Strategies for addressing cybercrimes

Summary

The paper presents a detailed synopsis of how we can effectively start to address cyber

war and cyber terror. Furthermore, it discusses how detailed knowledge can be obtained

regarding the types of crimes committed via any social or public platforms.

This paper has also been able to poke comments on: the translation of

cyber terrorism, the teachings and steps which are being used by the new terrorist, the

shifting aspects, the results and consequences of such a common new form of cyber-

attack. Thus in a nutshell, how to address cyber war and cyber terror, and in turn, discussing approaches to accomplishing this.

Furthermore, it introduces a suitable elixir to control and reduce the increasing rate of such

a cyber attack, also to increase the benefits attached to information streamlining and to

decrease the malicious acts committed by the terrorist. Effort to secure the cyberspace

should be given the ultimate priority; if not, the information restructuring will not be

effectively utilised by users. The terrorists of the future will win the wars without firing a

shot, this would be done by destructing a nation's analytical values and structures. Thus, if

any such steps are not taken in order to overcome such attacks, it may result in the rapid

increase in the cyber-attacks.

Introduction

Crimes, which are committed and completed through any social platform comes under cybercrime. Cyber terror is effectively a way of using social technology to combine it with terrorism. The term cyber terror is becoming increasingly common in the popular culture, yet a concrete definition of the word seems difficult to establish. While the phrase is loosely defined, there is a large amount of subjectivity in what exactly constitutes cyber terrorism.

Cyber war can be referred to as any type of conflict that occurs on a virtual platform, which is a result of an intended attack fueled by a political agenda. This is waged through the internet, such attacks restrict and nullify the systems of state or financial organisational systems. The consequences of such attacks are hostile, often date is stolen, classified date is amended, with the intention of undermining websites, networks and services. (Techopedia. com, 2019)

Janczewski, & Colarik (2008) discusses cyber terror in great depth and refers to it as a premediated attack fueled by a underlying political motivation targeting: computer systems, computer programs and data that results in violence against non-combatant targets. Such an attack is completed by national groups, secret agents or individual agents.

(WEIMANN, 2005) refers to cyber terror in such a way where he illustrates that the term is one that bodes well with the distrust and fear of computer technology. That the majority of such fears results in exaggerated reports; such so that not a single case of cyber terror has yet to be recorded, hackers are regularly mistaken for cyberterrorists. Weimann strongly suggests that whilst the potential threat seems likely to increase and cannot be contested, it is important to address it in such a way where the possible danger is not inflated or manipulated.

One could argue that cyber terror is what could result in and cause a cyber war, as it would provide the entry point for attack and cornering the adversary to a feeling of vulnerability and exposure. A cyber war would not be possible if not for the initial act of cyber terror. As discussed previously, cyber terror has yet to yield a single recorded case. Thus one would say that in order to effectively address cyber war and cyber terror, the higher institutions have area for improvement. Said institutions are those whom society relies upon for security and stability, thus they should address such substantial terms in ways that are representative and accurate.

Many feel that the higher institutions instill fear into members of society to justify hidden agendas. A novel that is perhaps not quite directly linked to the topic of a cyber sphere provides quotes that wholly relate to the topic in discussion. In the novel of 1984, a riveting read, (George Orwell) writes that " Reality exists in the human mind, and nowhere else." In addition to, " War is peace. Freedom is slavery. Ignorance is strength."

The reality is that cyber terror is overplayed, it is magnified, its sole purpose is to provoke a stir and controversy amidst society. A society that is made to feel pressured, feel vulnerable and be manipulated to feel as though a war is way to peace and tranquility. Civilians are slaves to such a state of affairs, they have been brainwashed through propaganda and doctrine. Hard there been a sense of ignorance through a lack of inaccurate information, they would not fear the internet, feel vulnerable free.

The American Dream is one which supposedly states that the government have a duty to protect each indviduals opportunity to pursue their own idea of happiness. (Amadeo, 2019)

The American Dream is the ideal that the government should protect each person's opportunity to pursue their own idea of happiness.

Thus, it could be said that it is far more important to address cyber terror as opposed to cyber war. A supporting reason for this is to reduce the possibility of an initial act of cyber terror; one which would have the possibility of sparking a cyber war.

How can we effectively start to address cyber war and cyber terror?

When we discuss cyber threats, one of the first thoughts that occupies our mind is whether or not the personal or secure information of a particular individual has been compromised. Terrorist’s use of the internet and telecommunications devices is growing both in terms of assisting with supporting organisational activities, and for gaining expertise to achieve operational goals. The term terrorism can be referring to the unlawful use of force or violence against persons or property so as to intimidate a government or its citizens and organizations, which may be to achieve a political, or fraudulent objectives. (Bogdanoski & Petreski, 2013).

Terrorism has transformed from the traditional form to the cyber form of technology assisted terrorism known as cyber terrorism. We can observe that crime is overly similar to terrorism and both target our societies. However, when any of the terms is used, one must be able to differentiate between the two terms. Crime is a word related to distinctive acts whereas terrorism often refers to a group of individuals. Crimes can be committed due to: personal conflict, jealousy, grudge and enviousness, which can be a result of insecurities. On the contrary, terrorism is comprised of the actions that occur prior to the

loss of something, or when an individual seeks to spark change. It is a situation where the terrorist desperately long for individuals to function according to their desire. Terrorism includes: abduction, destruction of any legal property, and making people suffer from extreme shock and fear.

The rise of the Internet and the growing importance of cyberspace to all parts of the modern world correspond with the rise of the United States as the world’s lone superpower. Over the last 25 years, the creativity of the American people hold the progress of cyberspace, and in turn, cyberspace has become fundamental to American money generation and renovation. Cyberspace is becoming an indivisible component of America’s financial, public, executive, and political living. Americans assume that the growing of the Internet would take the comprehensive urge for free expression and individual freedom globally. Americans seek to explore new openings to spread links, trading and to develop. Major segments of the world have clutched America’s thought process of a distributed and open cyberspace for the shared advantage of all.

New threats and a new era of strategic competition demand a new cyber strategy that responds to new realities, reduces vulnerabilities, deters challengers, and safeguards opportunities for the American people to thrive. Purchasing cyberspace is foundation to the approach and requires scientific improvements and administrative planning across the political governments and the private positions and groups. The Administration also identifies that a purely expert perspective to cyberspace is insufficient to address the use of the new problems, which is observed. The nation must also have policy alternatives to impose money charge if it hopes to discourage harmful cyber actors and stop further growth. The management is already taking action to vigorously address these attacking threats and adjust to new realities. The United States has authorised malign cyber attackers and accused all those who have previously committed cybercrimes. They have publicly assigned illegitimate activity to the responsible adversary and provided details of the tools combined with the overall structure they implemented. Departments, sections and approachable agencies are required in order to vanish software that is vulnerable to various security risks. Strict actions have been taken by America to identify the number of groups and agencies, whom are responsible. They are marked accountable for managing the cyber security opportunities to the systems they supervise, while empowering them to give appropriate security.

Cyber Terrorism is the terror and fear achieved through any social platform. In the current age, communal-social platforms are allowing a huge trade of information. In addition to this, the Internet has also produced a token for the attackers and criminals through which they can also communicate, via cyberspace. Cyberspace is nothing but a threat of terrorism’s production. Cyberspace is the main source, which is currently empowering cyber attackers. It is essentially the functioning and usage of computer grids for the purpose of presenting abuse to human life or to destruct most of the vital and national analytical infrastructure. Which in such a way that will shock the nation coupled with its citizens, cyber terrorism often appears as a result of the merging with the physical form of terrorism.

Cybercrimes done by cyber attackers through approaching cyber space, comes in many different forms, these attacks could be either targeted or untargeted and includes attaining any private or secured information. For example: password, personal accounts hacking, banking information, developing fake pages in order to effect user’s retention and files encryption.

On the majority of occasions, the Cyber terrorist attempts to make use of a password sniffer to carry out their cyberattack on any of the organization's and nation's critical internal structure. The password sniffer is a software, which is used as a scanner in the field of networks, and at the same time it hacks password that cycles through the network adaptor. (Hassan, Funmi, & Makinde, 2012)

A plethora of industries oriented organizations have been shut down and became inoperable as an outcome of the attack completed by the cyber terrorists. This has a ripple effect, and at some point affects the economical state of the nations in the globe. The cyberterrorist may also attempt to make a use of spam messages as a strategy to introduce the entry point of their attack. Spam is the release of unwanted bulk messages. Attackers use a vast range of spam messages and the most commonly used is via e-mail spam. At times, this can be in the form of advertisement for any products and services they impersonate. Therefore, if the message is to be opened by any user, consequently, it may automatically hack the sensitive information ranging from the username to his or her password. By hacking and acquiring such sensitive information, the attackers may have the option to use any acquired information for anonymous attacks. Computer viruses can every so often enter into a system to perform illegal activities. Moreover, it also acts as an agent to monitor the user, perhaps later the attacker may choose to destroy the entire system by flooding it with malicious attacks.

In the present day, individuals encounter such attacks, either targeted or untargeted, in almost every hour. Hackers are able to eradicate, edit or delete any of the personal data being monitored by the legal authorities of any given city. On much of the occasions, hackers attack political sectors of any state or an organization.

Cyberterrorism has experienced a noticeable increase in the 21 st century. It is a cause behind a sudden change and in increase in the anxious behavior of any ordinary citizen, particularly relating to their networking life. Cyberterrorism leans towards the mental destruction and affecting individual’s behavior in the worst possible ways. There is no loss of any life nor is there any physical injury. However, it leads to a number of mental and psychological conditions of individuals. There are many health-related problems, which occurs as result of this, and it includes: tension, anxiety, frustration, anger and many more.

On a daily basis, individuals are facing Cyberattacks and destruction. This can be through obliterating or acquiring data. It leaves individuals with a sense of insecurity and fear of the possibility of future attacks. There are three main factors which have been introduced in supporting of the increase in number of all such hacking attacks: insufficient and poor prevention of computer systems, growth and working of software tools that generates the increase in such attacks, and the increasing power of personal computers as a prey of hacking attacks.

Cyberterrorism has a vast range of forms, this paper demonstrates how even non-lethal, seemingly predictable forms of cyber terrorism have a considerable impact on the attitudes of victimised populations. Though, it is argued that cyber terrorists have neither directly killed nor injured any individual. Nor have they successfully destructed any critical architecture.

Cyber attackers are attacking innocent citizens, thus making them an ‘ easy’ mark. Victims are aware of the difference, under attack, they react with not only fear and demolition, but with demands for protection from the enemies of the state. This could be through harsh military retaliation, surveillance, and strong government. This is the psychology of terrorism. The effect of attacks on innocent individuals can spark and force change on the highest level of ruling within a country.

It is hardly an overstatement to say that the advent and global expansion of the Internet may prove to become the fastest and most powerful technological revolution in the history of mankind. In merely a decade, the amount of individuals, which are actively using the Internet, has increased by a wide range from an estimated 16 million in 1995 to more than 3. 5 billion in 2017. Today, cities, businesses, academic institutions and individuals have become socially interconnected by a knowledge of the events occurring not only on this planet, but others. There was a point in time when these topics were hard to even comprehend. At the same time, the government’s dependency on computer systems and networks has increased rapidly with the inventions of new technologies. Without giving any second thought, due to the occurrence of theory and claims, existing global and intercontinental law oversees state activities wherever they are carried out, including in cyberspace. However, applying pre-existing legal rules, concepts and terminology to a new technology may entail certain difficulties in view of the specific characteristics of the technology in question. For example, it is commonly known that through smartphones, certain governmental agencies are able to access certain features without the user’s knowledge, such as the camera, microphone and messages. It begs the question of whether or not this is permitted and how it can be seen as a violation of The Right of Privacy law. Many would argue that this is justified, should it assist in establishing and counteracting acts of cyberwar and cyber terror.

Conclusion

The significance of information technology all around the globe can never be over prioritize only that the destruction created by terrorist who has taken its edge to shut down many fields and companies and also have destructed nations relied and critical architecture are just too threatening. In the period of information mechanization, terrorism can be seen as a standard terrorism, in which traditional weapons are used for the destruction of resources and labor in a physical teaching, in which the classic cannon are used for destroying infrastructure and causing damage in cyberspace; and as cyber terrorism, where new weapons are used for the destruction and moderation of the collected facts and figures in cyberspace.

Bibliography

- Techopedia. com. (2019). *What is Cyberwarfare (Cyber War)?* . [online] Available at: https://www. techopedia. com/definition/13600/cyberwarfare [Accessed 16 Jan. 2019].
- WEIMANN, G. (2005). Cyberterrorism: The Sum of All Fears?. *Studies in Conflict & Terrorism* , 28(2), pp. 129-149.
- Amadeo, K. (2019). *5 Ways Our Founding Fathers Protect The American Dream* . [online] The Balance. Available at: https://www.

thebalance. com/what-is-the-american-dream-quotes-and-history-3306009 [Accessed 16 Jan. 2019].

- https://www. researchgate. net/publication/326450147_The_War_on_Cyberterrorism
- https://en. wikipedia. org/wiki/Cyberwarfare
- African Union. (2014). African Union Convention on Cyber Security and Personal Data Protection. Retrieved 20 July 2017 from:
- https://au. int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e. pdf
- https://www. informationvine. com/index? qsrc= 999&qo= semQuery&ad= semD&o= 33784&l= sem&askid= 3286bd66-4387-4ce4-90e8-fa62c1ef6079-0-iv_gsb&q= cyber%20attacks&dqi=&am= broad&an= google_s
- https://foreignpolicy. com/2018/09/12/in-cyberwar-there-are-no-rules-cybersecurity-war-defense/
- United Nations, International Telecommunication Union. (2017). UN Resolutions Related to Cybersecurity [Website]. Retrieved 20 July 2017 from: http://www. itu. int/en/action/cybersecurity/Pages/un-resolutions. aspx
- https://littlefield. co/cyber-terrorism-understanding-and-preventing-acts-of-terror-within-our-cyber-space-26ae6d53cfbb
- https://blog. netwrix. com/2018/05/15/top-10-most-common-types-of-cyber-attacks/
- https://en. wikipedia. org/wiki/Cyberterrorism
- https://www. ncbi. nlm. nih. gov/pmc/articles/PMC5370589/

- https://www. google. com/search? ei= 7ZI_XNbMHc7LrQG5hKSADA&q= cyber+space&oq= cyber+space&gs_l= psy-ab. 3.. 0i10l10. 37430. 39760.. 40120…1. 0.. 1. 376. 1804. 0j11j0j1……0…. 1.. gws-wiz……. 0i71j0i67j0i131j0j0i131i67. q8SFO7ABN6c
- https://www. whitehouse. gov/wp-content/uploads/2018/09/National-Cyber-Strategy. pdf