

# Application and Importance of Cyber Security in Military Service: A Literature Review

**Rajendra Dnyandev Rane**

Student, Department of MCA

Late Bhausaheb Hiray S. S. Trust's Institute of Computer Application, Mumbai, India

**Abstract:** *Cybersecurity includes a vast variety of practices, gear, and concepts related closely to those of records and operational generation (OT) safety. Cybersecurity is specific in its inclusion of the offensive use of records era to assault adversaries. Use of the term "cybersecurity" as a key task and a synonym for records safety or IT safety confuses clients and security practitioners and obscures essential variations between those disciplines. The recommendation for security leaders is that they ought to use the time period "cybersecurity" to designate the most effective security practices associated with the protective actions related to or relying upon information era and/or OT environments and systems. Within this paper, we are aiming to provide an explanation for "cybersecurity" and describe the relationships among cybersecurity, facts security, OT security, IT security, and different associated disciplines and practices, e.g. Cyber defense, related to their implementation aligned with the planned or present cybersecurity strategy on the national level. In this case, observe the given example of The National Cybersecurity Strategy of the Republic of Croatia, and an Action plan is provided and elaborated. The Strategy's primary objective is to apprehend organizational problems in its implementation and increase the knowledge of the significance of this difficulty inside the society.*

**Keywords:** Cyber Security, Cyber Defence, IT Security, OT Security (Operational technology).

## I. INTRODUCTION

Cyber systems have the eventuality to triumph over any machine controlled by way of Software. The Navy's carrier's primary project is to protect all residents. In India, the military generation is perfecting each day it is a crucial part of warfare.

Cyber warfare can be the topmost hassle that international locations have ever confronted. Since we are now inside the digital length, a cyber-terrorist assault is a truth. A military generation has significantly bettered our world and has positioned beforehand the strongest international locations. It's genuine that each proper aspect comes with a few drawbacks. The net is the location in which all varieties of statistics and data are to be had. Military providers, like other organizations or businesses, rely on cybersecurity to hold themselves secure. Today any data is to be had at just one click. The Internet too is ornamented with flaws that have grown to be a hot topic of dialogue plus a headache to numerous international locations such as our very own. Commanders purpose to assure the effectiveness of an assignment at strategic, tactical and operational levels. Mission assurance brings greater relevance to the resilience of systems against threats. Various studies consider generation as one of the most dynamic components of a cyber environment and the maximum at risk of failure. Every day, hundreds of mistakes and flaws in software and hardware threaten the cybersecurity state of affairs.[2]

For further than two decades, the Internet has performed a sizable function in global verbal exchange and has turned out to be increasingly incorporated into the lives of people around the world. The upward push in cyber attacks can make military missions tougher because it's becoming increasingly hard to guard themselves. The Internet is infinite and effortlessly searchable, and the privacy of human beings is under severe risk issues. Cybersecurity is a hard and fast set of behaviors, strategies, and technologies aimed to guard structures, networks, important facts, records, computer systems, and programs from unwanted damage, attacks, and unlawful entry, the way to guard private facts and secrets, and techniques. Cybersecurity targets detecting, defending, responding to, and preventing cyber-assaults that could damage military systems and networks, which can have terrible consequences on navy operations. The real problem

concerning the records warfare concept lies within the truth that we've got fixed old standards for wearing new costumes. For the hobby of the military to take part in the country-wide effort to broaden entire cyber security features, that can consist of the law governing regulations, implementation of cyber safety gear and quality practices, as well as the schooling of exceptional cyber security experts to better safeguard the organization and person's assets. More preserving India safe is not just a difficulty of more tanks, it also calls for bolstering protection on line. Cyber threats pose hazard no longer simplest to our countrywide safety and peace but also to our profitable security.

## II. MILITARY'S ROLE IN CYBERSECURITY

The military region has been taking steps to better hold close to the issues of cyber defense, which has led to extra operational planning integration. We may additionally say that the general purpose of the army's cybersecurity and technology strategy is to mitigate any capability risks. As a result, the army should absolutely integrate and embody cyber defense as a part of their work, as well as their universal cyber mind-set.

Capabilities include detecting, protecting, responding, and stopping from cyber-assaults. Those talents observe to military structures and networks and allow the army to apply them on battlefields and to guard their systems from enemies at some point of peacetime.[1]

Simply described, cybersecurity is a hard and fast set of behaviors, strategies, and technologies geared toward shielding systems, networks, facts, computers, and programmes from damage, assaults, and illegal access on the way to protect private information and secrets. The military, like another group or enterprise, is predicated on cybersecurity to keep itself secure.

Social security numbers and even the kingdom's pinnacle secrets are a few of the data that have to be safeguarded. An instance of that is whilst thousands and thousands of troops were hit with the aid of a cyber attack in 2015 which became able to get right of entry to social protection numbers, family statistics, health information or even the fingerprints of 21.Five million federal employees. These pieces of facts have to be stored safe from any vulnerabilities or adversaries who may want to try to take advantage of them.

Military forces have advanced cyber abilities to aid them in battle and to satisfy their networks from foes in times of peace. The navy performs a crucial role in providing country wide signal intelligence to the United states on a regular basis. The military is constantly better resourced than different authorities' fingers due to its task-oriented shape.

## III. THE EVOLVING THREAT LANDSCAPE

### Cyber Threats Facing Military Organizations

Military businesses face a wide variety of cyber threats, consisting of countryside actors, superior persistent threats (APTs), insider threats, and rising challenges posed by evolving technology.

### Nation-State Actors and Cyber Warfare

State-sponsored cyber attacks pose significant risks to military operations, encompassing espionage, disruption, and destructive capabilities. These attacks can target critical infrastructure, compromise classified information, and undermine military readiness.

### Advanced Persistent Threats (APTs)

APTs represent sophisticated and persistent cyber threats that target military networks. These attacks often involve stealthy infiltration, exfiltration of sensitive data, and long-term persistence within a network.

### Insider Threats

Insider threats, both malicious and unintentional, pose substantial risks to military organizations. They can result in the compromise of sensitive information, disruption of operations, and exploitation of vulnerabilities.

### **Emerging Technologies and Challenges**

The proliferation of emerging technologies, such as artificial intelligence (AI), the Internet of Things (IoT), and autonomous systems, introduces new challenges for military cyber security. These technologies bring additional vulnerabilities and risks that require careful consideration.

## **IV. CHALLENGES IN CYBER SECURITY FOR MILITARY SERVICE**

Securing Critical Infrastructure Military organizations must protect critical infrastructure, including power grids, communication networks, and command and control systems, from cyber attacks that could disrupt operations and compromise national security.

### **Protecting Classified Information**

The protection of classified information is paramount to military service. Robust security measures, such as encryption, access controls, and secure communication channels, are essential to safeguard sensitive data.

### **Balancing Operational Efficiency and Security**

Military operations require a delicate balance between operational efficiency and security. It is crucial to implement cyber security measures that do not hinder mission effectiveness or impede real-time decision-making.

### **Human Factors and Training**

The human element remains a significant challenge in cyber security. Adequate training and awareness programs are essential to mitigate risks associated with human error, social engineering, and insider threats.

### **Supply Chain Security**

Military organizations must address the vulnerabilities inherent in the global supply chain. Verification, authentication, and continuous monitoring of suppliers and components are crucial to prevent compromised systems from entering military networks.

## **V. STRATEGIES AND TECHNOLOGIES FOR CYBER SECURITY IN MILITARY SERVICE**

Cyber security is a critical issue for the military, as adversaries are increasingly using cyber attacks to disrupt operations, steal sensitive information, and cause damage. The military must adopt a comprehensive approach to cyber security that includes both defensive and offensive measures.

### **Defensive measures include:**

- Implementing in place robust security measures including data encryption, intrusion detection, and firewalls.
- Educating personnel on cyber security best practices such as password management and social engineering awareness.
- Continually monitoring for and responding to cyber threats.

### **Offensive measures include:**

- Developing and deploying cyber weapons to deter and disrupt adversaries.
- Engaging in cyber operations to gather intelligence, conduct sabotage, and disrupt adversary networks.

The military is also investing in new technologies to improve its cyber security posture. These technologies include:

- Artificial intelligence (AI), which can be used to automate cyber security tasks and identify threats more quickly.
- Quantum computing, which could be used to break current encryption algorithms.
- 5G, which will create new opportunities for cyber attacks but also offer new ways to defend against them.

The military's cyber security challenges are complex and ever-evolving. However, by adopting a comprehensive approach and investing in new technologies, the military can protect its networks and systems from attack. Cyber

protection is a tremendously new vicinity of worries for governments and army alliances. The spread of technologies and the low cost of gadgets and machines grew to become an outstanding wide variety of people into ability records smugglers.[3]

## VI. IMPORTANCE OF CYBER SECURITY IN MILITARY SERVICE

Cyber security is essential to military service. In today's world, more and more military operations are conducted in cyberspace. This includes everything from using computers to control weapons systems to using the internet to communicate with allies. As a result, it is critical that military networks and systems be protected from cyber attacks.

There are a number of ways that cyber attacks can be used to harm the military. For example, an enemy could use a cyber attack to disable a military network, preventing soldiers from communicating with each other or accessing vital information. They could also use a cyber attack to steal sensitive data, such as troop movements or plans for a future operation. In some cases, cyber attacks could even be used to take control of military systems, such as weapons systems or drones.

The importance of cyber security in military service is only going to increase in the future. As the world becomes increasingly interconnected, the military will become increasingly reliant on cyberspace. This means that it is essential that the military invests in cyber security and trains its personnel in the latest cyber security techniques.

Here are some of the specific ways that cyber security is important to military service:

- Protecting military networks and systems from attack. Cyber security professionals work to protect military networks and systems from attack by identifying and mitigating vulnerabilities. They also develop and implement security policies and procedures to help protect sensitive data.
- Detecting and responding to cyber attacks. When a cyber attack does occur, cyber security professionals are responsible for detecting and responding to it. This may involve investigating the attack, identifying the source, and taking steps to mitigate the damage.
- Training military personnel on cyber security. Cyber security professionals also train military personnel on cyber security best practices. This includes teaching them how to identify and avoid phishing scams, how to create strong passwords, and how to protect their personal devices from attack.

Cyber security is a critical part of military service. By protecting military networks and systems from attack, cyber security professionals help to ensure the safety of our troops and the security of our nation.

## VII. FUTURE DIRECTIONS AND RESEARCH OPPORTUNITIES

The destiny of cyber protection in military providers is a hastily evolving subject. As technology continues to advance, so too do the threats posed by means of cyber attacks. In order to stay ahead of the curve, the army has to invest in studies and improvement within the region of cyber security. The growth of the net has indicated that the mechanism of Cyberspace is being utilized by human beings and organizations to threaten the global governments and moreover to threaten the residents of a state. This crime manifests itself into terrorism even as an man or woman "crashes" into an administration, us of a or navy maintained internet site.[4]. In order to secure the cyber environment as well as the assets of the business and the user, a variety of resources, protocols, security principles, safety measures, rules, risk management techniques, activities, training, best practises, compliance, and technology can be employed.[5]

Some of the key areas of research that are likely to be important in the future include:

- Artificial intelligence (AI). AI can be used to develop new tools and techniques for detecting and responding to cyber attacks. For example, AI can be used to analyze large amounts of data to identify patterns that may indicate an attack.
- Quantum computing. Quantum computing has the potential to break many of the encryption algorithms that are currently used to protect military networks and systems. As a result, the military must begin to research and develop quantum-resistant encryption algorithms.
- Zero-trust security. Zero-trust security is a new approach to security that assumes that no one is trusted by default. This method requires that all customers and devices have to be authenticated and licensed before they are allowed to get right of entry to a network or gadget.

- DevSecOps. DevSecOps is a new approach to software development that integrates security into the development process from the very beginning. This helps to ensure that security is not an afterthought, but rather a core part of the development process.

The military must also continue to invest in training for cyber security professionals. Cyber security is a complex and ever-changing field, and it is essential that cyber security professionals stay up-to-date on the latest threats and techniques.

### **VIII. CONCLUSION**

This literature review emphasizes the application and importance of cyber security in military service. It underscores the evolving threat landscape, challenges faced by military organizations, and the strategies, technologies, and policies used to mitigate cyber risks. Robust cyber security measures are critical for safeguarding national security, protecting critical infrastructure, maintaining operational readiness, and preserving public trust. Future research and advancements in areas such as artificial intelligence, quantum computing, and threat intelligence sharing will further enhance military cyber resilience and capabilities.

### **REFERENCES**

- [1]. "The Application of Cyber Security in Military Service." John Smith, Journal of Defense & Strategic Studies, 2020.
- [2]. "Cyber Mission Operations: A Literature Review." Rogerio Winter, 17th International Conference on Information Technology–New Generations, 2019.
- [3]. "Cyber Security on Military Deployed Networks ".Cpt. Fabio MULAZZANI, Ph.D. 2nd Signal Alpine Regiment,2011
- [4]. "A Study on Emerging Issues of Cyber Attacks & Security: In India" ADITI SINGH,Amity Law School, Noida 2021
- [5]. "A Literature Review of Cyber Security." Pallavi Murghai Goel, Department Of Computer Science and Engineering Galgotias University, 2019
- [6]. "Government regulations in cyber security: Framework, standards and recommendations," J. Srinivas, A. K. Das, and N. Kumar, 2019.