International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

India's Framework for Cyber Security Since 2014 and its Significance for Armed Forces

Nikhat Parveen

Research Scholar, Department of Political Science. Patna University, Patna

ABSTRACT:

The character of warfare changes with the change in its nature. In the last two decades, cyberattacks have expanded in their dimensions with the advent of digital networking in the military sector. Cyber security occupies a significant position in the Indian armed forces because of the increasing threat of cyberattacks from hostile neighbouring countries, particularly China and Pakistan. Cyber threat undermines military preparedness and warfighting capabilities by infiltrating critical weapon systems, vital infrastructure, crucial communication networks, and Intelligence, Surveillance, and reconnaissance (ISR) systems. India is now concentrating on framing its cyber security policy to mitigate the cyber threat and enhance the cyber capabilities of its armed forces. With its cyber security policy, India aspires to make digital armed forces.

The present research article will focus on the efforts the Indian government has taken since 2014 to neutralize cyberattacks and the policies it has framed to ensure cyber security. The article will also analyze the significance of the government efforts on the armed forces in the direction of defensive cyber policy.

Keywords: Armed Forces, China, Cyber Security, Cyber Attack, Digital Armed Forces.

TERMINOLOGY:

Cyber security can be expressed as a strategy to protect hardware, and software connected to the internet from cyber threats. It is a practice used by individuals and organizations to safeguard data, hardware, and software from unauthorized access and malicious attacks such as deleting, destroying, or extorting the user's system and sensitive data. Cyber security is an attempt to disable and disrupt the attacks.[1] Individually, cyber means technology and security refers to protection. Combining the two terms cybersecurity can be defined as the tools or procedures intended to defend networks, devices, data, and programs from intrusion, loss, or any other threats. Cyber security is a tactic to protect vulnerable data from the malicious intent of the enemy. Cybersecurity is occasionally referred to by different terms such as electronic information security or information technology security.[2]

INTRODUCTION:

In the era of technology, the internet is one of the significant inventions. In the 21st century, the internet has become part and parcel of every activity of people's life. Every sector i.e. banking, healthcare, financial institutions, government institutions, defence, manufacturing industries, etc. is now affected by the Internet. However, the advantages of the Internet are accompanied by certain threats. The introduction of the Internet has led to an increment in computer attacks. According to a report, about 25 computers are

targeted by cyberattacks every second. The Computer Emergency Research Team (CERT) in its reports has mentioned that between 2011 and 2013 around 308371 Indian websites were hacked.[3] Every year the cases of cyberattacks are increasing. India has experienced a 15 percent surge in cyberattacks since 2022.[4] The defence sector is also not aloof from the cyberattack. The defence sector is a frequent target of the cyberattack. The priority of the Armed Forces is to ensure the security of its nations and citizens. The rise of cyber-attacks has imposed a new challenge in front of the Indian armed forces. The defence sector is entrusted with planning and implementing the plans required to protect the country's border from external and internal threats. With the advancement of technology in the defence industry the military operations and management of national security have been redefined. Now countries are making use of Artificial intelligence, drones, robotics, laser weapons, CCTV, Sensor systems, and virtual reality to defend their territory or to attack their enemies.[5] However, the growing reliance on technology and the internet have made the defence sector more prone to cyberattacks. Therefore, cyberattacks in the contemporary period are both national and international concerns.

Indian military faces threats from its neighbouring countries, particularly from China and Pakistan. The Indian Armed Forces are frequently involved in direct clashes with China and Pakistan over issues like Jammu & Kashmir, Water Sharing (with Pakistan); Arunachal Pradesh, Tibet, Dokalm, and Galwan Valley (with China), etc. China and Pakistan always try to debilitate and sabotage India by covert infiltration, psychological tactics, traditional and non-traditional techniques, hybrid manoeuvers, etc.[6] Notably in the present day, both countries have started cyberwarfare with India. Specifically, China with its cyberwarfare technique tries to degrade the military readiness of the Indian armed forces and wreak havoc on the ability to mobilise for battle. Indian critical infrastructure such as atomic energy, space, and power sectors have been the prey of cyberattacks from China. During the Galwan Valley clash in 2020, China made massive cyberattacks on India. According to a news report China launched about 40, 300 cyberattacks in the Indian cyberspace. Over the last two decades, China has been capable of repeatedly attacking government ministries like the Ministry of Defence, Defence Research and Development Organisation (DRDO), Bhabha Atomic Research Centre (BARC), Ministry of Home Affairs (MHA), etc.[7] This has necessitated India to reassess its efforts to advance its armed forces in the twenty-first century, more specifically bolstering capacities against cyber threats.

OBJECTIVES:

The objective of the research paper is: to examine cyberattacks in the field of defence; to study Indian government initiatives and policies since 2014 to regulate cyberattacks in defence sector; and to assess the significance of cyber security policies for the Indian Armed forces.

INDIA'S FRAMEWORK FOR CYBER SECURITY:

The perpetual advancement of technology has resulted in the emergence of cyberspace warfare. Cyberattacks have been a key element in the military sector because of the introduction of advanced technology. The global military, including the Indian military, is increasingly focusing on network-centric warfare. The linkage of the Internet of Things (IoT), Artificial Intelligence, and Automation with the military industry improves battlefield readiness. Due to the proliferation of linked devices, military networks are especially susceptible to cyberattacks. Hackers sabotage the enemy country's weaponry, computer, and software programs through cyberattacks. The hacker country uses malware and viruses to infiltrate the computer and weapon systems, which causes missiles to self-destruct, disable defense

mechanisms, or entirely take control of potent ground vehicles, naval platforms, radar mechanisms, etc. Most significantly the rise of Artificial Intelligence in the military has posed a crucial cyberattack threat to military developments. As per the research of 'Recorded Future', an American cybersecurity company, China-backed hackers consistently target Indian defence research. In the report of January 2023, a cyberattack was made on the Nagpur defence industry.[8]

Since the Indo-China war of 1962, India has emphasized on military modernisation by developing of new weapon systems, establishing of vital infrastructure, and improving ISR (Intelligence, Surveillance and Reconnaissance) system.

As national security is the prime concern of the government, the defence sector has become an important area of focus. Within defence sector, the Signal Corps is the nodal branch that works on telecommunication and cyber security. It traces its origin to the British period. Over the years it has evolved with the change in modern communication technology. Initially, its work was focused on electronic surveillance and countermeasures. In the contemporary period, it functions in the direction of cyber security and defending the armed forces from cyber threats. Since 2014, the government has been promoting 'Atmanirbharta' in the defence sector, working on robust cybersecurity measures. India since 2014, has been using defensive and offensive mechanisms to leverage military cyber security. India developed its cyber security policy in 2013 but has been actively progressing since 2020. India's cybersecurity strategy aims at assessing and combating different verticals of data breaches. The cybersecurity strategy of India covers people, processes, and technology. By establishing the National Critical Information Infrastructure Protection Center (NCIIPC) in 2014, the government took a significant step toward cybersecurity. The NCIIPC was responsible for tackling national-level threats to critical information infrastructure.

To fortify its cyber security the Indian government is working on developing quantum cryptography. It is an encryption protocol and hackproof that safeguards against unlawful interception. The Indian Army has cracked deals with industries to develop quantum cryptographic techniques to include it in the military sector. In December 2021 the Army established a quantum Lab at the Military College of Telecommunication Engineering, Mhow with the support of the National Security Council Secretariat. The government in 2021 formed the Defence Cyber Agency (DCA), an integrated tri-services agency to cater the cyber security threats. The Defence Cyber Agency (DCA) aimed to develop a cyber strategy and doctrine; and to collaborate with the National Technical Research Organisation (NTRO), Defence Research and Development Organization (DRDO), Research and Analysis Wing (RAW), and National Security Council to resist cyberattack. The Indian Army in April 2023 during the Army Commander's Conference (ACC) decided to activate Command Cyber Operations and Support Wings (CCOSWs) to improve its online platforms, defend its networks, and counter threats in the cyberspace domain. The Indian Army's CCOSWs are specialized units that will help in carrying out prescribed cyber security responsibilities. The team would be in charge of improving the Indian Army's cybersecurity posture along with network safety. Additionally, they will enable the Indian Army to make better use of contemporary networks and communication technologies. The CCOSWs will assist the Indian Army in fending off its adversaries' cyber warfare activities. In the direction of cyber security in the defence capabilities, the Cyber Defence Agency conducted 'Exercise Cyber Suraksha' in May 2024. The exercise emphasizes on increasing cooperation and integration between members of different armed forces and national organisations. Further, the Indian Armed Forces developed a cyberspace warfare doctrine which they released on 18th June 2024. This initiative was taken by the Armed Forces in response to China's

increasing cyber warfare and cyber espionage capabilities.[9] The doctrine will direct the commanders in organization and execution of cyberattack operations against the attackers.

SIGNIFICANCE OF CYBER SECURITY FOR ARMED FORCES:

Cyber security protects the armed forces from adversaries' cyberattacks. Cyber security restricts the attacker from stealing sensitive information, disrupting military operations, etc. In the contemporary world where countries more often make use of cyberattacks to disable the military network, and defeat their enemy, the significance of cyber security has increased. A robust cybersecurity defence can act as a disincentive to cyberattacks. Cyber Security counters numerous threats related to command and control systems, electronic warfare systems, piloted systems, etc. Strong and resilient cyber defence enables armed forces to handle core tasks of deterrence and defence, cooperative security, and crisis prevention and management. A country's cyber security ability helps to identify, prevent, and respond to detrimental cyber activities. A secure cyberspace prepares the armed forces to defend its network and operations from increasingly sophisticated cyber threats. Cyber security in the armed forces is crucial to protect the confidential data necessary for safeguarding national interests. The cyber security standards protect computer networks, and connected weapon systems from cyber threats. It helps the armed forces to build a resilient nation and internal digital defense. A proactive cyber security strategy allows armed forces to predict and mitigate advanced threats. It enhances the decision-making of armed forces in cyber intelligence. The cyber security is crucial in establishing real-time connections. Efficient cyber security strategies build up trust and confidence between the partner countries and allies. It exhibits a dedication to defend not only military hardware but also the larger objectives of both domestic and international security. Armed forces should build cyber security capabilities to assist them on battlefields and keep their system safe from adversaries during peacetime.

CONCLUSION:

Cyber Policy is now the alarm for examining India's pragmatic approach to confronting cyber challenges. Cyber security should be treated as par with terrorism and climate change. India is making significant efforts in addressing cyber threats with the government in 2019 approving the creation of only a small tri-service defence cyber agency. In comparison to China, which has built major capabilities in the cyber warfare domain including cyberweapons to degrade or destroy an adversary's networks, to sabotage satellites, India has been lagging far behind in this arena. India should formulate a clear and coherent cyber doctrine to guide Armed forces during digital skirmishes. Besides, for achieving strategic objectives of the military sector the Command Cyber Operations and Defence Cyber Agency should function efficiently. India needs to accelerate cyber security capabilities and quickly realize the necessity of customizing cyber policies to suit its unique context. India should reinforce its defensive abilities in cyberwarfare with the utmost urgency.

ENDNOTES:

1. Sharon, S. Gillis, A.S. Cybersecurity. Retrieved from https://www.techtarget.com/searchsecurity/definition/cybersecurity#:~:text=Cybersecurity%20is%20the%20practice%20of,centers%20and%20other%20computerized%20systems.
2. What is Cyber Security?. Retrieved from https://www.javatpoint.com/what-is-cyber-security.

3. Pande, J. Introduction To Cyber Crime. Introduction To Cyber Security. (2017). Haldwani. Uttarakhand Open University. p. 15.
4. (2024, January 22). India witnesses 15% rise in cyber attack cases in 2023: emerges as 2nd most targeted nation. Mint. Retrieved from https://www.livemint.com/news/india/india-witnesses-15-rise-in-cyber-attack-cases-in-2023-emerges-as-2nd-most-targeted-nation-11705939863447.html.
5. Cyber Security in the defense sector: the scenario, risks and future challenges. https://safecore.io/en/industries/la-cyber-security-nel-settore-difesa-lo-scenario-i-rischi-e-le-sfide-future/.
6. Poornima, B. (2023). Cyber Preparedness of the Indian Armed Forces. Journal of Asian Security and International Affairs, 10(3), p. 302.
7. Katoch, P.C. (2021, April 20). India in China's Cyber Crosshairs. Retrieved from https://www.spslandforces.com/experts-speak/?id=757&h=India-in-Chinas-Cyber-Crosshairs.
8. Poornima, B. (2023). Cyber Preparedness of the Indian Armed Forces. Journal of Asian Security and International Affairs, 10(3), p. 312.
9. Pandit, R. (2024, June 18). Armed forces formulate new doctrine for cyberspace operations. India News. Times of India. Retrieved from https://timesofindia.indiatimes.com/india/armed-forces-formulate-new-doctrine-for-cyberspace-operations/articleshow/111089679.cms