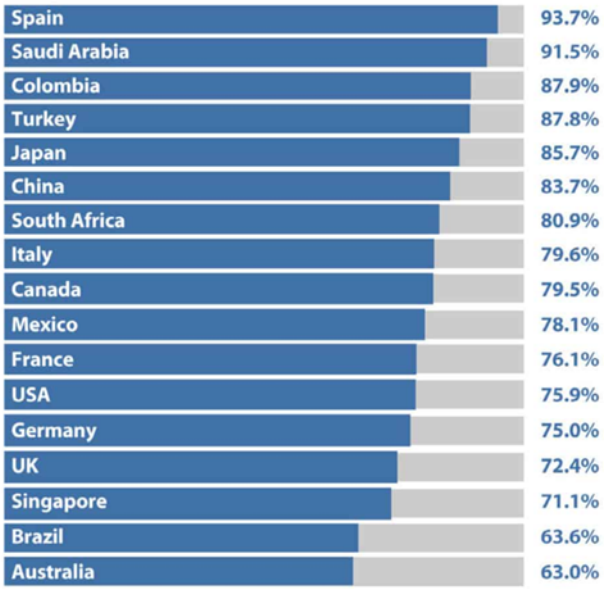

Figure 6: A graph showing the percentage of ransomware per country (Zaharia, 2019).

Increasingly, OSNs are being used to attract users to web pages, where malicious software can be downloaded (Javed, Burnap, & Rana, 2019). The investigation and prosecution of criminals, who make use of OSNs to deliver ransomware, cyber attacks and other digital criminal activities are the primary motivation for the research.

Cybercrimes perpetrated through OSNs do not only have financial ramifications; some have a very personal agenda like cyberbullying[4] and harassment, cyberstalking[5], slander, copyright infringement, identity theft, and cyber-extremism.

Cyberbullying and harassment are usually perpetrated through aggressive, demeaning comments or messages on OSNs. According to Whittaker & Kowalski (2014), cyberbullying has the highest negative impact when committed by peers. Peers usually understand their intended victim's weaknesses and use these weaknesses as a tool to damage their character.

Over the years, cyberbullying has been associated with suicidal behaviors (Luxton, June, &Fairall, 2012), which makes it a criminal offense.

[4] Technophobia (https://www.techopedia.com/definition/2389/cyberbullying) defines cyberbullying as "…a practice where an individual or group uses the Internet to ridicule, harass or harm another person. The social and emotional harm inflicted by cyberbullies grows out of - or leads to - physical bullying in the offline world."

[5]Techtarget (https://searchsecurity.techtarget.com/definition/cyberstalking) defines cyberstalking as "Cyberstalking is a crime in which the attacker harasses a victim using electronic communication, such as e-mail or instant messaging (IM), or messages posted to a Web site or a discussion group. A cyberstalker relies upon the anonymity afforded by the Internet to allow them to stalk their victim without being detected."

OSNs facilitate the stalking of people due to the easy access to personal information. The catalyst to the stalking may arise out of delusions created by the perpetrator through the use of social media or in instances of jilted love relationships. Stalkers often tend to exhibit psychotic behaviors, which makes it a psychiatric need (Krishna, et al., 2013). In extreme cases, cyberstalking has been involved with criminal acts such as violence and murder.

Due to the ease in communication, OSNs are accessible vehicles to spread false information. In such instances, the goal is usually to destroy the image and reputation of the victim, and in other cases, to spread propaganda and fear amongst the targeted recipients. It is usually a tedious process verifying the information across all the OSNs to ensure that hoaxes and fake news are not spread (Kumar & Shah, 2018). While the information may be retracted, it may be impossible to reclaim the previous position after the damage.

The ease of use of the OSNs has also enabled copyright infringement across brands and identity theft among individuals. Identity theft occurs when criminals take on the identity of another by replicating their information. On some social media accounts, there is no verification required to authenticate identity (Steel, 2010). Further, users of OSNs can post copyrighted content and claim it as theirs . Thus, it becomes easy for criminals to execute crime using fake accounts containing false information (Tsikerdekis&Zeadally, 2014). This is known as spoofing. Spoofing exposes the real owners of the content to criminal investigations and legal repercussions if their innocence is not proven on time.

Cyber-extremism occurs when OSNs are used by extremist groups to gain support for their activities. Some of the known culprits include militia groups and groups that make use of dark networks such as drug syndicates and human traffickers. The militia groups post videos or images they know will further their agenda. Militia groups and extremists enhance their reputations by taking responsibility for terrorist attacks. Extremists also post alluring messages portraying ‘cool’ images of themselves, such as holding guns to attract unsuspecting targets into their groups (Awan, 2017). For drug dealing and human trafficking, OSNs serve as planning and recruitment grounds (Bright, Hughes, & Chalmers, 2012; Latonero, 2011).

Using OSNs makes it easy to target young, vulnerable youth who are attracted to the messages being portrayed by criminals.

Very little information exists on the successful litigation against cybercriminals, who have used OSNs. The purpose of this paper is to propose policy and training that need to be put in place to ensure the successful forensic investigation of cybercrimes committed using OSNs.

3. Methodology

Cybercrimes differ from the traditional crimes in that there is no physical involvement in the former. Their execution speed is quite fast and may target any location across the world where internet connectivity exists.

In this paper, we make use of a secondary research methodology to obtain quantitative and qualitative data on OSNs and their use in cybercrimes. Secondary research data is based on data that has been published by other researchers, scientific organizations, and, in our case, consulting companies (Stewart & Kamins, 1993). The research data that has been published fits the needs of our research, so we do not have to engage in any primary research activity to collect new data. Hox and Boeije (2005) discuss the drawbacks of using secondary data in research. One of the biggest concerns they raise is that primary data is obtained to answer a specific question. This question may not be related in any way to the question being asked by secondary users of this data. The concerns raised by Hox and Boeije (2005) do not apply here as the data we are using is specific to cybercrimes and OSNs. Glass (1976) discusses the role played by secondary research in obtaining essential findings that have occurred in education when secondary data is used correctly.

The data used in this paper involved an assessment of online scholarly articles on digital forensics, specifically online social networks forensics. The scholarly articles were obtained from journal hubs such as Science Hub Publishing (Sci-Hub), Emerald, Science Direct (Elsevier), Research Gate, Emerald Insight, and Springer. Key terms and their combinations were used to select journals such as digital forensics, online social network forensics, cybercrimes, cybersecurity, digital forensic experts, digital forensic tools, and digital forensic models. The relevant articles based on the search criteria were used in developing the article.

4. Case Study

In this section, we consider the hacking of the University of Michigan's most popular Facebook pages (Sunstrum, 2019). The hack started on Wednesday, August 12, at approximately 3:30 am. The Facebook pages were defaced with malicious postings. The hack occurred through Facebook, the world's most popular OSN.

The University was able to track the security breach to a phishing scheme operating through Facebook Messenger. One of the staff members at the institution responded to an email that looked like the ones in Figure 7. This gave hackers login and password access to the University's Facebook page.

According to Facebook, the following two scripted messages reflect what the individual may have received:

Dear Nikki Sunstrum,
Data that you have filled do not match your fanpage, precisely the Security Question, and Answer do not match in your records.
Please fill the application again.
[Malicious link was here]
Sincerely,
Facebook Support Center

or

Dear Nikki Sunstrum,
Data that you have filled do not match your fanpage please fill the application again
[Malicious link was here]
Sincerely,
Facebook Support Center

Figure 7: Example of a phishing email used to extract Facebook login information(Sunstrum, 2019).

Because of the University of Michigan's swift response to the hack, the damage to the reputation of the University was minimal. New security protocols for logging in to the University's Facebook page were put in place to prevent a phishing attack like this from taking place.

School Safety

Teen Takes Own Life After Classmates Share Intimate Messages Online

Our second case study is the story of Channing Smith. Private messages of the 16-year-old were shared to Instagram and Snapchat. Channing was bullied by classmates and took his life on September 22, 2019. Channing's family found out about him being cyberbullied when they could not find any other motive for him taking his own life.

5. Results and Discussion

With new technology, new hurdles come for investigators involved in digital forensics. For OSNs, the number of platforms and users, and the volume of data generated are increasing daily. Criminals targeting OSNs to perpetrate cybercrimes are devising new techniques and methodologies to take advantage of the new platforms and increased data sizes. It is evident that, over time, old techniques become obsolete and new challenges emerge. This section addresses such challenges and the ***anti-forensic*** techniques applied by the criminals.

5.1 Anti-Forensic Techniques

Obtaining evidence from the OSNs is encumbered by technical challenges. Ant-forensic techniques are used by the criminals to hide evidence or to distract the investigation process. The processes used to hide evidence involve encryption, steganography, covert channeling, storage space data hiding, and residual data wiping.

Encryption involves encoding data to be accessible only to authorized parties, who have the decryption keys (Huber, et al., 2011). The process of decoding the encrypted files is tedious and time-consuming, and at times it is impossible and futile. Steganography is also an additional method of protecting data used together with cryptography.

In this method, the look of the file is unaltered as hidden files cannot be identified at a glance (Ning, et al., 2014).

To implement this technique, the Digital Forensic and Information Security (DFIS) of the document is known so that the hidden information can be revealed and extracted.

Covert channeling involves hiding data across the networks and also entails bypassing any forms of intrusion (Ning, et al., 2014). Since the transmitting channel is different from the main channel, it becomes difficult to suspect or identify criminal activities. In addition, data hiding in storage spaces entails hiding data from standard commands and programs in the system (Sindhu & Meshram, 2012). Hidden data causes complexity in the investigation as some of the information becomes difficult to even impossible to retrieve. Further, residual data wiping involves erasing data trails to wipe out any traces of system manipulations or the presence of an external party (Jain & Chhabra, 2014).

Trail obfuscation and attacks against the tools used in digital forensic investigations are used to obstruct the activities of the DFIs. Through trail obfuscation, the criminals use false information that misleads the DFIs during the investigation process. One way of executing the process is through defragmentation, whereby the criminals break down the evidence into parts and store it into different storage spaces (Jain & Chhabra, 2014). The DFIs are required to reorganize the files and arrange them to build a comprehensive report, which is not only time consuming but also derails the process extensively. The second technique is by modifying the metadata (Jain & Chhabra, 2014). The modifications misalign the process flow of data in the systems, thus disorienting the trail of the evidence, making it difficult to follow through an investigation due to the distractions in the process.

The criminals may also launch attacks on the tools used in the investigation process. These attacks are usually executed through denial of service (DoS) attacks such as compression bombs, zipped file bombs and regular expression DoS (Jain & Chhabra, 2014). The goal of the attacks is usually to destroy the reliability of the evidence collected or to destroy the evidence completely. For instance, when a compression bomb is launched, the intention is to tamper with the device storage such that there is no space enough to store the evidence. Other attacks may be in form of viruses and worms into the tools to corrupt the memory or the data processors (Chen S. , Xu, Nakka, Kalbarczyk, & Iyer, 2005).

5.2 Legal Challenges

Legal challenges are related to the difficulties in investigations attributed to the lack of universally accepted guidelines and standards guiding the field. Even though internet usage across the globe has increased (Zaharia, 2019), there exists no unifying legal framework for different jurisdictions. Many countries develop policies in line with their regulatory framework (Park, et al., 2018), which often tends to be different in different countries. This encourages the cybercriminals to target their crimes in jurisdictions where the legal framework is inadequate to elongate or frustrate the investigation process. The lack of cross-border collaboration also promotes cybercrimes because the conviction of the criminals across borders is a daunting task.

Another legal barrier is on the privacy rules put in place by institutions to safeguard the privacy of their users. For instance, Facebook has privacy terms that require consent from the one being investigated to collect data from them and any data relating to their account. In such an instance, given the prior notice that an investigation will be conducted, a criminal may tend to manipulate or destroy any incriminating evidence so that the investigators do not get hold of it during the investigation process. On the other hand, launching an investigation without the consent (although it provides enough room to collect evidence with minimal chances of manipulation) puts the DFIs under a breach of the privacy rights on the platform. In such an instance, the usage of the evidence could be barred in a court of law as it is not in conformity with the required adherence to rules and regulations on the investigation. Alternatively, the DFIs have to obtain a search warrant to investigate an individual (Ami-Narh & Williams, 2008). The downside of this is when obtaining the search warrants takes more time while the investigation is urgent and requiring immediate action. In such instances, the investigation will not be effective.

5.3 Resource Challenges

The technological advancement creates opportunities for improvements in cybercrimes and techniques of promulgating them and dodging investigations. For the OSNs, the volume of data open for assessments is usually massive. The DFIs are required to identify the most relevant data needed without compromising the quality of the evidence. Thus, there is a dire need for a continuous progression of the tools and mechanisms of combating cybercrimes as well as trained personnel to execute the same.

For effectiveness and efficiency, high-level computing tools and techniques need to be employed to optimize data search (Chen L. , Xu, Yuan, & Shashidhar, 2015). As digital forensics on OSNs is an emergent field, there are still significant limitations to the resources needed as new technology poses new threats.

6. Discussion

The space and provisions for the use of OSNs provide an environment for the push-and-pull of good and evil. OSNs comes with freedom of expression where there are no limitations on what one says or does online. Thus, it is harboring a generation of "free spirits" that say things at will without concerns on their repercussions to other people. This has been the main driver of cyberbullying and harassment (Whittaker & Kowalski, 2014). Besides the personal privacy settings to limit access of OSNs to certain people, one can take extensive searches on people and businesses without their knowledge. This is the main reason behind cyberstalking (Krishna, et al., 2013). Also, OSNs provide a large audience where information is disseminated at the snap of a finger. This has encouraged slander spreading as the perceived benefits are reaped almost immediately (Kumar & Shah, 2018).

Further, most social media handles are motivated by views, likes, reposts, and shares. Thus, some people and businesses opt for more straightforward mechanisms such as riding on the work of known brands to create a platform for themselves. This has promoted copyright infringement and identity theft (Steel, 2010; Tsikerdekis & Zeadally, 2014). Moreover, the OSNs provide privacy protection rights to their users that protect them from intrusion. Combined with the large audience, they have enabled cyber extremism through the actions of terror groups, drug syndicates, and human trafficking (Awan, 2017; Bright, Hughes, & Chalmers, 2012; Latonero, 2011).

Upon the occurrence of the cybercrimes, it is further becoming more challenging to obtain evidence to convict the perpetrators in courts of law. The criminals are becoming wiser by the day and are using every form of technological advancement to perfect their art in confiscating or altering evidence (Lillis, Becker, O'Sullivan, & Scanlon, 2016).The DFIs are tasked with unearthing the required evidence, which is cumbersome, time-consuming and frustrating. For instance, with progress on phone technology, the data processes are altered so that the new versions have improved data processing capacities and features. This forms a ground for discoveries on means of circumventing investigations and mechanisms for launching advanced attacks.

Also, the encryption for data stored in the devices varies for the new and the old models. This means that the knowledge needed to decrypt files in older phone models differ from that for the newer versions. For the digital forensic investigations to be successful, it is a requirement that the personnel involved be conversant with the skills and knowledge needed, which keeps changing from time to time. The tools and algorithms used also need to be updated to cater for the new challenges too. This poses a resource constraint in the field as huge investments are needed to deploy qualified DFIs and to have updated tool kits (Chen L. , Xu, Yuan, & Shashidhar, 2015).

Notwithstanding, there is no uniform legal framework that guides the global OSNs forensics due to the widespread use of the networks in jurisdictions employing differing laws (Park, et al., 2018). This gives the criminals a field day as they are at ease in launching attacks at nations where it is difficult to convict them. On the other hand, it is difficult for DFIs to conduct cross-border investigations as they will have to adhere to the laws and regulations in all the nations concerned. Even for the privacy protection for the OSNs users, in as much as the innocent are protected, the criminals are protected too from unwarranted investigations. Thus, while the law ought to protect its citizens from unscrupulous and criminal activities, it is limiting for OSNs.

7. Recommendations

- Countries need to invest in constant training for DFIs to ensure the most up to date tools are used for forensic investigations.
- The tools used to investigate cybercriminal activity need to be updated on a regular basis.
- New tools that are capable of handling the complex algorithms used by cybercriminals need to be developed.
- A legal framework for dealing with cybercrimes that arise from OSNs needs to be developed.

8. Acknowledgment

For my parents, family and University of Umm Al Qura for their support, help and assistance.

References

1. Ami-Narh, J. T., & Williams, P. A. (2008). Digital Forensics and the Legal System: A Dilemma of our Times. *Australian Digital Forensics Conference* (p. 41). ECU Publications. Retrieved from https://www.researchgate.net/publication/49280065_Digital_Forensics_and_the_Legal_System_A_Dilemma_of_our_Times

2. Awan, I. (2017). Cyber-Extremism: Isis and the Power of Social Media. *Society, 54*(2), 138-149. doi:10.1007/s12115-017-0114-0

3. Bright, D. A., Hughes, C. E., & Chalmers, J. (2012). Illuminating dark networks: a social network analysis of an Australian drug trafficking syndicate. *Crime, Law and Social Change, 57*(2), 151–176. doi:10.1007/s10611-011-9336-z

4. Chaffey, D. (2019). *Global social media research summary 2019*. Retrieved from www.smartinsights.com: https://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/

5. Chen, L., Xu, L., Yuan, X., & Shashidhar, N. (2015). Digital forensics in social networks and the cloud: Process, approaches, methods, tools, and challenges. *International Conference on Computing, Networking and Communications (ICNC)* (pp. 1132-1136). Garden Grove: IEEE. doi:10.1109/ICCNC.2015.7069509

6. Chen, S., Xu, J., Nakka, N., Kalbarczyk, Z., & Iyer, R. K. (2005). Defeating Memory Corruption Attacks via Pointer Taintedness Detection. *International Conference on Dependable Systems and Networks (DSN'05)* (pp. 378-387). Illinois: IEEE. doi:10.1109/DSN.2005.36

7. Glass, G. V. (1976, November). Primary, Secondary, and Meta-Analysis of Research. *Educational Researcher, 5*(10), 3-8. Retrieved from http://www.jstor.org/stable/1174772 .

8. Hox, J. J., & Boeije, H. R. (2005). Data Collection, Primary vs. Secondary . *Encyclopedia of Social Measurement*, 593-599.

9. Huber, M., Mulazzani, M., Leithner, M., Schrittwieser, S., Wondracek, G., & Weippl, E. (2011). Social snapshots: digital forensics for online social networks. *Proceedings of the 27th Annual Computer Security Applications Conference* (pp. 113-122). Orlando: ACM.

10. Jain, A., & Chhabra, G. S. (2014). Anti-Forensics Techniques: An Analytical Review. *Seventh International Conference on Contemporary Computing (IC3).* Noida: IEEE. doi:10.1109/IC3.2014.6897209

11. Javed, A., Burnap, P., & Rana, O. (2019, May). Prediction of drive-by download attacks on Twitter. *Information Processing & Management, 56*(3), 1133-1145. doi:https://doi.org/10.1016/j.ipm.2018.02.003

12. Kemp, S. (2019, January 2019). *Digital 2019: Global Internet Use Accelerates*. Retrieved October 30, 2019, from we are social : https://wearesocial.com/blog/2019/01/digital-2019-global-internet-use-accelerates

13. Krishna, N., Fischer, B. A., Miller, M., Register-Brown, K., Patchan, K., & Hackman, A. (2013). The role of social media networks in psychotic disorders: a case report. *General Hospital Psychiatry, 35*(5), 576.e1-576.e2. doi:10.1016/j.genhosppsych.2012.10.006

14. Kumar, S., & Shah, N. (2018). *False Information on Web and Social Media: A Survey.* Retrieved from https://arxiv.org: https://arxiv.org/abs/1804.08559

15. Latonero, M. (2011). *Human Trafficking Online: The Role of Social Networking Sites and Online Classifieds.* Los Angeles: Center on Communication Leadership & Policy. doi:10.2139/ssrn.2045851

16. Lillis, D., Becker, B. A., O'Sullivan, T., & Scanlon, M. (2016). Current challenges and future research areas for digital forensic investigation. *arXiv preprint arXiv:1604.03850*, 1-11. Retrieved from https://arxiv.org/pdf/1604.03850.pdf

17. Luxton, D. D., June, J. D., & Fairall, J. M. (2012). Social Media and Suicide: A Public Health Perspective. *American Journal of Public Health, 102*(S2), S195-S200. doi:10.2105/AJPH.2011.300608

18. Myhre, J. W., Mehl, M. R., & Glisky, E. L. (2017). Cognitive Benefits of Online Social Networking for Healthy Older Adults. *The Journals of Gerontology: Series B, 72*(5), 752–760. doi:10.1093/geronb/gbw025

19. Ning, J., Singh, I., Madhyastha, H. V., Krishnamurthy, S. V., Cao, G., & Mohapatra, P. (2014). Secret message sharing using online social media. *IEEE Conference on Communications and Network Security* (pp. 319-327). San Francisco: IEEE. doi:10.1109/CNS.2014.6997500

20. Park, S., Akatyev, N., Jang, Y., Hwang, J., Kim, D., Yu, W., . . . Kim, J. (2018). A comparative study on data protection legislations and government standards to implement Digital Forensic Readiness as mandatory requirement. *Digital Investigation, 24*(Supplement), S93-S100. doi:10.1016/j.diin.2018.01.012

21. Sindhu, K. K., & Meshram, B. B. (2012). Digital Forensics and Cyber Crime Datamining. *Journal of Information Security, 3*, 196-201. doi:10.4236/jis.2012.33024

22. Statista. (2019). *Most popular social networks worldwide as of April 2019, ranked by number of active users (in millions)*. Retrieved from www.statista.com: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

23. Steel, E. (2010, March 29). Nestlé Takes a Beating on Social-Media Sites. *The Wall Street Journal*, p. B5.

24. Stewart, D. W., & Kamins, M. A. (1993). *Secondary Research: Information sources and methods* (2nd ed.). London: SAGE Publications.

25. Sunstrum, N. (2019). *Hacked: A Case Study*. Retrieved November 1, 2019, from Michigan Social: https://socialmedia.umich.edu/blog/hacked/

26. Tsikerdekis, M., & Zeadally, S. (2014, September). *Online Deception in Social Media.* Retrieved from uknowledge.uky.edu: https://uknowledge.uky.edu/cgi/viewcontent.cgi?article=1013&context=slis_facpub

27. Whittaker, E., & Kowalski, R. M. (2014). Cyberbullying Via Social Media. *Journal of School Violence, 14*(1), 11-29. doi:10.1080/15388220.2014.949377

28. Yusoff, M. N., Dehghantanha, A., & Mahmod, R. (2017). Forensic Investigation of Social Media and Instant Messaging Services in Firefox OS: Facebook, Twitter, Google+, Telegram, OpenWapp and Line as Case Studies. *Contemporary Digital Forensic Investigations of Cloud And Mobile Applications*, 41-62. Retrieved from https://arxiv.org/ftp/arxiv/papers/1706/1706.08062.pdf

29. Zaharia, A. (2019, May 13). *300+ Terrifying Cybercrime and Cybersecurity Statistics & Trends [2019 EDITION]*. Retrieved October 30, 2019, from Comparitech: https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/

30. Zheng, X., Cheung, C. M., Lee, M. K., & Liang, L. (2015). Building brand loyalty through user engagement in online brand communities in social networking sites. *Information Technology & People, 28*(1), 90-106. doi:10.1108/ITP-08-2013-0144

الطب الشرعي الرقمي: الجرائم والتحديات في الطب الشرعي للشبكات الاجتماعية عبر الإنترنت

بندر فقيها

قسم الخدمات الطبية الطارئة، كلية العلوم الصحية بالقنفذة، جامعة أم القرى– المملكة العربية السعودية

bfageeha@hotmail.com

الملخص

أدى النمو في الشبكات الاجتماعية عبر الإنترنت (OSN) إلى فتح التواصل والتفاعل بين الأفراد والشركات في جميع أنحاء العالم. وقد مكن هذا التواصل خارج التفاعلات وجها لوجه بينما يمكن للشركات الحصول على المبيعات على الصعيد الدولي. ومع ذلك، فهي أيضًا قناة لارتكاب جرائم الإنترنت، مثل العدوان والمضايقة السيبرانية ومطاردة الإنترنت وانتشار القذف وانتهاك حقوق النشر وسرقة الهوية والتطرف الإلكتروني. وبالرغم من عديد من الجرائم الإلكترونية على شبكات OSN، فهناك تحديات لا حصر لها تواجه الطب الشرعي الرقمي الخاص بشبكات OSN. وتشمل أساليب مكافحة الطب الشرعي والتحديات القانونية والتحديات القائمة على الموارد.

إنها تحد من التحقيقات الجنائية، ما يجعل من الصعب إدانة المجرمين. وتشير التحديات التي لا تنتهي في إجراء الأدلة الجنائية OSN إلى منطقة رمادية تتعلق بمكافحة الجريمة وسلامة المواطنين في جميع أنحاء العالم.

وعملت في هذه المقالة على دراسة الجرائم الإلكترونية المختلفة على شبكات OSN والتحديات التي واجهتها في إجراء الطب الشرعي الرقمي على شبكات OSN. والتي تشكل أساسًا للتجمع للحصول على دعم ثابت وموجد في جميع أنحاء العالم لمكافحة الجرائم.

الكلمات المفتاحية: *تقنيات مكافحة الطب الشرعي، الجرائم الإلكترونية، الشبكات الاجتماعية عبر الإنترنت، الطب الشرعي الرقمي.*