A Deep Dive into the Cyber Terrorism

Ivani Patel

November 13, 2023

Story:

Cyber Security accepts a vigorous role in the area of information technology. Safeguarding the information has become an enormous problem in the current day. The cyber security the main thing that originates in mind is 'cyber crimes' which are aggregate colossally daily. Different governments and organizations are taking numerous measures to keep these cyber wrongdoings. Other than different measures cyber security is as yet a significant worry to many. We will take a deep dive on cyber security and cyber terrorism. The significant trends of cybersecurity and the consequence of cyber security will be discussed in proposed paper. The cyber-terrorism could make associations lose billions of dollars in the region of organizations. The paper will explain the components of cyber terrorism and motivation of it. Some solution about cyber security and cyber terrorism will also be provided in it.

Need:

Today an individual can receive and send any information may be video, or an email or only through the click of a button but did she/he ever ponder how safe this information transmitted to another individual strongly with no spillage of data? The proper response lies in cybersecurity. Today more than 61% of full industry exchanges are done on the internet, so this area prerequisite high quality of security for direct and best exchanges. Thus, cybersecurity has become a most recent issue. The extent of cybersecurity does not merely restrict to verifying the data in IT industry yet also to different fields like cyberspace and so forth. Improving cybersecurity and ensuring that necessary data systems are vital to each country's security and financial prosperity.

Creating the Internet safer has become to be essential to the improvement of new management just as a legislative strategy. The encounter against cybercrime needs an extensive and more secure practice. The particular estimates alone cannot keep any crime; it is essential that law authorization offices are allowable to investigation and indict cybercrime efficiently. Nowadays numerous countries and administrations are compelling strict rules on cyber safeties to keep the loss of some vital data. Each should be equipped on this cybersecurity and save themselves from these increasing cybercrimes.

Cyber-security is both about the insecurity made by and through this new space and about the practices or procedures to make it secure. It alludes to a lot of exercises and measures, both specialized and non-specialized, expected to ensure the bioelectrical condition and the information it contains and transports from all possible threats. This research aims to gather all the information and overview related to cyber-crime and provide the historical facts and perform reports on the analyzed data of different attacks reported everywhere in the last five years.

Approach:

In order to fully comprehend the dynamics of modern day cyber attacks it is important to understand the unique dimensions of the cyber space. Since the cyber space environment is not limited by any conventional boundaries or borders, clandestine cyber attacks can be carried from thousands of miles away at unbelievable speeds. Such attacks can easily be carried out by an individual or a group of individuals with computers, sitting safely in their living rooms without the need for a huge physical army on the ground. The damage from such cyber attacks can be as deadly as any conventional warfare, if not more, so the possibility of such assaults has never been as high as today. There are several aspects or factors that have contributed to the massive increase in cyber attack threats across the globe and the most prominent one is the ubiquity of the Internet. As organizations go for new software upgrades and installations new vulnerabilities and weaknesses emerge that can be exploited by cyber terrorists. The tools that are necessary to carry out an effective cyber attack can even be downloaded from the Internet and there is no need for lengthy and expensive acquisitions and training. It is not

wrong to comment that today a simple personal computer can actually be used as a more effective weapon than a conventional gun. A terrorist organization with limited manpower and infrastructure can launch cyber attacks from any location and can cause massive loss, be it infrastructure, finance or human life. James Lewis from the Center for Strategic and International Studies appropriately defines the threat of cyber attacks in the twenty-first century as "a massive electronic Achilles' heel". In order to properly understand the dynamics of cyber attacks and cyber terrorism it is important that the reasons behind their popularity among the terrorists are thoroughly comprehended. Cyber attacks can cause extensive damage at tremendous speeds and in little time. In essence, the outreach of such attacks is massive and the level of publicity that an organization mounting such an attack is enormous. Given the extensive dependence on information technology today, legitimate organizations also bend under a constant fear of becoming the target of malicious agents. All of these make the paradigm of cyber attacks extremely attractive for terrorists. The popular culture has also contributed immensely in creating the paranoia surrounding cyber attacks where scenarios such as terrorists taking control of the air space and nuclear installations and wreaking havoc on millions are routinely publicized and narrated. It will also be prudent to ascertain if the threat of cyber attacks is as real and imminent as is projected by the print and electronic media. As Weimann puts it, virtually every major government, defence and private infrastructure in the west are highly networked and depend heavily on computers. Even though this makes operations extremely smooth and agile the possibility of cyber attacks also increases many fold. Terrorist organizations can exploit the loopholes in the network and can launch massive attacks on financial and military installations and can hold an entire nation to ransom.

While information technology has significantly improved the quality of life, the tradeoff comes in the form of the increasing vulnerability of major installations to such attacks. These observations clearly establish that the perceived levels of threat surrounding cyber attacks are not unfounded and there is a clear necessity for robust policies to ensure that such attacks never happen. This paper will attempt to present an insight surrounding the possibility of cyber attacks in the present day and in the future and will thoroughly examine the different aspects and dynamics of cyber attacks and cyber terrorism.

Milestone 1 will provide topic discussion which will indicate why cyber security a major concern for nations across the globe. And different aspects of cyber attacks and explored the reasons behind their increasing popularity among the terrorist organizations and state players.

Milestone 2 will provide an empirical model that can be used to estimate the risk levels associated with different types of cyber attacks will provide a road map to conceptualize and formulate highly effective counter measures and cyber security policies. (with 6-7 page rough draft)

Milestone 3 will provide final draft of paper and presentation.

Benefit:

This paper will help to advance the scientific interests in the exploration of cybersecurity, particularly to respond to the procedural questions of the prediction of future data and actions significant to security patterns. This study will set the background to begin executing rules for all intentions as indicated through the usual security issues and answers for data systems. And will focus on the dynamics of cyber attacks and cyber terrorism and highlight the ever-growing possibility of cyber warfare in recent times. With the human race becoming more and more dependent on technology and computers becoming ubiquitous in people's lives, the scope of exploiting the cyber space to compromise the security of an organization or an entire nation is growing rapidly.

Over the next five years, cyber-crime may create severe damage in information technology. According to the researchers they have estimated an approximate close to 6 trillion dollars loss. So, there would be a very bright scope for people who work and resolve the issues related to cyber-crime and provide all the necessary security measures. Big organizations like CISCO which is completely related to networking technology which is one of the top organization has approximately millions of openings related to cybersecurity because which is the future for the safety of Information technology. They are also wide opportunities in government-related fields and also defence field to save the countries secure data from cyber attackers.

Summary:

Based on the analyzed information, I would like to provide all the countermeasures that organizations may undertake in order to ensure improved security that would support in defending the organizations from being attacked by the hackers and provide a cyber-security to avoid all risks.

If technology can take us to the moon, a breakdown or compromise of the same will ensure that we stay there forever and never return. In essence, when gains are huge the losses can be equally big and when seen in this context a more resurgent and robust cyber security policy appears absolutely logical and necessary.

References

[1] Kumar, S., Somani, V. (2018). Social Media Security Risks, Cyber Threats And Risks Prevention And Mitigation Techniques. International Journal of Advance Research in Computer Science and Management, 4(4), pp. 125-129.

[2] Sutton, D. (2017). Cyber Security: A Practitioner's Guide. Swindon, UK: BCS, the Chartered Institute for IT.

[3] Herzog, S. (2011). Revisiting the Estonian cyber attacks: Digital threats and multinational responses. Journal of Strategic Security, 4(2), 49–60.

[4] Rid, T., McBurney, P. (2012). Cyber-weapons. The RUSI Journal, 157(1), 613.

[5] Gross, M. L., Canetti, D., Vashdi, D. R. (2017). Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes. Journal of Cybersecurity, 3(1), 49–58. doi:10.1093/cybsec/tyw018

[6] Gade, N. R., Reddy, U. G. (2014). A Study Of Cyber Security Challenges And Its Emerging Trends On Latest Technologies. Retrieved from

https://www.researchgate.net/publication/260126665_A_Study_Of_Cyber_Security_Challenges_And_Its_Emerging_Trends_On_Latest_Technologies

[7] Hua, J., Bapna, S. (2013). The economic impact of cyber terrorism. The Journal of Strategic Information Systems, 22(2), pp. 175-186

[8] Samuel, K. O., Osman, W. R. (2014). Cyber Terrorism Attack of The Contemporary Information Technology Age: Issues, Consequences and Panacea. International Journal of Computer Science and Mobile Computing, 3(5), pp. 1082-1090.

[9] Panchanatham, D. N. (2015). A case study on Cyber Security in E-Governance. International Research Journal of Engineering and Technology.

[10] Weimann, G. (2005). Cyberterrorism: The sum of all fears? Studies in Conflict Terrorism, 28(2),129–149

[11] Wilson, C. (2003). Computer attack and cyberterrorism: Vulnerabilities and policy issues for congress.Washington, DC: Congressional Research Service.