Chapter 4
Virtual Threats and Asymmetric Military Challenges

C. V. Suresh Babu
https://orcid.org/0000-0002-8474-2882
Hindustan Institute of Technology and Science, India

P. M. Akshara
Hindustan Institute of Technology and Science, India

ABSTRACT

Security challenges are faced by every single country on this planet. These threats can occur through violent non-state habitats, any organized group of criminals, economic threats, disasters, or native citizens. In ancient wars, nations used physical forces and weapons as a tool to acquire regions, resources. Whereas, in the future, a wide range of technologies like automated weapons, drones, and cyber warfare may come into action. A single person can control an army of computers, and the person behind the actions can go unidentified. The surging need for the use of computers has greatly imposed an effect on the military. Unlike traditional warfare, where large mobilizations of military forces were involved, in modern warfare, integration with latest innovations in military forces like guided munition systems, explosives, and nuclear weapons are brought into use. As a result, there rises an inevitable need to acquire insight into the field of cyber military technology. This chapter mainly aims to analyse the nation's virtual threats and asymmetric military challenges.

INTRODUCTION

Cyberattacks on military networks and their systems are referred to as virtual military threats. These evil attacks are imposed by hackers, hacktivists, terrorists, or opponent countries. Threats may consists of phishing attacks, malware infections, denial of service attacks and data theft. Virtual threats may highly harm a nation's military operations by threatening the confidentiality, integrity and availability of sensitive information and infrastructure. Countries undergo various security issues. It may be both in the real world and the virtual world. Off late attacking through virtual world is exponentially increasing.

DOI: 10.4018/978-1-6684-8846-1.ch004

The evolving crisis is that every gadget can turn into a weapon on a virtual battlefield for which the loss may be felt in the real world. Virtual threats to the military may include stealing sensitive information from the system by introducing malicious code and phishing techniques etc., dignitaries can be compromised to reveal confidential information to unauthorized parties, supply chain attacks, and IoT attacks (Suresh Babu, 2023).

To bring about a change in the prevailing unsecured system, blockchain technology can be merged with military forces like ammunition, and nuclear weapons, and bringing the entire network under blockchain can make things more secure. By applying blockchain in supply chain systems, ammunition can be tracked and information like production date, manufacturing location and storage location could be managed and recorded securely in such a way thereby making it hard for the attackers to sniff the data.

Secondly, the proliferation of nuclear weapons along with terrorism and computer technologies increasingly leads to the risk of virtual threats. Blockchain when integrated with nuclear weapon technology can bring about a solution to this problem. This chapter will provide suggestions and techniques to put a stop to the virtual threats through blockchain technology.

In today's world, employment of big armaments and ammunition for wars are outdated strategies to conquer one's nation. Cyberwarfare is the developing trend where every computer under the internet becomes a weapon. So there arises an urge for the government to protect each and every device from the attackers. Cyber-attacks on military systems can affect seriously on weapon systems, disrupt communication routes, and steal confidential data. Military enterprises must do the needful cybersecurity measures which includes firewalls, intrusion detection systems, and encryption protocols to guard against asymmetrical and virtual military attacks (Suresh Babu & Srisakthi, 2023). Cyber hygiene training for employees can also help to reduce the risk of invasions. Defined practises must be created in order to minimise damage and swiftly restore activities following a cyber-attack. As days move by there is an increasing need for military to invoke technologies like artificial intelligence, blockchain technology and internet of things etc. Invocation of blockchain technologies in military programme can build meticulously secure environment.

RATIONALE BACKGROUND

A military system without threats is ideal, but it is unlikely to be achieved due to the constant evolution and adaptation of cyber threats. However, if we make the assumption that a military system is completely immune to cyberattacks, it would look very different from the military systems we currently have. In a system free from cyber threats, military organisations could confidently share and access sensitive information across numerous networks without worrying about unauthorised access or data breaches. This might lead to a more collaborative and successful military where commanders seek for accurate and perfect facts to make wise decisions. Military systems wouldn't need regular cybersecurity updates or ongoing cyberattack monitoring if there were no cyberthreats. This might really free up resources and labour to focus on other fundamental military operations. It's crucial to remember that this perfect situation is unlikely to occur in reality but Military systems need to be created to resist and adapt to cyberthreats since they will never go away. This study provides a more practical methodology can be improved the network safety posture of military frameworks, utilising the most recent innovations and best practises to reduce the risks of digital hazards.