

y
by Z Z

Submission date: 03-Dec-2020 08:48PM (UTC+0300)

Submission ID: 1463691917

File name: cyber_terrorism_5pgs.edited.docx (19.32K)

Word count: 1857

Character count: 10148

Cyber-Terrorism

Student

Institution

Course

Instructor

Date

Cyber-Terrorism

Cyber-terrorism is one of the criminal activities carried out using computers. Just like cybercrimes, there is no consensus on a specific meaning of the term computer-assisted terrorism. As of now, the term is described with either broad or narrow descriptions. With the broader meaning, cyber-terrorism is where terrorists' activities are executed using the internet. On the other hand, the narrow definition is where criminals use the internet to execute political aimed activities. Internet is used to either bring fear, intimidation or bring threats so that harm results. Even though many studies have been done, there is no estimate of the actual threat caused by the practice. Cyber terrorism debate has been there since the 1990s when Barry Collin coined it. In 2000 more fear and uncertainty were evident because the millennium bag issue was discussed more, and so was the higher the risks for cyber terrorists to attack the nation. The mainstream media also covered the story, claiming that the chances of terrorists using the internet to conduct their activities were higher. The literature describes cyber-terrorism, cases and law enforcement responses.

One of the aspects to assess cyber-terrorism are the types and the criminals' motivations. The Californian Center for the Study of Terrorism and Irregular Warfare says that there are three primary forms of cyber terrorism. Simple-unstructured is one type, referring to where criminals use necessary tools created by other people to target a small target (Taylor et al., 2017). In this form, much learning is not needed, and many terrorists, therefore, conduct it. Advanced-structured is the other type, where more sophisticated attacks are made, targeting several systems. Here, the terrorist organization does target analysis, applies control skills, and incorporates more learning before executing (Albahar, 2019). With the complex coordinated type, the aim is to cause mass disruptions in integrated defenses. Here, advanced technology tools are used, commands and control and take a long time as the

criminals have to be trained. Therefore, the type of cyberterrorism attack employed depends on the size of the target group, the tools used, and the learning level.

Another aspect of understanding cyberterrorism is the terrorist's motivations. These are the reasons why criminals would prefer to engage in this practice. One of the aims is to alter their rivals' functional capabilities. When the internet is used to cause harm, the costs incurred are low, but the damage done is high (Blakemore, 2016). Therefore, they use such tools to destroy their targets to make them experience problems, so they do not reach them. When terrorists succeed in this motivation, the damage is too great as it could collapse a significant economic or social aspect. For example, if the national surveillance sector is attacked, the whole nation's welfare is threatened, as fear increases, making people halt their daily activities.

Another reason cyber terrorists would prefer cyberterrorism is to destroy an organization's reputation to the public. Most of the national organizations perform well because of no known scandals. Notably, the public has become keen on companies' operations, where those with scandals are avoided. Criminals would use the internet to spread rumors and false accusations via tools such as emails and websites, leading to the spread of the wrong information to many populations (Zuberi, 2018).

Criminals also become motivated to engage in cyberterrorism to convince companies to break ties with their partners. For example, they could attack one of the partners, making the management consider not cooperating with the other to reduce chances of losses. It is challenging to execute because partners use similar information communication technologies, but it could occur. Here, the partners need to cooperate more to develop strategies to overcome the enemies as separating would imply a win to the criminals. The last reason why cyberterrorism is preferred is to show the members and the public that they have the power to meet their objectives (Shires, 2020). Thousands of recruits are acquired every year, making

the organizations have adequate human resources to execute their goals. To convince them of their power and attract new ones, they would plan a target. Besides, they could do it to prove to the public that they can perform despite the government's strict measures.

Several cases have been recorded as the worst in history regarding cyber-terrorism. The first one was recorded in 1988, conducted by Robert Morris, a student at Cornell University, United States. The learner claimed that the intention was to assess the extent of cyberspace. The plan failed because the worm developed experienced an error producing a virus which replicated infecting over 6000 computers. The affected organizations spent about 100 million dollars to recover their information. The event is an accident, but it opened criminals' eyes to conducting denial of service types of cyber terrorism.

Another incident was recorded in 2000 concerning a Canadian high schooler known as Michael Calce. He developed the DDoS attack, targeting high-profile sites such as Amazon, CNN and Yahoo (Chuiyka, 2017). He was juvenile and was therefore not imprisoned but was closely monitored by the government, especially on internet use. The incident is categorized as a cyber terrorism case as it instilled fear in the websites' users, making most of them lose personal data.

The other attack occurred in 2009 when Google's offices in China identified an attack in December. On opening, it was noticed that the criminals reached the company's corporate servers, whereby intellectual information was stolen. Investigations showed that the attack targeted the Chinese' Gmail of the leading activists. The objective had been met, as users in the United States, China and Europe had been accessed by unauthorized people (Chuiyka, 2017). The Chinese administration was blamed for allowing criminals to violate human rights on privacy, where the accusations are there to date. One year later, Google had to move its servers to Hong Kong for protection, and the strategy was revised. In 2008, another cyberterrorism case was recorded in New Jersey. A group of youths launched a DDoS

targeting the Church of Scientology, claiming to be against it. Guzner was accused of the incident and charged to pay \$37 500 for the loss made (Naik, 2017). Therefore, some attacks are conducted to explore cyberspace's extent, while others are done to alter operations.

The law enforcement department has handled the problem by blocking the servers used by the criminals. For example, in 2011, the Botnet Operation was disabled by the FBI, an international cyber fraud that infects over two million computers with software enabling them to access personal details. According to the FBI, the Botnet networks are remotely managed by the attacker, in which money and identities could be stolen, among other crimes (Stevens, 2019). In the 2011 case, a Core flood virus was used, referring to a critical logging element that allows the criminals to access personal and financial information when they cannot detect it. After the virus is introduced into the computers, the users would open the malicious emails giving the criminals the chance to control them with remote servers. If the planned botnet were deployed, the United States' economic security would be affected because most of the functions depend on information infrastructure.

Another method used by the law enforcers in preventing cyber terrorism is educating the public on preventing them. As noted in the above case, the users allow criminals to access the data because it occurs when they open malicious emails. After the Botnet attempt, information was given to the public, educating them on the measures to ensure access is not granted. Notably, the Core flood virus affects Microsoft Windows machines, and it is hard for users to detect the actions. The law enforcers said that the Microsoft Windows auto-updates should be turned on at all times (Tehrani, 2017). It would ensure that the latest security measures are put in to prevent crimes. The anti-virus programs should be up to date, and a security firewall needs to be run on computers regularly. Besides, users should check their banking and credit history from time to time to ensure they are not compromised. In case one

is compromised, the financial institution should be contacted immediately for further protective actions.

For cyber-terrorism attacks to be prevented, the government, companies and the general public need to consider it a personal issue. The administration should engage in research so that new technologies are developed that ensure information safety. Criminals try to be up to date to curb the rival's actions to fight them, as discussed above (Tehrani, 2017). It means the government has to be steps ahead of the criminals to counter their plans before damage is caused. Organizations also need to take similar actions. Instead of considering security as a burden, they should consider it a necessary measure to be integrated into the organizational culture. For example, the oil and gas industry has considered the issue personally, making cybersecurity a central part of their culture. The employees are trained to protect the companies from attacks, after which they are rewarded. Individuals and other companies need to take similar measures so that cyber terrorism in the nation is controlled.

In summation, having described cyber-terrorism, cases and law enforcement responses, it is clear that cyber terrorism is a severe problem in ¹the criminal justice system that needs to be addressed. As covered in the paper, the criminals are motivated by different aims, determining the form of attack applied. The paper has also discussed the most severe cases of cyber terrorism, indicating how much the public's confidentiality is threatened and significant losses incurred. Law enforcers have addressed the issue by halting the hackers and educating the public on the measures they should take to counter the malicious activities. Moreover, organizations and the public need to contribute to this battle by considering it a personal responsibility to counter the practices. Instead of relying on the government's actions, they should ensure that computers are updated, and unknown emails and messages are avoided. By that, the battle would be won where the expected cyber terrorism cases would be prevented.

References

- Albahar, M. (2019). Cyber attacks and terrorism: a twenty-first-century conundrum. *Science and engineering ethics*, 25(4), 993-1006.
- Blakemore, B. (2016). *Policing cyber hate, cyber threats and cyber-terrorism*. Routledge.
- Chigozie-Okwum, C. C., Michael, D. O., & Ugboaja, S. G. (2017). Computer forensics investigation; implications for improved cybersecurity in Nigeria. *AFRREV STECH: An International Journal of Science and Technology*, 6(1), 59-73.
- Chuiipka, A. (2017). The Strategies of Cyberterrorism: Is cyberterrorism an effective means of Achieving the Goals of Terrorists?.
- Naik, S. S. (2017). A Biggest Threat to India—Cyber Terrorism and Crime. *Journal of Research in Humanities and Social Science*, 5(4), 27-30.
- Shires, J. (2020). Cyber-noir: Cybersecurity and popular culture. *Contemporary Security Policy*, 41(1), 82-107.
- Stevens, T. (2019). Strategic cyberterrorism: problems of ends, ways and means. In *Handbook of Terrorism and Counter-Terrorism Post 9/11*. Edward Elgar Publishing.
- Taylor, R. W., Fritsch, E. J., Liederbach, J., Saylor, M. R., & Tafoya, W. L. (2019). *Cyber crime and cyber terrorism*. New York, NY: Pearson.
- Tehrani, P. M. (2017). *Cyberterrorism: The Legal and Enforcement Issues*. World Scientific.
- Zuberi, K. J. Z. K. J. (2018). Use of Cyber Space by Terrorist Organizations. *IJECl*, 2(1), 6-6.

ORIGINALITY REPORT

0%

SIMILARITY INDEX

0%

INTERNET SOURCES

0%

PUBLICATIONS

0%

STUDENT PAPERS

PRIMARY SOURCES

1

"The Palgrave Handbook of International
Cybercrime and Cyberdeviance", Springer
Science and Business Media LLC, 2020

Publication

<1%

Exclude quotes On

Exclude bibliography On

Exclude matches Off