OPEN ACCESS Freely available online

International Journal of Advancements in Technology

Commentary

Brief Note on the Cyberterrorism Technology

Poong Hyun Seong*

Nuclear and Human Fctors Engineering, Korea Advanced Institute of Science and Technology, Daejeon, South Korea

DESCRIPTION

For several years, experts and government officials have warned of cyber terrorism as an imminent threat to national security. However, if we define cyber terrorism as an attack or series of attacks by terrorists with political, religious or ideological motives that instill fear through destructive or disruptive, both of these are recent cyber events. This white paper analyzes US cyber terrorism discourse from a constructive perspective in security research, rather than trying to answer periods when cyberterrorism is likely to remain a fictitious scenario. A method and speculation about the characteristics that cause the rapid and significant political impact of the broad conceptualization of the aspects of information technology as a security issue in the 1990s.

The study of cyber terrorism remains quite anecdotal, as known cases of cyberattacks against sovereign power are rare. The terrorist discourse itself remains unclear, as there is little consensus on the thresholds that clearly distinguish between crime and terrorist attacks. This article explores a combination of cyber terrorism that emphasizes symbolism and public opinion and distinguishes between real and perceived threats. An objective analysis of historical events will show that the adaptive techniques and sophistication of first world forces provided adequate protection against the "Cybergedon". But this reality must be in contrast to recalled by mainstream media regarding the digital end of the world. In examining this dichotomy between real and perceived threats, we explore the idea that the current direction of cyber law could increase international inequality. As the world shifts to more cyber dependence, the dominant economies have the opportunity to become more inclusive in working towards global law enforcement. This article calls for attention to social justice to mitigate public fears associated with cyber threats.

Technology is strategic in promoting the use of the internet by terrorist organizations and their supporters for a variety of purposes, including recruitment, financing, advertising, training, incitement to acts of terrorism, and the collection and dissemination of information for terrorist purposes. It is one of the factors. While the many benefits of the internet are obvious, it can also be used to facilitate communication within terrorist organizations and to send information and important support about planned terrorist acts. All of these require specific technical knowledge to effectively investigate these crimes.

Much has been said about the threat of cyberterrorism since the 1990s marsh commission report. However, current analysis only identifies the abundance of vulnerabilities in automated information systems (computers), and assumes that terrorist organizations are ready to exploit these vulnerabilities. They perform a basic strategic analysis and conclude that cyber terrorism is inevitable because it gives terrorists a potential strategic advantage over the United States. We do not deny the fact that our vulnerabilities are real and numerous. In addition, if the event occurs in the manner described in some scenarios, the consequences of the abuse are serious and can be strategically debilitating. However, based on our research, we do not believe that terrorist organizations will soon have access to the features described in many of these scenarios. According to many analyses, the tools needed to exploit infrastructure vulnerabilities are readily available and soaring at an alarming rate. Still, the United States has never seen a strategic attack on critical infrastructure by a terrorist organization (or any other organization). Even during the Kosovo conflict, the most serious "attacks" were website destruction and denial of service attacks on email servers. This is not enough for these tools to be used for large-scale confusion purposes, and there are requirements for effective use, not just wanting to own and harm these tools. Simply offsetting development costs is just one of several challenges that need to be taken into account. Terrorist organizations may measure the benefits of pursuing cyber-terrorism in terms of both internal and external incentives. In addition to development costs, internal incentives should also include the psychological processes of individuals and groups that have a significant impact on terrorist organizations. In terms of external interests, the cost of pursuing cyberterrorism may never be attractive as long as traditional terrorist methods are feasible. We examined the issue of cyberterrorism from the perspective of an organization seeking a comprehensive assessment of its activities. Our assessment examines the costs, risks, and benefits of deploying cyberterrorism as a stand-alone operation or as a complement to traditional counterterrorism operations.

Correspondence to: Poong Hyun Seong, Nuclear and human factors engineering, Korea Advanced Institute of Science and Technology, Daejeon, South Korea, Tel/Fax: +44 (0)300 019 6175; E-mail: phseoghyun@kist.ac.kr

Received: 26-May-2022, Manuscript No. IJOAT-22-18017; Editor assigned: 01-Jun-2022, Pre Qc No. IJOAT-22-18017 (PQ); Reviewed: 15-Jun-2022; Qc No. IJOAT-22-18017 Revised: 22-Jun-2022, Manuscript No. IJOAT-22-18017 (R); Published: 29-Jun -2022, DOI: 10.35248/ 0976-4860.22.13.186.

Citation: Seong PH (2022) Short Note on Computer Hacking and Cyber Terrorism. Int J Adv Technol. 13:186.