I.T. Case Study

Name

Institutional Affiliations

I.T. Case Study

Introduction

Cyberterrorism might seem new to most people, it has proven to be very challenging. Currently, there has been a huge improvement in industry and government initiatives in most countries towards protecting people against cyber attacks since it has become a serious threat. In order to have a better understanding of Cyberterrorism, the following paper is Ardit Ferizi's cyberterrorism case that will be supplemented by two theories General Theory of Crime (GTC) and Lifestyle Exposure Theory. The paper begins by giving an overview of the case followed by general description of the two theories. The paper will then discuss how the two theories apply to the case study and finally give counter measures to Cyberterrorism.

Case Overview

- ✓ Ardit Ferizi's Cyberterrorism Case

Ardit Ferizi a citizen of Kosovo was the first person to be charged by the United States Justice Department for cyber terrorism and hacking. Ferizi was a known hacker and was apprehended in Malaysia following an arrest warrant offered by the United States government (Stewart). Ferizi was arrested in September 2015 and charged in October 2015 (Stewart, 2016). Ferizi was charged for supporting the Islamic State by providing material support, identity theft, and computer hacking (InfoSec Institute, 2016). All these charges were in conjunction with the stealing and releasing of information that was personally identifiable. The information released was connected to 1,351 United State Service members as well as government employees (Stewart, 2016). The information was stolen from an unnamed server in the United States' retail chain. Prior to this, the Islamic State was for long trying to hack the most powerful companies in

the United States of America (Stewart). Ferizi managed to steal the personal information including names, e-mail addresses, passwords, locations, and phone numbers and provided it to Junaid Hussain a popular IS militant and member of the Islamic State. Hussain was later killed during an airstrike in the Syrian capital, Raqqa (InfoSec Institute, 2016).

Description and Review of Theories

- ✓ General Theory of Crime (GTC)

Crime is a concept that has been around since the beginning of civilization and as the crime trends evolve the theories of why people cause crimes changes with time. It is necessary for every individual to be familiar with the different theories of crime causation since anyone can be a victim of a crime. There are several competing theories with some trying to explain criminal behaviour.

According to Akers (2017), general theory of crime was developed by Gottfredson and Travis Hirschi in the year 1990. This is a worldwide theory that maintains to be having the capability to explain any form of crime at any time. This theory has a central construct which includes criminal behaviour and self-control. In this case, low self-control is the number one and most essential predictor of delinquent behaviour (Agnew, 2005). Further, the general theory of crime is a form of control theory that asserts that it can explain different acts of crime as well as 'analogous' behaviour such as accidents and divorces where low self-control is dominant. Typically, a family is the most essential institution when it comes to the development of self-control and explanation of delinquent behaviour. School and neighbourhood institutions have a secondary role to play and it is not guaranteed that they will play. The general theory of crime is the most tested criminological approach from both a theoretical and empirical point of view.

In their definition of the crime, Gottfredson and Hirschi define it as "...acts of force or fraud were undertaken in pursuit of self-interest". (1990: 15). However, their definition fails to build on the legal definition of crime as an offense. The reason behind this is for them to comfortably determine the nature of criminal acts as a scientist without depending on political decisions. In their view, the definition of crime is the most essential point of their theory arguing that crime itself is the central concept of a theory of crime (Arneklev, Elis & Medlicott, 2006).

- ✓ Lifestyle Exposure Theory

The analysis of Richard Cloward and Lloyd Ohlin's on criminal behaviour and how it extended the variety of pertinent theoretical questions beyond the search for motivational factors led to the development of 'Lifestyle Exposure Theory' (Bastien, 2012). Developed by Michael Hindelang, Michael Gottfredson, and James Garofalo, this theory is important in that it talks about the importance of understanding how criminal inclinations are channelled by opportunities to be criminal (Bastien, 2012). The trio discusses this theory in their book "Victims of Personal Crime." Therefore, Lifestyle Exposure Theory is a theory that pays attention to the tendency whereby individuals possessing certain demographic characteristics allocate their time and vigour across different activities which might lead to their victimisation by offenders. Since the early 1970's, the study of criminal opportunities has for long been dominated by scholars as well as researchers interested in victimization. The explanation that these researchers give regarding the Lifestyle Exposure Theory is that it pays attention to how spatial as well as temporal variations in crime connects to or relates to the opportunities to carry out the criminal act.

For instance, if a person goes to bed early, there will be less risk involved when compared to visiting a bar. This confirms Hindelang et al. (1978) findings that individuals who spend most of

their time in public places are most likely at a risk of experiencing personal crimes. Considering that it is a theory of victimization, Lifestyle Exposure Theory acknowledges that people will always have a different lifestyle and some will expose them to more risk compared to others (Yucedal, 2010). Strategies for crime control would include those that enhance or increase effective guardianship and at the same time minimise the availability of motivated offenders. Hindelang and associates developed the Lifestyle Exposure Theory in an attempt to explain the correlates of crime against individuals and later on was extended to property crime by Cohen and Felson. With the victimology literature, lifestyle exposure theory emphasises that different forms of antisocial behaviour such as violent offending are indicators of a lifestyle that places individuals at increased risk for violent victimization (Yucedal, 2010).

Hindelang and his colleagues drew their analysis within 8 United States of America cities asserting that the risk of victimisation significantly depended on "routine daily activities" either vocational of leisure activities. Their findings show that individuals are exposed differently with some of the lifestyles ending up exposing individuals to crime-prone situations whereby there is immense exposure to higher victimization risk (Yucedal, 2010).

Application of the theories

- ✓ Application of Lifestyle Exposure Theory to Cyberterrorism

The contemporary world is dependent on information technology. As many people use technology for personal benefit especially through aiding and supporting lives, it also comes along with differing risks and vulnerabilities to the society. There are those individuals who will use computer technology to carry out crimes as well as acts of terror hence posing an alarming threat in every corner of the world as people become more dependent on information technology

than ever before. The increased use of computer technology and cyber-dependent attacks is on a daily basis becoming a top threat by rebel groups. This emerging threat is what is now referred to as cyber terrorism (Littlefield, 2017).

According to New Hampshire Department of Safety (2014), some of the cyber threats posed by these groups include viruses that are capable of deleting an entire system, intruders using other people's computers to attack others, intruders that break into computers to alter files or steal confidential information such as the Kosovo citizen Ardit Ferizi who is the main actor in the chosen cyber terrorism case. As noted by Cohen and Felson, advancements in technology including automobiles, telephones, power tools and weapons can be used for illegal purposes. This means that technology cannot only make daily life easier but can help criminals carry out their deviant activities.

Similarly, advancements in computer technology are giving room to cyberspace that has changed the routine activities of individual's right from communicating and doing business. Cyberspace provides offenders with the opportunity to find suitable targets and at the same time commit crime easily. Applying Lifestyle Exposure Theory to cybercrime, Internet users are a target and offenders are always on toes to victimise them. Also, individuals who engage in online activities and at the same time expose their personal information are prone to victimization risk. Though offenders have an opportunity to locate suitable targets, it is not true that every individual has the same level of victimization risk (Yucedal, 2010).

The different level of victimization is based on the activities an individual does while using the internet. Programs such as freeware downloads as well as visiting unprotected websites create a victimization risk that is higher than when visiting online news channels or checking

emails. According to a 2008 study by Choi, he found out that people download video games, videos, music, and visit unknown websites are prone to higher risk of cyberspace victimization. It is therefore important for individuals to have a better understanding of how individuals are victimised based on their lifestyle and hence need to take measures (Yucedal, 2010).

Even if, studies that used Lifestyle Exposure Theory show that postulations of the theory are applicable in cyber space, some questions come up regarding the extent to which these theories can be applied to cybercrime. As noted earlier, Hindelang and his colleagues stated that a person significantly contributes to his or her effect on victimization risk through self-exposure to different situations that are capable of increasing chances of coming into contact with potential offenders (Yucedal, 2010).

From the case study, one group that suffered a victimisation risk was the unnamed United States online retail company whereby the offender Ferizi (Kosovan hacker) accessed data on about 100,000 individuals. Ferizi chose his target aiming to gather information on United States military personnel. In the process, he discovered personal information of about 1,351 military personnel and government employees. Ferizi was part of the Kosova Hacker's Security a team that conducted cyber attacks against global organisations. The group is said to have carried out cyber attacks on more than twenty thousand websites in different countries (InfoSec Institute, 2016).

- ✓ Application of General Theory of Crime to Cyberterrorism

According to Bossler & Burruss (2012), in the most recent times, scholars and researchers, especially from the file of psychology and criminology, have embarked on studying the hacker's personality and communication traits. However, different questions have remained

unanswered. For instance, does Gottfredson and Hirschi concept of low-self control predict the unauthorised access of computer systems? Do hackers have low self-control as has been proven in other criminal mainstream society? Typically, if a low level of self-control shows cases of computer hacking, then, it would support the generality argument of the general theory of crime implying that computer hacking, as well as other forms of cybercrime, are to an extent similar to terrestrial crime.

As noted earlier on, the growth of computer technology, as well as the Internet, has both positive and negative impacts on modern life. It is true that newer technology makes communication and business transactions more efficient, but on the other hand, makes work easier for criminal as well including computer hackers who are always set to victimise individuals as well as businesses without sharing the same physical environment. Typically, computer hacking is the unauthorised access and use of other people's computer systems. According to Richardson (2008), roughly 29% of all security professionals reported that their computer system had experienced unauthorised in the year 2007 (Bossler & Burruss, 2012). It is important to note that hacking is increasing at both frequency as well as complexity. Hackers have linked with rebel groups such as Ardit Ferizi who is involved with organised crimes as well as state-sponsored terrorism. According to Gottfredson and Hirschi's general theory of crime or self-control theory, people commit a crime since they are unable to resist temptation and end up committing acts that have long-term consequences compared to short-term benefits (Bossler, & Burruss, 2012). Self-control is said to be carrying the weight of crime in both digital and traditional piracy literature. The duo state that most hacking is one-dimensional and hackers take advantage of people who have low self-control.

Implications of theories for Prevention

For successful countering of the negative impact of cyber terrorism effects on humans, crucial infrastructure, and businesses, it is necessary to have a multidimensional and comprehensive strategy. For instance, there are some strategies that are shallow but effective including pursuing and persecuting the perpetrators (Jalil, 2003). However, more complex and far-reaching strategies are as follows.

The first measure that can be adopted is the enactment of a legal framework. Typically, a legal framework regulates the Internet in relation to the different threats posed by cyber terrorism; social media monitoring in order to sense, act in response and dissuade any possible spreading of terrorist propaganda, radicalisation communication, data mining in readiness to planning terrorist attacks or recruiting people (Zerzri, 2017).

The second measure is through national partnerships. These partnerships will most likely strengthen stakeholder's capacity such as specialists in cybersecurity, the judiciary as well as law enforcement agencies. Also, ties between the public and private sector. The people who can join hands, in this case, include the government, cybersecurity experts, telecommunication network, security forces, and telecommunication network operators (Zerzri, 2017).

The third measure is a national strategy. For instance, a national cybersecurity strategy should aim to create and improve cybersecurity to be resilient as well as secure to threats of cyberspace. Also, there should be a national strategy to counter terrorist online propaganda and this can be through the removal of their content (Zerzri, 2017).

Be Proactive is another measure that can significantly help curb cases of cyber terrorism and improve awareness among individuals who offenders tend to victimise. Organisations and the members of the general public ought to be more proactive when dealing with cases of cyber

attack issues. They should always be updated on the latest information related to vulnerabilities, threats, and incidents and as a result improves their information security postures (Jalil, 2003). Also, to void victimisation risk, organisations should always make sure that they improve their security infrastructure by employing multilevel security architecture other than employing the single-tier ones for better protection.

Conclusion

As noted from the two theories, General Theory of Crime and Lifestyle Exposure Theory, the lifestyle we live and the traits we possess determine how individuals are affected by cases of cyber attacks. Security is a continuous journey that brings everyone on board. There are many aspects that come along with cyber terrorism including understanding different motivations and types of attack, getting to know its impact on humans, businesses, and critical infrastructure, and to some extent undertaking sophisticated steps to curb the occurrence of such attacks.

All in all, by employing strategic security measures such as partnering with different bodies including industry, the general public, and the government provides hope of winning the cyber terrorism battle. The fact remains that cyber terrorism is here to stay and there is a need for more seriousness in protecting self-interests, businesses, and the nations at large. However, proper implementation of the suggested countermeasures provides hope of getting closer to realising the primary goal of having a cyber safe working environment.

References

Agnew, R. (2005). Why do criminals offend?: A general theory of crime and delinquency.

Akers, R. (2017). *Social learning and social structure: A general theory of crime and deviance*. Routledge.

Arneklev, B. J., Elis, L., & Medlicott, S. (2006). Testing the General Theory of Crime: Comparing the Effects of "Imprudent Behavior" and an Attitudinal Indicator of "Low Self-Control". *Western Criminology Review*, *7*(3), 41-55.

Bastien, B. (2012). Lifestyle Exposure Theory. Retrieved from http://rezi.com/vgxnkqdod3ue/lifestyle-exposure-theory/

Bossler, A. M., & Burruss, G. W. (2012). The general theory of crime and computer hacking: Low self-control hackers?. In *Cyber Crime: Concepts, Methodologies, Tools and Applications* (pp. 1499-1527). IGI Global.

InfoSec Institute. (2016, March 9). The Ferizi Case: The First Man Charged with Cyber Terrorism. Retrieved from https://resources.infosecinstitute.com/the-ferizi-case-the-first-man-charged-with-cyber-terrorism/#gref

Jalil, S. A. (2003). Countering cyber terrorism effectively: Are we ready to rumble. *GIAC Security Essentials Certification (GSEC) Practical Assignment Version*, *1*(4), 10-15.

Klein, J. J. (2015). Deterring and Dissuading Cyberterrorism. *Journal of Strategic Security*, *8*(4), 2.

Littlefield, R. (2017, June 7). Cyber Terrorism: understanding and preventing acts of terror within our cyber space. Retrieved from https://littlefield.co/cyber-terrorism-understanding-and-preventing-acts-of-terror-within-our-cyber-space-26ae6d53cfbb

New Hampshire Department of Safety. (2014). Cybercrime and Cyber Terrorism | Disasters | ReadyNH. Retrieved from https://www.readynh.gov/disasters/cyber.htm

Stewart, S. (2016). The Coming Age of Cyberterrorism. Retrieved from https://mysu.susqu.edu/personal/rusek/news/Saved%20Articles/Coming%20Age%20of%20Cyberterrorism.pdf

Yucedal, B. (2010). *Victimization in cyberspace: An application of Routine Activity and Lifestyle Exposure theories* (Doctoral dissertation, Kent State University).

Zerzri, M. (2017). The Threat of Cyber Terrorism and Recommendations for Countermeasures. Retrieved from https://www.cap-lmu.de/download/2017/CAPerspectives-Tunisia-2017-04.pdf