[1]Clement Agbeboaye

Investigative Analysis of Cybercrime in Nigeria: Using Theft Triangle

Journal of Electrical Systems

Abstract: - Cybercrime or computer related crime is a criminal activity carried out with the aid of computer and the internet. The internet has contributed to the growth and development of the Nigerian economy and the world at large. However, the correlation between the growth of the internet and cybercrime in Nigeria is directly proportional to each other. Cyber insecurity is one of the biggest vices threatening the growth and advancement of the Nigerian economy. This paper provides investigative analysis of cybercrime in Nigeria using "theft triangle". Theft triangle comprises of the three key elements that must be present before theft can take place which are "desire, motive and opportunity". Nevertheless, since the desire and motive of a criminal cannot easily be controlled, the paper focuses more on "opportunity" as a measure to enhance the security of cyberspace in Nigeria. An experimental set-up was done to determine the security of cyberspace when "opportunity" was not controlled and when it was controlled over a period of time. The investigation revealed that cyberspace is subject to theft when "opportunity" was not controlled than when it was controlled. Hence, the study suggests appropriate modalities to enhance the security of cyberspace in Nigeria.

Keywords: Cybercrime, Theft Triangle, Cyber Security, Cyberspace

I. INTRODUCTION

The geometric growth of technology and the widespread adoption of the internet have brought about numerous benefits to society. However, despite these advancements, there has been an alarming surge in cybercrime globally, posing significant threats to individuals, organizations, and nations. The term "cybercrime" refers to criminal activities that are carried out using digital tools, particularly the internet. Nigeria, with its huge population and expanding digital landscape, has not been immune to this threat. Cybercrime has emerged as a pressing problem in the country, necessitating a comprehensive investigative analysis to understand its dynamics and devise effective countermeasures. Cybercrime is thriving in Nigeria undetected, affecting its critical national infrastructure, causing prolonged terrorism, affecting national security and the safety of national environment due to weak cyber security capability [1].

According to [2], nearly two-thirds of internet users (more than two billion) have their personal data stolen or compromised. Over one million users fall prey to some form of cybercrime every day [2]- [4]. In recent years, Nigeria has witnessed a surge in various forms of cybercrime, including online fraud, identity theft, phishing scams, data breaches, cyber espionage and distributed denial of service attacks. Cybercrime also includes non-monetary offenses, such as creating and distributing viruses or worms on other people's computers or posting confidential business information on the internet [5]. Nigeria's growing digital landscapes, its status as a major African economy and poor cyber security architecture have made it an attractive target for cybercriminals. The scale and complexity of cybercrimes make them challenging to investigate and prosecute, requiring specialized skills, collaboration between law enforcement agencies, and robust legal frameworks.

The Theft Triangle is a criminological theory that explains the three elements that must be present before crime can occur; desire, motive and opportunity. According to the theory of theft triangle, no crime or theft can take place without the complete presence of these three elements. Desire refers to the strong craving or want for something, such as material possessions, financial gain, or personal gratification. It is an internal drive or impulse that motivates individuals to fulfill their wants or needs. Controlling desire is challenging because it is rooted in individual motivations, preferences, and emotions. Motive represents the fundamental reason or purpose behind a person's action. It provides an explanation for why an individual may engage in criminal activities. Motives are often complex and influenced by a combination of internal and external factors, including

[1] Department of Electrical/Electronic Engineering Technology, National Institute of Construction Technology and Management, Uromi, Nigeria.

[1]c.agbeboaye@nict.edu.ng

personal experiences, social influences, and psychological factors. Similar to desire, controlling motive can be difficult as it pertains to deeply inbuilt aspects of an individual's mind. Opportunity refers to the favourable circumstances or conditions that enable a criminal act to occur. It includes factors such as vulnerable targets, lack of security measures, or situations where the risk of detection or punishment is low. Unlike desire and motive, opportunity can easily be controlled to a greater extent through preventive measures. References [6] and [7] argue that improved security is the best explanation for the recent declines in crime in most Western countries. The more opportunities for crime that exist, the more crime there will be [6].

This study aims to conduct an investigative analysis of cybercrime in Nigeria, utilizing the framework of the Theft Triangle. However, since the desire and motive of a criminal cannot easily be controlled and the urgency of proffering solution to cyber insecurity in Nigeria, the paper focuses more on "opportunity" as a measure to enhance the security of cyberspace in Nigeria. An experimental set-up was done to determine the security of cyberspace when "opportunity" was not controlled and when it was controlled over a period of time.

II. MATERIALS AND METHODS

1. **Materials:** The materials that were used in this research were an Android phone with WPA2 PSK security protocol feature, a Glo Sim Card and 15GB data subscription for browsing.
2. **Methods:** In this research, an experimental set-up was carried out to determine the security of cyberspace when "opportunity" was not controlled and when it was controlled over a period of time. The investigation was carried out at the Engineering block of the National Institute of Construction Technology and Management, Uromi, Edo State, Nigeria. In order to determine the security of cyberspace in Nigeria, two different investigations were carried out, that is:

(a) To determine intrusion opportunity in Nigerian cyberspace when no security protocol was used (security was opened) in a wireless local area network (WLAN).
(b) To determine intrusion opportunity in Nigerian cyberspace when security protocol was enabled with a password in a wireless local area network (WLAN).

The data obtained from the investigations were presented in sections **a.** and **b.** respectively.

a. Investigation to determine intrusion opportunity in Nigerian Cyberspace when no security protocol was used (security was opened) in a WLAN

To carry out the investigation to determine intrusion opportunity in Nigerian cyberspace when no security protocol was used in a WLAN, the following procedures were followed:

❖ First, the Wi-Fi hotspot on the Android mobile phone was enabled. To do that, navigate to the Wi-Fi settings and toggle it to the ON position. Next, the security setting was accessed and the 'NONE' option was chosen. It's important to keep in mind that the maximum number of users allowed to connect to this Wi-Fi hotspot is ten (10).

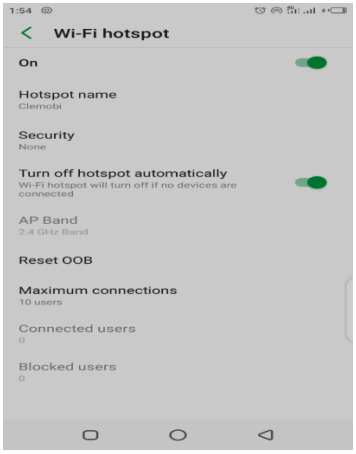

Fig 1: steps to determine intrusion opportunity in Nigerian cyberspace when no security protocol was used in a WLAN, 1

❖ In Fig 1, at about 1:54pm when wifi hotspot was ON and no security was chosen, the number of users connected to the WLAN was zero (0).

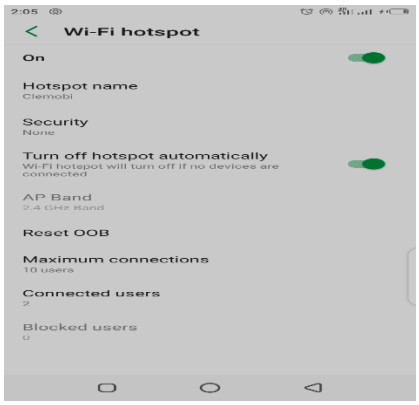

Fig 2: steps to determine intrusion opportunity in Nigerian cyberspace when no security protocol was used in a WLAN, 2

❖ In Fig 2, at about 2:05pm, the number of unauthorized users connected to the WLAN was two (2).

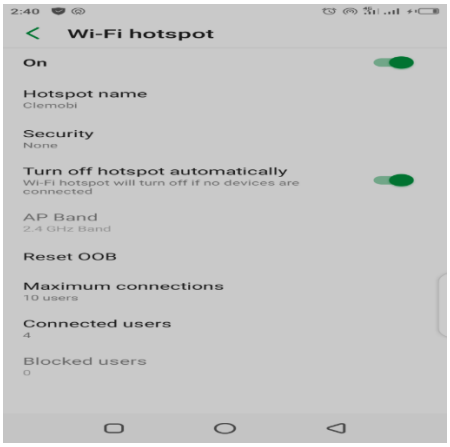

Fig 3: steps to determine intrusion opportunity in Nigerian cyberspace when no security protocol was used in a WLAN, 3

❖ In Fig 3, at about 2:40pm, the number of unauthorized users connected to the WLAN was four (4).

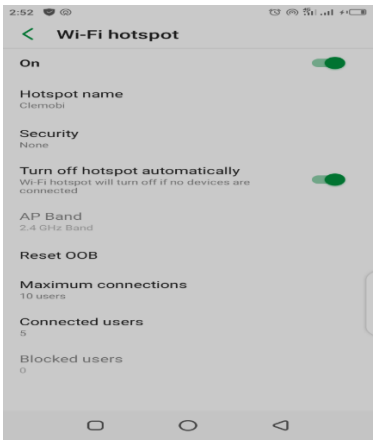

Fig 4: steps to determine intrusion opportunity in Nigerian cyberspace when no security protocol was used in a WLAN, 4

❖ Finally, in Fig 4, at about 2:52pm, the number of unauthorized users connected to the WLAN was five (5).

b. **Investigation to determine intrusion opportunity in Nigerian Cyberspace when WPA2 PSK Security protocol was enabled with a password in a WLAN**

To carry out the investigation to determine intrusion opportunity in Nigerian cyberspace when WPA2 PSK security protocol was enabled with a password in a WLAN, the following procedures were followed:

❖ First, the Wi-Fi hotspot on the Android smart phone was enabled. To do that, navigate to the Wi-Fi settings and toggle it to the ON position. Next, the security option was accessed and WPA2 PSK was chosen. Then, the desired password was entered at the "hotspot password" section. In this instance, eight-character alphanumeric password was used. It is important to emphasize that this particular password was not shared with anyone.

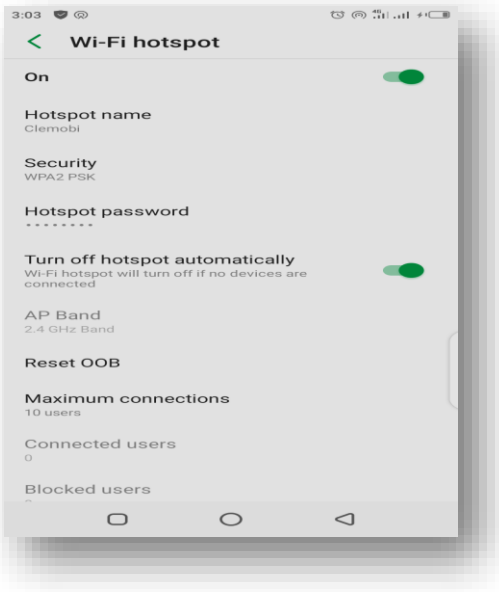

Fig 5: steps to determine intrusion opportunity in Nigerian cyberspace when WPA2 PSK Security protocol was enabled with a password in a WLAN, 1

❖ In Fig 5, at about 3:03pm when wifi hotspot was ON and WPA2 PSK security protocol was enabled with a password, the number of users connected to the network was zero (0).

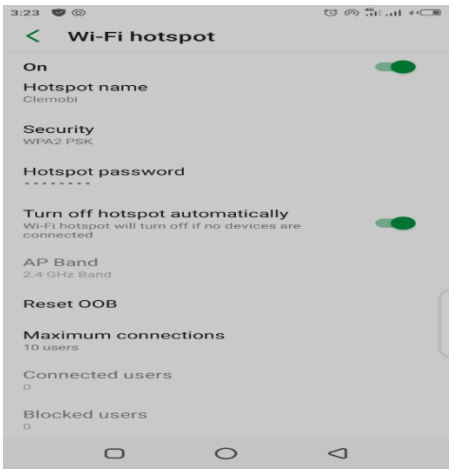

Fig 6: **steps to determine intrusion opportunity in Nigerian cyberspace when WPA2 PSK Security protocol was enabled with a password in a WLAN, 2**

❖ In Fig 6, at about 3:23pm, the number of users connected to the network was still zero (0).

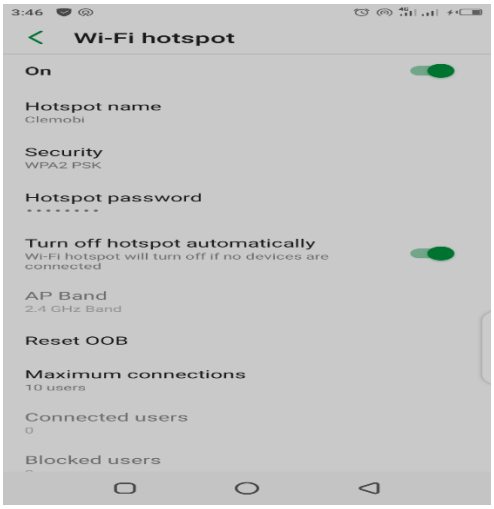

Fig 7: steps to determine intrusion opportunity in Nigerian cyberspace when WPA2 PSK Security protocol was enabled with a password in a WLAN, 3

❖ In Fig 7, at about 3:46pm, the number of users connected to the network remains zero (0)

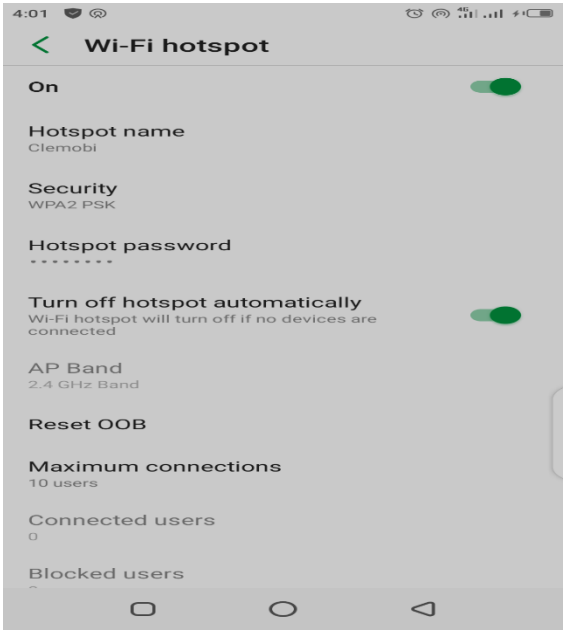

Fig 8: steps to determine intrusion opportunity in Nigerian cyberspace when WPA2 PSK Security protocol was enabled with a password in a WLAN, 4

❖ Finally, in Fig 8, at about 4:01pm, the number of users connected to the network still remains zero (0).

III. RESULTS AND DISCUSSION

The numbers of unauthorized users connected to the WLAN at various times when no security protocol was enabled are presented in Table 1 and the numbers of unauthorized users connected to the WLAN at various times when WPA2 PSK security protocol was enabled with a password are presented in Table 2.

Table 1: Number of unauthorized users connected to the WLAN at various times when no security protocol was enabled.

S/N	Time (1:54pm – 2:52pm)	No of unauthorized users connected to the WLAN
1	1:54pm	0
2	2:05pm	2
3	2:40pm	4
4	2:52pm	5

Table 2: Number of unauthorized users connected to the WLAN at various times when WPA2 PSK security protocol was enabled with a password.

S/N	Time (3:03pm – 4:01pm)	No of unauthorized users connected to the WLAN
1	3:03pm	0
2	3:23pm	0
3	3:46pm	0
4	4:01pm	0

.

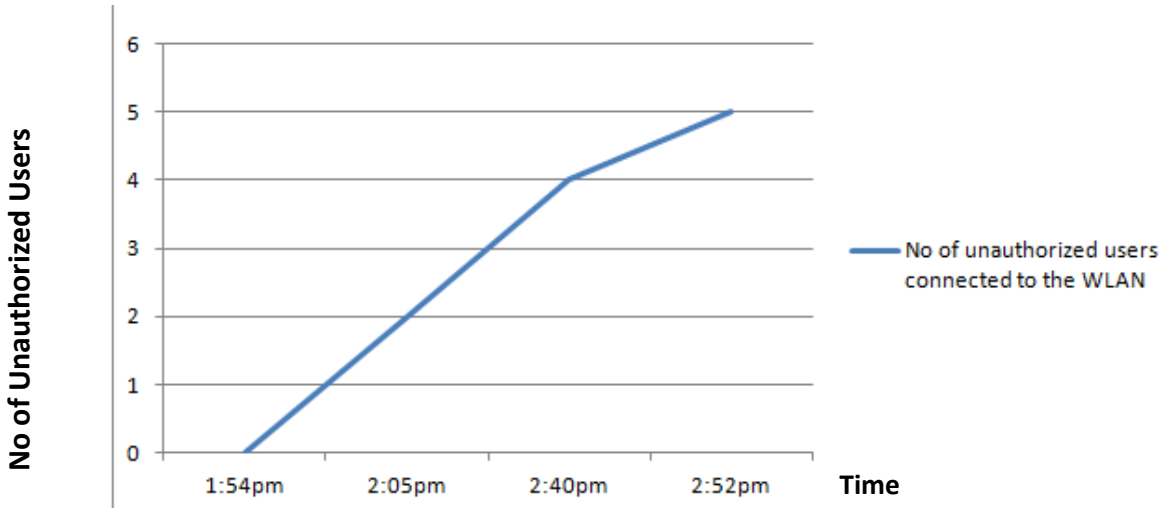

Fig 9: Number of unauthorized users versus time when no security protocol was used

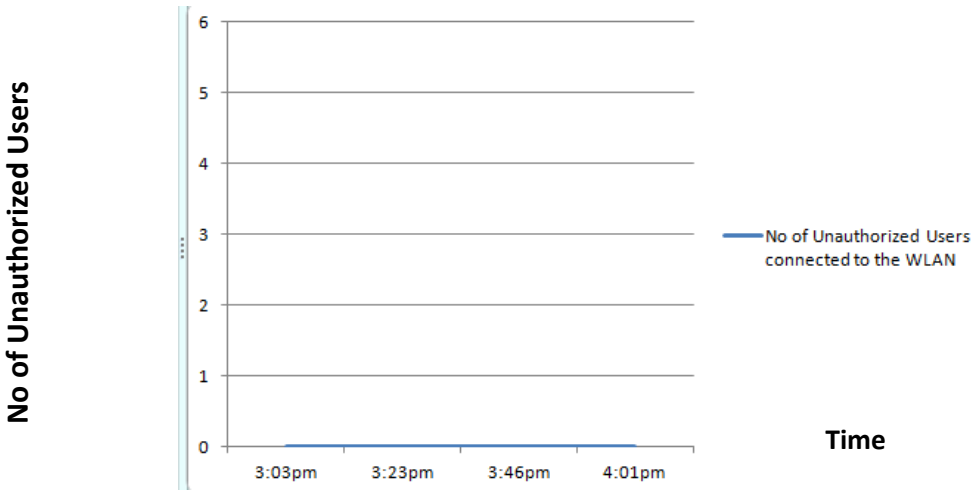

Fig 10: Number of unauthorized users versus time when WPA2 PSK security protocol was enabled with a password.

In Fig 9, the graph demonstrates that during a 58-minute time span without any security protocol for the WLAN, five unauthorized users connected to the network. These users had the desire and motive to connect without notifying the network authority before 1:54 PM on that particular day. However, due to the unavailability of "opportunity", they were unable to do so. Between 1:54 PM and 2:52 PM, when the opportunity arose, the necessary elements for theft (desire, motive, and opportunity) were complete for these five individuals, and they were able to exploit it.

Conversely, in Fig 10, it is evident that during the same 58-minute time span, when the WPA2 PSK security protocol was activated with an unknown password, no one could connect to the WLAN even when the Wi-Fi hotspot was enabled. While some individuals may have attempted to connect, the lack of opportunity prevented their success. Therefore, in this scenario, the required elements for theft were not complete due to controlled opportunity.

Furthermore, the graph in Fig 9 illustrates an increase in the number of unauthorized users as time progresses. This may be attributed to the availability of data for browsing (i.e., opportunity) and the continued presence of desire and motive. It can be hypothesized that opportunity can trigger the "desire" and "motive" for theft. This finding agrees with the research "Opportunity makes the theft" by [6] who asserted that the more opportunities for crime that exist, the more crime there will be. This may explain why individuals who never believed they had the desire and motive to steal later regret their actions when caught, as the opportunity presented itself. It is important to note that the application of the theft triangle for analyzing security extends beyond cyber security and applies to various other aspects that require protection. Therefore, this research is valuable not only for network experts but also for anyone interested in enhancing security measures for different domains.

IV CONCLUSION

The research clearly indicates that among the three factors necessary for theft to occur (known as the theft triangle), opportunity is the most controllable. Another important finding from the research is that the presence of opportunity can trigger the "desire" and "motive" of a potential thief. If a thief has no plan of stealing but an opportunity arises, the desire and motive can easily be instigated. Conversely, if an opportunity is not readily available, the desire and motive can be easily discouraged or suppressed.

From the research findings, it becomes evident that addressing the loopholes in the area of opportunity is an urgent solution to combat cybercrime in Nigeria. The concept of opportunity within the theft triangle framework refers to the conditions or circumstances that enable cybercriminals to exploit vulnerabilities and gain unauthorized access to systems or networks.

V RECOMMENATIONS

Based on the findings from this research, the following recommendations are made to secure cyberspace in Nigeria:

1. **Address Vulnerabilities in Systems and Networks:** Organizations and individuals should prioritize identifying and patching security vulnerabilities in their systems, networks, and software. By actively addressing these vulnerabilities, opportunities for cybercriminals to exploit weaknesses and gain unauthorized access can be significantly reduced.
2. **Strengthen Security Measures and Implement Industry Best Practices:** Organizations and individuals should enhance their security measures and adopt industry best practices to mitigate the opportunities for cybercriminals to exploit weaknesses. This includes implementing strong passwords, utilizing encryption for sensitive data, keeping software and systems up to date, and establishing robust access controls. By prioritizing these security measures, the risk of unauthorized access and exploitation by cybercriminals can be significantly reduced.
3. **Raise Awareness and Educate Users about Social Engineering and Phishing Attacks:** Organizations and individuals should prioritize raising awareness and providing education on social engineering and phishing attacks. By familiarizing users with common tactics used by cybercriminals and teaching them how to identify and respond to such attempts, the opportunities for successful social engineering and phishing attacks can be significantly reduced. Regular training programs, awareness campaigns, and simulated phishing

exercises can be implemented to empower users with the knowledge and skills needed to protect themselves and their organizations from these threats.

4. **Mitigate Insider Threats through Strict Access Controls and Employee Training:** Organizations should implement strict access controls, conduct regular employee training, and implement monitoring systems to mitigate the risks associated with insider threats. By carefully managing user access privileges, ensuring that employees only have access to the information and systems necessary for their roles, and regularly reviewing and revoking access for employees who no longer require it, the opportunities for internal individuals to engage in malicious activities can be minimized. Additionally, conducting comprehensive employee training programs that cover security policies, procedures, and the consequences of insider threats can increase awareness and foster a culture of security within the organization. Implementing monitoring systems to detect and flag any suspicious activities can also help identify potential insider threats and allow for timely intervention.

5. **Enhance Network Monitoring:** Implementing effective network monitoring tools and techniques can help detect and prevent unauthorized access attempts in real-time. Network administrators should invest in intrusion detection and prevention systems, log analysis tools, and traffic monitoring solutions to identify any suspicious activities and take immediate action to mitigate potential security breaches.

Acknowledgement

The author would like to sincerely express his gratitude to the management of the National Institute of Construction Technology and Management, Uromi, and the Tertiary Education Trust Fund (TETFund) for their generous support in sponsoring his participation in the 6th International conference on Multidisciplinary Approaches in Technology and Social Development (ICMATSD-2023), Seoul, South Korea.

REFERENCE

[1] S. Babayo, M. Bakri, S. Usman, K. T. Mohammed and A. Y. Muhammad, "Cybersecurity and Cybercrime in Nigeria: The Implications on National Security and Digital Economy," Journal of Intelligence and Cyber Security, pp. 27 – 61, October 2021.

[2] P. Kaur, "Cyber Connectivity, Cybercrime, and Cyberspace Regulations," Auburn University at Montgomery, Alabama, USA, Book Chapter, pp 299 – 315, November 2020

[3] European Commission, "The European agenda on security. Strasbourg: European Commission," 2015. Retrieved from http://ec.europa.eu/dgs/homeaffairs/elibrary/documents /basicdocuments/docs/eu_agenda_on_security_en.pdf.

[4] Europol, "The relentless growth of cybercrime," 2016, Retrieved from https://www.europolo.europa.eu/newsroom/news/relentless-growth-of-cybercrime

[5] C. Chigozie-Okwum, S. Ugboaja, D. Micheal and M. Osuo-Genseleke, "Proliferation of cyber insecurity in Nigeria: a root cause analysis," *AFRREV STECH: An International Journal of Science and Technology*, Vol *6, No* 2, 2017.

[6] R. V. Clarke, "Opportunity makes the theft. Really? And so what?," Crime Science, a Springer Open Journal, Vol 1, No 3, 2012.

[7] D. J. Van and T. A. Farrell, "The International Crime Drop," Palgrave Macmillan, London, 2012.