OPEN ACCESS Freely available online

International Journal of Advancements in Technology

Commentary

Short Note on Computer Hacking and Cyber Terrorism

Poong Hyun Seong*

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

DESCRIPTION

We live in a society that is becoming heavily reliant on information technology as the new millennium approaches. While technology has many advantages, it also creates new flaws that can be exploited by those with the proper technical capabilities. Hackers are a well-known threat in this regard, and they are responsible for a large amount of information system interruption and damage. They aren't, however, the only culture of violence that needs to be considered. Technology is increasingly being considered as a possible tool for terrorist organizations, according to evidence. As a consequence, a new threat has emerged in the shape of "cyber terrorists," who target technology infrastructures like the Internet in order that would further their purpose. This commentary describes the issues raised by these groups and considers the types of response needed to ensure the future security of our society.

Computerization and digitalization began to affect a growing number of aspects of state and society operations and activities. Despite the great benefits of the foregoing, the procedures that were launched resulted in major threats. Initially, they were one-off attacks carried out by individuals for whom hacking was a pastime. However, the nature of that activity has evolved over time. Hackers began to organize themselves into independent groups around the turn of the century, with state governments increasingly supporting them. The previously trivial acts of hacking into computer networks turned into coordinated actions by groups of programmers collaborating with secret agencies with the goal of gaining a specific political, economic, or military advantage. Furthermore, types of hackers were increasingly focusing on servers and networks essential to the functioning of governmental entities, rather than just websites. As a result, at the dawn of the 21st century, cyberspace became a hotbed of activity that jeopardized not just the security of secret data but also the operation of essential infrastructure. As a result, at the turn of the first and second decades of the twenty-first century, it is worthwhile to evaluate the actions taken by nations and international organizations to adjust to the new security scenario.

The term "hacker" was coined in the computer world to describe people with a basic understanding of the technology and the ability to create technically elegant software solutions. However, over decades, the meaning of the phrase has evolved, and it is now widely understood to refer to anyone who purposefully gain (or attempt to gain) illegal access to computer systems. Hackers are not a new menace; in fact, they have frequently appeared in news articles during the last two decades.

Hobbyists who created computer viruses were the first to pose a threat. The number of hacking assaults on computer networks and government entities increased in the second half of the 1990s. Individual hackers as well as organized crime organizations have carried out hacking attacks. States began to utilize cyberspace in the first decade of the 21st century. Hacking groups hired by governments to complete certain tasks on the Internet began to play a unique role. Terrorist-type organizations have made extensive use of information technology in recent years. This has resulted in the rise of a new type of threat known as "cyber terrorism." Because physical terror is not involved, this can be distinguished from 'conventional' terrorism. This differs from 'conventional' terrorism in that there is no physical terror involved, and instead the focus is on assaulting information systems and resources. Terrorist and insurgent groups have long struggled to communicate their political beliefs to the wider public without being banned. They can now, however, use the Internet for this purpose. The Irish Republican Information (IRI) service is one example of where this is already the case. Terrorists will utilize more advanced encryption methods and improved anonymous electronic re-mailers to create a command system that is impossible to break and allows for group control anywhere on the planet. This is an issue for security services since it means they will have to devote more time and money to decrypting electronic messages.

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: 02-Feb-2022, Manuscript No. IJOAT-22-17091; **Editor assigned:** 07-Feb-2022, Pre Qc No. IJAOT-22-17091 (PQ); **Reviewed:** 21-Feb-2022, Qc No. IJOAT-22-17091; **Revised:** 24-Feb-2022, Manuscript No. IJOAT-22-17091 (R); **Published:** 03-Mar-2022, DOI: 10.35248/0976-4860.22.13.178.

Citation: Seong PH (2022) Short Note on Computer Hacking and Cyber Terrorism. Int J Adv Technol. 13:178.