Identification of Network Security Issues and Challenges in Defense Environments

Manu Gautam, Dr. Gyan Prabhakar
Department of Electronics and Communication Engineering,
Babasaheb Bhimrao Ambedkar University, Lucknow
Email:-manugautam19998@gmail.com

Abstract: Network security refers to all physical and virtual assets that allow data to be transmitted between nodes or endpoints. As a result, network defence is a comprehensive and critical data security function that encompasses a wide range of job activities, such as detecting security flaws, stopping common intrusion attempts, detecting advanced network threats, monitoring traffic, enforcing security regulations, and protecting data. Threat actors' network attack policies evolve in tandem with the technological landscape. Technological progress is directly proportionate to developments on both sides of the threat-security split. As a result, there is a lot of ground to cover when teaching the notion of network security and associated dangers. This webinar will discuss the fundamental concepts, tools, and terminologies connected with network assaults, vulnerabilities, and defence. It's important to keep in mind that network security rules should be customised to the unique needs and risk profile of the defence acquisition environment. It is advisable to consult security professionals and follow any rules, specifications, or directives that apply to the defence sector. State actors, non-state actors, and persistent hacking and cyberattacks pose a danger to the Department of Defence Network. Physical assaults from radio jamming, logical cyber threats from hacking, or a mix of physical and logical attacks are all possible risks to the network.

Keywords: Network Security; Defence Software; Defence Environments; Data Security.

1. Introduction

‘Network security rules are crucial in the context of acquisitions for immediate defence. Data integrity, vital systems, and sensitive information security are of utmost importance while making purchases for the defence industry. A strong network security architecture protects against unauthorised access and potential cyber threats while guaranteeing the confidentiality, integrity, and accessibility of sensitive information. In order to fully comprehend the concept of network security, it is important to first have a general understanding of security as a whole. Security is defined as the process of continuously protecting an item from illegal access, ensuring a condition or sense of safety from danger. In order to fully comprehend the concept of network security, it is important to first have a general understanding of security as a whole. Security is defined as the process of continuously protecting an item from illegal access, ensuring a condition or sense of safety from danger. This item can take many forms, including a person, a company, an organization, or a piece of property such as a computer system or a file) **[1]’.** The creation of network security policies in the area of acute defence acquisitions should be guided by the important factors and concepts outlined in this introduction. Acute defence acquisitions should prioritise network security rules that safeguard sensitive data, stop unauthorised access, and guarantee the confidentiality, integrity, and availability of vital systems and data. Network security is necessary to provide both offensive and defensive cyber warfare capabilities. The DoD and national security organisations rely on cutting-edge network security technology and procedures to identify, assess, and counter cyber threats. This include gathering intelligence, examining weaknesses, doing penetration tests, and developing sophisticated cybersecurity technologies. Network security describes the policies and procedures used to guard against unauthorised access, interruption, and alteration of computer networks, devices, and data. To protect the privacy, integrity, and accessibility of network resources, multiple technologies, rules, and processes must be put into place. ‘Network security, on the other hand, is a more specific term that refers to the various procedures and preventative measures put in place to secure the underlying networking infrastructure of an organization. The main goal of network security is to monitor and prevent unauthorized access to an organization's network, resources, and assets. By doing so, the organization can safeguard against a variety of potential threats, such as cyber-attacks data breaches, and system downtime. To better understand the concept of security, it can be helpful to view it in relation to privacy. Privacy refers to the need to protect something or data from unauthorized access, while security is what guarantees that protection **[2]’**. In the linked world of today, where networks are the basis for data movement, corporate operations, and communication, network security is crucial. For businesses to safeguard sensitive information, keep customers' confidence, adhere to regulations, and

guarantee business continuity, they need a secure network architecture. Network security must be prioritised by the DoD and national security programmes if sensitive data, critical infrastructure, and operational capabilities are to be protected from cyberattacks. Cooperation is enhanced, data integrity, availability, and confidentiality are improved, and the country's military and security systems are made more resilient.

Figure 1: Network Secutrity to Defense Environments

2. Network Security Challenges in Defence Environments

2.1Technical Challenges

Networks frequently experience serious security setup errors [7,8]. Building cyber capabilities and addressing cyber security threats are hard tasks for the defence industry due to a variety of technological, organisational, and people issues.

Correct network configuration is challenging for a number of reasons, including:

- The configuration of networks is sometimes difficult and entirely manual, which causes mistakes and inefficiency. One example is a big an institution like a university is going to set up and control millions of unique network regulations throughout its networking infrastructure.
- preserving constancy and employing a large-scale network security that is error-free mostly manual procedure is difficult and hardly ever achieved.
- Low-level information must be manually set and is frequently input improperly. Examples include IP addresses and port numbers.
- Technology from several suppliers, each having their own proprietary and device-specific setup needs, is frequently found in environments. This increases complexity and creates more room for error in configuration.
- Most crucially, a single network security may include thousands of rules, some of which may clash due to faults.

2.2Operational challenges

In the linked world of today, where networks are the basis for data movement, operational challenges, and communication, network security is crucial. For defence to safeguard sensitive information, keep confidence, adhere to regulations, and guarantee defence department continuity, they need a secure network architecture. Network security must be prioritised by the DoD and national security programmes if sensitive data, critical infrastructure, and operational capabilities are to be protected from network attacks. Defence strategy will direct how things happen in the defence industry. As a result, it is critical that it be thoroughly thought out and that it serves its purpose of connecting theory to practise. Defence policy should consider the particularities of the situation at hand along with potential differences thereof; set achievable and realistic aims that strive towards overall national security goals. and do so in accordance with national and international principles, standards, and good practises. A defence planning should anticipate all stages of the policy making process, with specific emphasis on the planning and administration phases.

Network Attackers: These are technology officers who have received the necessary training and who have the acumen and experience to infiltrate the opponents' online communities, deploy crimes, and use the proper tools and procedures for full spectrum cyber operations[9].

Cyber Assistants: This group of employees would be specially trained to help cyber attackers carry out their duties. They would report to the attackers on the internet and be ORs or comparable civilian professionals with diploma-level training in cyber specialties[9].

Network Scientists: The most skilled cyber specialists, network scientists would have a deep level of expertise in a certain area of cyber operations. These staff members would conduct the required research to identify fresh vulnerabilities in current systems and create malware to take advantage of them. This degree of proficiency would likely come with years of experience as Network attackers[10].

Network Domain Experts: Security has become important issue for large computing organizations [11] Cyber domain experts are those who have super-specialized knowledge in a certain field, such as incident responders, auditors, big data analysts, etc.

Regulation challenges

The military environment of today is data-centric and depends more and more on stable, reliable, and scalable networks. The network rapidly gathers, combines, and uses data to take action in order to optimise operational benefit and boost efficiency. Data, along with the network that supports it, must be viewed as a strategic asset that must be operationalized in order to enhance military capabilities and make them more potent and efficient. Delivering a number of fundamental capabilities requires it to be built on a secure platform from the edge to the cloud, across multiple domains, and in a way that enables the flexible and secure movement of sensitive information and communications anywhere, anytime, in any mission environment. Defence capabilities are constantly improving, but the threat spectrum is constantly changing security architect at Curtiss-Wright Defence Solutions. Old attacks are constantly being used against new systems, so don't forget about them, and new attacks are constantly being developed.

I. **Data at mission speed, where it's needed**-Across the network operations platform, mission-grade visibility, information access, improved situational awareness, and security.
II. **Automating and orchestrating intelligently**-All defence users and devices will have automated provisioning, monitoring, and administration at scale that is in line with the operational goals now being pursued by the Defence Department.
III. **Critical infrastructure's resilience-**proactive critical infrastructure monitoring, analytics, and optimisation to carry out operations at high speed and provide scale-based support for resources and services that are mission-critical.

IV. **complete protection**-End-to-end security that is integrated, AI-driven, and improves incident detection and prevention also streamlines security operations by automating and coordinating response[13].

2 Literature Reviews

With the introduction of the Internet and new networking technology, the globe is becoming increasingly linked. Worldwide, there is a wealth of personal, economic, military, and government information about networking infrastructures. Because of the ease with which intellectual property may be obtained over the internet, network security is becoming increasingly important. Network security begins with authorisation, which is often accomplished through the use of a username and password. Network security refers to the rules and policies set in place by a network administrator to prevent and monitor unauthorised access, system modification, abuse, or denial of a computer network and its resources. Essentially, network security is the authorisation of data access in a network, which is regulated by the network administrator. Many network attacks on vital infrastructure in recent years have gone unnoticed due to national security concerns. Cyberspace has grown into a crucial component of a government, a society, and people's everyday lives as a result of the rapid expansion and broad usage of computer technology. The short-term character of deployed networks (2) the absence of training and direction (3) technological and cultural issues were major contributors to the security gap. This type of Cyber and network Security on Military Deployed Networks. We used this Technique is unauthorised or anonymous access. Anomaly being identified, protected management of groups and branch of this defence is It would be worth using the identified variables to statistically evaluate whether there exists a significant correlation between those (independent) variables and information leaks (binary dependent variable) [19]. Essential creation and establishment of trust. High-level security breaches and intrusions. Intrusion Detection for Air Force Networks Operational, Performance, and Implementation. Network monitoring should be able to operate with at least TCP/IP protocol suite operating over Ethernet, Fast Ethernet, IEEE 802.3, and FDDI Microsoft Networking protocols operating over Ethernet, Fast Ethernet, IEEE 802.3, and FDDI Banyan Vines operating over Ethernet, Fast Ethernet, and IEEE 802.3Network monitoring should be able to operate with TCP/IP traffic on ATM, X.25, and ISDN Novell traffic on ATM, X.25, and ISDN. This paper does not examine specific methods for detecting intrusions, does not address preventive measures that might forestall intrusions, and, generally, does not attempt to put intrusion detection into a total security posture context [18]. Routing protocols that are secure. In addition to being the primary counterinsurgency force, the Army is also instrumental in strengthening police and paramilitary forces (PMFs) in various states by providing them training, establishment of counterterrorism schools and intelligence. Doctrinal Changes for the Army. The prevailing internal security environment demands an astute national level conflict management strategy, comprehensive multidepartmental policy formulation and vigorous implementation [57]. Ambient and substance cybersecurity. With respect to the industry at hand (and not all industries), broad legal inspection could be necessary. Unique network security guidelines from regulators depending on region (not all companies). Encryption at the link/network layer. Security of the environment and physical objects Submission to Privacy [17]. Generally the network security system tools in the past were command line interface (CLI) based. It's only in this last few years that more and more computer and network administration task is done remotely through a web-based tool. Network system tools are very important no matter whether they are GUI or CUI, in today's heavily inter-connected era. MODERN NETWORK SECURITY: ISSUES AND CHALLENGES**.** Security Attacks; Security Measures; Security Tools; WAN; Security Factors; Firewalls;

Gateways; Intrusion Detection. The need is also induced in to the areas like defense, where secure and authenticated access of resources are the key issues related to information security. This paper explores important security measures related to different network scenarios, so that a fully secured network environment could be established in an organization [31]. DDoS attacks- To consume resources uselessly, To interfere with any system resource's intended function, or To gain system knowledge that can be exploited in later attacks Network Security Basics. Special-Purpose Computing Monte Carlo Method Noise and Signal Interaction Computing in Anatomic Rendering Multigrid Computing Mechanical Engineering Design and Tools. Network traffic, Network intrusions [32]. The security measures adopted in the database of the emergency command information website are: professional training for system managers, setting up security passwords and setting up protection software. Threat Assessment, lnerability and Assessment Risk Analysis. Risk Safety Assessment Based on AHP-Fuzzy Comprehensive Judgment and AHP-Fuzzy Comprehensive Evaluation Mode. Information Security Risk Assessment of Hazardous Chemicals Emergency Command System [33]. To achieve effective network security, businesses and organizations must consider multiple layers of control. Protection, detection, and reaction are the three basic frameworks of network security that should underpin any networking strategy. Network Security Concepts, Dangers, and Defense Best Practical. Network, Internet, Security, Security Threats, IP Address, Network Attack, Attackers. End-Users should Be Updated and Educated on Security Policies, anti-virus measures, Secure Data in Transit [34]. Exploring defense of the DOD's cyberspace domain in 2030 was clearly a challenging endeavor, but as reinforced by the conduct of this research, is vitally important. AIR FORCE AND THE CYBERSPACE MISSION DEFENDING THE AIR FORCE'S COMPUTER NETWORK IN THE FUTURE. Naval Network Warfare Command Desktop Computers Become Part of USAF Everyday Life. Off We Go to the Wild Blue Yonder McAfee's software. The Air Force must consider the effects of cyberspace in the future, and should consider the fact that this domain may be the weapon system of choice over the next 25 years [35]. Evaluation of the SDN control plane performance in large-scale heterogeneous networks, and its ability to respond to failures Evaluation/investigation of the number and placement of controllers. A centralized management miles away from the forwarding devices in an operational scenario is challenging, and the number and placement of controllers is a research problem in military networks. A Systematic Literature Review on Military Software Defined Networks. Military networks, network function virtualization; SDN; software defined networks; software defined radio; systematic literature review; survey; tactical networks; wireless sensor networks. Software Defined Networking (SDN) is an evolving network architecture paradigm that focuses on the separation of control and data planes. SDN receives increasing attention both from academia and industry, across a multitude of application domains [36]. More studies might compare military and security mechanisms to other types of mechanisms and investigate additional elements that can impact the efficacy of military and security mechanisms in order to acquire a clearer vision and a better understanding of this issue. Furthermore, for future studies, quantitative research methodologies will be examined in order to give a more systematic assessment of the data in this work. Analysis of Factors Affecting the Effectiveness of Military and Security Mechanisms. Global Security Development. Ineffective. Lack of Communication. Factors Affecting the Effectiveness of Military and Security Mechanisms. Military and security procedures include military collaboration, the development of military bases, military training, military exchange, and security agreements [43]. This paper reviewed the implications, challenges and the effects of cybercrimes and cybersecurity in the society. It fully defined cybersecurity based on governmental and national view, industrial view and academic. This research paper also reviewed different strategies used by different researchers to prevent cyber-attack in different areas of work and also exposed the most recent used cyber security attacks, preventions, future threats and prospective ways to avoid cyber-attacks. Cyber Security, Threats, Challenges and Different Fields. Cyber Security. using Machine Learning Cyber security in New Space. Cyber Security in Smart Grid. Responses from participants that have knowledge in cyber security indicated that they were able to distinguish between different types of cyber-attacks, whereas novice participants were not sensitive to the attack types. This showed that a cyber can be protected to a certain percentage based on the experience and training of workers regards the security threats and its likes [44]. It is beyond doubt that cybersecurity is critical for protecting personal and sensitive business and client data held by these organizations or their contracted third-party vendors.

No network is safe from intrusions, and data breaches and the aftermath of cybercrime can cost these organizations dearly. Cybersecurity Technologies and Trends Shaping the Current State of Security. Hybrid Cloud and Multi-Cloud Security. Advanced Persistent Threats (APTs). uncertainty of the Metaverse. These professionals must stay current with the latest cybersecurity resources, threats, and insights to tackle the escalating crisis. Whether an organization is securing its critical infrastructure, network, applications, or Internet of Things (IoT) devices, staying aware of threat vector surfaces and the most recent cybersecurity trends can help them prepare for cyberattacks against their organization [45]. It is necessary to extend the proposed approach to a framework that can be applied to combat systems and other weapon systems. this situation must be analyzed and studied by weapon system and security experts, and appropriate countermeasures must be established based on the mission characteristics associated with the weapon system. It is also important to develop a security framework that can be practically applied in weapon system development and guidelines for the security of weapon system software. In future work, we will develop additional subitems of the security test in consideration of future combat system trends. To solve this problem, an effective and practical software security testing approach is proposed in this paper to fundamentally deal with cyberattacks when considering the characteristics and environment of the combat system. Security Testing for Naval Ship Combat System Software. Weapon system, combat system, software security, security test. Military weapon systems, cyber-physical system, software-based complex system [46]. There is dearth of international literature on DISM in the field of libraries, and there is need to conduct more studies on DISM phenomenon. There is limited literature available on DISM policy in academic libraries, so research should be conducted on DISM policy in academic libraries in developing countries. Academic library security policy; adoption of DISM; barrier of DISM; data protection security; digital IS management; digital security; practice of DISM in libraries; security in libraries. Security policy, information security management policy, InfoSec policy, digital security policy, academic library security policy, data protection policy, Information security infrastructure policy, library security policy, data backup security policy. Digital information security management policy in academic libraries [47]. DDoS attacks are progressively becoming the most common form of cyber threat, according to recent market research, and have risen increasingly in both number and volume in the past year. The trend is towards a shorter length of attack but a greater number of packet-by-second attacks. it faces some security and privacy challenges due to the devices' vulnerabilities and vast heterogeneous networks. A comprehensive study of Distributed Denial of Services(DDoS)attacks over IoT network and their countermeasures. IoT layers, embedded smart system, advanced DDoS. The small devices have low computational power and less storage capacity and hence protection mechanisms and the cryptographic algorithm used for security are hard to implement over them [48]. It may expand on this publication and potentially cover topics such as how the SSDF may apply to and vary for particular software development methodologies and associated practices like DevOps, how an organization can transition from their current software development practices to also incorporating the SSDF practices, and how the SSDF could be applied in the context of open-source software. Secure Software Development Framework (SSDF). **S**ecure software development; Secure Software Development Framework (SSDF); secure software development practices; software acquisition; software development; software development life cycle (SDLC); software security. Prepare the Organization (PO), Protect the Software (PS), Produce Well-Secured Software (PW), Respond to Vulnerabilities (RV) [49]. We were troubled, however, when we looked at the presence of open source in tandem with vulnerabilities; of particular note was the Aerospace, Aviation, Automotive, Transportation, and Logistics sector. All—100%—of the codebases we examined in this sector contained open source, and open source made up 73% of its code. Sixty-three percent of its codebases contained vulnerabilities classified as high risk (those with a severity score of 7 or higher). We saw more of the same with the Energy and Clean Tech sector, in which 78% of the total code was open source and 69% contained high risk vulnerabilities. The total open source identified within this sector's codebases was 95%. OPEN SOURCE SECURITY AND RISK ANALYS. Software composition analysis (SCA) product team and the CyRC Audit Services team

have helped security, development, and legal teams around the world strengthen their security and license compliance programs for almost 20 years. Black Duck Security Advisory (BDSA) Software component. Open Source software risk and supply chain security are inextricably linked [50]. The purpose of the CSRA is to establish characteristics for cybersecurity architecture in the form of principles, fundamental components, capabilities, and design patterns to address threats that exist both inside and outside traditional network boundaries. Alignment of the CSRA to other RAs and solution architectures must include existing command and control (C2) orders and directives. The alignment of C2 and the CSRA will improve cyberspace survivability and enhance resiliency in operations and war fighter support to achieve integrated deterrence. Department of Defense (DoD) Cybersecurity Reference Architecture. Cross domain technology, Cross domain technology, Space Systems, Reduce risk from the inside out, Increase mission assurance through resilience. Enable modernization. When anomalous activity is detected, it must be analyzed to determine the risk to the DAAS and impact to cyber survivability. Traffic content and measurement inspection results must be logged to facilitate reduction in data storage requirements and accelerate automation and orchestration of responses. MCA has access to the environment and continuous analysis is required to achieve desired outcomes [51]. The goal is to explore new and emerging technologies related to fending-off cyber-attacks and cyber security, open system architectures, avionics, and sensors. Air Force wants new ways to find vulnerabilities to cyber-attacks in electronic warfare (EW) and avionics. Georgia Tech to investigate cutting-edge cyber security software and testing to foil enemy computer hackers. Cyber threats to evade network defenders and assess how critical networks fare against a determined cyberattack [52]. This essay has attempted to analyse the defence sector needs that are required to be mobilized on a ―war footing‖ and every department, agency or individual connected with the procurement or manufacture has to be held accountable. MAKE IN INDIA –CHALLENGES FOR INDIAN DEFENCE SECTOR, Ministry for Skill Development. Broad front licensing strategy, Creation of general-purpose R& D structure, Creation of specific mission-oriented institution, Creation of scientific and technical work force. Defence production within India is experiencing a tremendous change to accomplish self-reliance in defence technology. A growing number of AONs have been released under Make India, Buy and Make India Categorization [53]. The issue of attribution has also been a major impediment to identifying and going after the bad actors and it is unlikely to be resolved unless the web is reconstituted fundamentally. Militaries in Cyberspace Approaches, Expectations and Outcomes. Cyberwar, Cybersecurity, Military Restructuring, Cyber Command. The threats to the military are seen not only to its own immediate networks but also to that of suppliers, i.e., the defence industrial complex sub-contractors in the procurement, logistics and support areas [54]. In terms of systems, most generally, air defense can be defined as separated forces and measures organized in a specific structure aimed at ensuring safety in the airspace. The challenge for the air defense system in question is the implementation of tasks in the area of state air security by ensuring an appropriate degree of reaction of the assigned forces to emerging threats. Cybersecurity of Air Force. cybersecurity, Offensive Cyber Operation, Defensive Cyber Operation, satellite technologies, Air Force, Air and Space Force. On the ground-segment side of satellite control, the debut of privately owned communication antennas for rent and a move to cloud-based operations or mission centers will bring new requirements for cyber protection for both Department of Defense (DOD) and commercial satellite operations alike [55]. Posture the Force for Multi-Domain Operations. Security and Survivability Commander's Freedom of Action. Reform Processes & Policies. (Over the past several years, the Army has made tremendous strides modernizing its tactical formations with the deployment of Integrated Tactical Network (ITN) Capability Sets). THE ARMY UNIFIED NETWORK PLAN ENABLING MULTI-DOMAIN

OPERATIONS. SET THE UNIFIED NETWORK, OPERATIONALIZE THE UNIFIED NETWORK, CONTINUOUSLY MODERNIZE THE UNIFIED NETWORK. Optimize Governance Processes and Structure. Reshape Policy. Ensure Unified Network Investment Accountability [56]. According to the us hopes, the study's importance has been to offer a deeper knowledge of potential threats to the Department of Defence (DOD) for Network based on information gleaned through a review of the literature. Defence continues to experience problems with its network infrastructure from different unidentified network threats, making it difficult to provide security for the network there resources. The modern technology for defence employs for The challenges of ensuring network security in DOD are numerous. which the newest technology must overcome. Also, The existing network security regulations in DOD have several faults and require significant adjustments. This paper includes new technology and suggested changes DOD needs to polices its network infrastructure in order to can be protected from network threat ' ongoing onslaught. Establishing an acceptable defensive posture requires knowledge of the literature on intelligence sharing across DOD. With the exception of studies on the technical standards of information sharing, there is minimal practise research on the act of sharing to identify of network security issues and challenge in defence environments. The literature discusses the Police, issue and of military, Airforce and Army force (DOD) and facilitators to information sharing.

Networks should be protected from both internal and external attack. Take control of the network. weed out harmful content and unauthorised accessibility. Observe and test security measures. Make appropriate policy and set up anti-malware defences that apply to and are pertinent to all company areas. Scan the organisation for malware [12]. An interconnected network of information technology infrastructures, such as the World Wide Web, telecommunications infrastructure, computer systems, and integrated processors and controllers, constitute a global domain inside the information environment [13]. New features are being implemented, expanding the scope of network security. defence identification is being employed together with the same approaches. Compared to passwords, defence offers a more reliable authentication mechanism. As a result, there may be far less unauthorised access to secure systems. Researchers studying network security are discovering new technology, Network security's software component is always changing. New firewalls and encryption techniques are constantly being used. The study being done helps to forecast future advancements and comprehend existing trends in the subject. Both software and hardware development are active fields in network security.

3 Network Security Statistics and Trends

The next stage for leaders will be to determine how to safeguard their data once they have determined where their data risk is; to achieve this, they should think about using a find, protect, and control process. Given that nation-states continue to target the US using increasingly sophisticated techniques like AI/ML, quantum computing, and other technologies, Biden's national network security plan is expected to adopt a more aggressive posture to safeguard the country's infrastructure **[14].** In a tech environment that is continuously growing, an offensive strategy offers a more quick reaction than slow-moving laws on strategies like Zero Trust, which have evolved into a need and are now seen as fundamental insurance. If forecasts are true, the critical infrastructure sector will be subject to fresh security rules derived from the National Defence Strategy. While this may give the impression that organisations are scurrying to find budgets, resources, and plans, this does not have to be the case. If the Quantum Computing Cybersecurity Preparedness Act taught us anything, it is that waiting is not the best option. Regulations will not force the adoption of solutions that do not already exist, and

the best way to get ahead and receive government support is by starting evaluating technology now, figuring out the necessary skill sets for executing the solution, and locating trusted advisors to guide you through the application procedures.

3.1 Network Security in Military

Cyber systems have the potential to defeat any software-controlled system. Keeping all residents safe is the main goal of the military service. Military technology is advancing daily in India and is a crucial component of battle. The greatest challenge that governments have ever faced may be internet warfare. We are currently living in the digital era, thus network-terrorist attacks are a possibility. The strongest countries now dominate the globe thanks to military innovation. It's true that anything that is nice has its cons. All kinds of data and information are accessible on the internet. Like any other organisation or company, the military depends on network security to keep itself secure. The Internet has played a vital role in international communication for more than 20 years and has gotten more and more ingrained in people's daily lives. Military missions may become more challenging as a result of the surge in network attacks since it's getting harder for personnel to stay safe **[14]**.

The privacy of individuals is seriously threatened by the Internet's limitless nature and ease of search. In order to secure sensitive information, personal information, computers, and programmes against injury, attacks, and unauthorised access, network security refers to a collection of behaviours, techniques, and technology. Detecting, protecting, responding to, and preventing cyberattacks that might damage military systems and networks and have a detrimental impact on the military was the focus of cybersecurity. The fact that we have a number of outdated ideas in modern attire is the true issue with the idea of information warfare. In order to better protect the organization's and users' assets, it is in the military's best interest to join the national effort to develop comprehensive cyber security measures, which could include the legislation of governing policies, implementation of cyber security tools and best practises, as well as the training of excellent cyber security experts. Increasing internet security is just as important as purchasing additional tanks to keep India secure. Cyber risks put our profit security in peril in addition to our national security and peace **[15]**.

According to the NCO hypothesis, utilising networking to accelerate interactions while enhancing situational awareness would raise both the efficiency and effectiveness of warfare. A military doctrine or war theory known as network-centric warfare, also known as network-centric operations or net-centric warfare, aims to turn an information advantage, made possible in part by information technology, into a competitive advantage through the effective computer networking of geographically dispersed but well-informed forces.

Figure 2: Graphical representation of Military Network.

The United States Department of Defence invented it in the 1990s.The phrase "network-centric warfare" (NCW) is used to refer broadly to the collection of cutting-edge tactics, strategies, and procedures that a completely or even partially networked army might use to gain a decisive tactical advantage. By connecting sensors, decision-makers, and shooters, NCW increases combat capability by enabling shared awareness, quick command decisions, high-tempo operations, enhanced lethality, increased survivability, and some degree of self-synchronization. Network-centric operation is another name for network-centric warfare. By successfully tying together friendly troops inside the battlespace, it converts information dominance into combat strength by fostering a far higher level of shared contextual awareness and facilitating quicker, more informed decision-making [**16]**.

Now days Cyber attackers are getting increasingly tech-savvy and capable of launching a sophisticated assault into the networks that run the national infrastructures thanks to the abundance of information available in cyberspace and low-cost computer equipment. The Distributed Denial of Service is a similar attack that overwhelms systems (of national infrastructures) with more requests than they can handle, paralysing them as a result. 'Botnets', which are networks of computers that have been commandeered by remote users, sometimes without the target's knowledge, typically carry out distributed denial of service attacks. Once a botnet has been created, the attacker may control an attack by giving each bot remote commands. In addition to networks, software and hardware are also vulnerable to hacking even before they are connected to one another in a functioning system. DDoS assaults target a variety of network connection components.

3.2 Network Security in Air Force

Historically, strategic efforts in this area have concentrated on securing the information that sits within our networks by erecting taller and stronger walls around our crown jewels, stationing gate guards who question everyone entering or departing, and constructing several checkpoints. These attempts aim to reduce accessibility, which is precisely what our contemporary networks are built to give. Undoubtedly, this proved to be an unsuccessful plan because the expense of protecting these networks considerably outweighs the cost of attacking and entering these. Critically, it also impedes our soldiers' unhindered swift access to key information. The current network enclave defence approach is similar to these old perimeter defences in that it restricts access to seemingly valid users or transactions. However, it offers little to clarify the goal of the initiative.

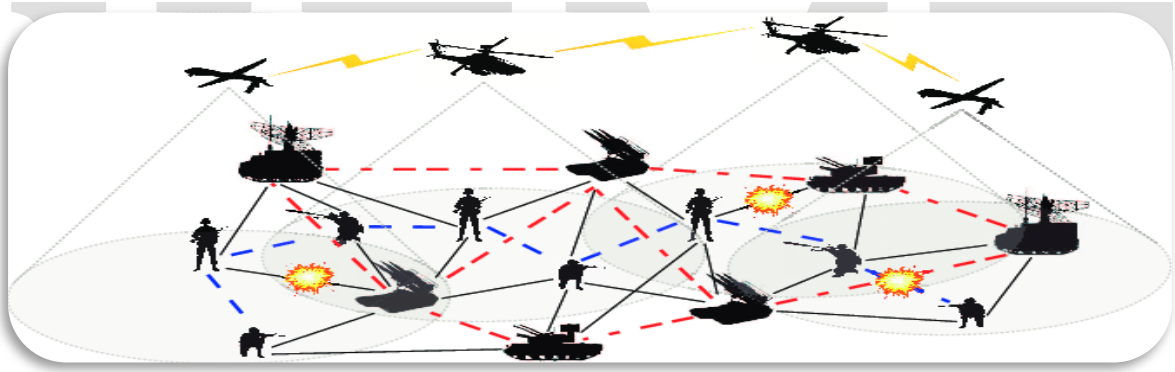

Figure 3: Graphical Representation of Air Force.

As a result, without a clear understanding of what needs to be defended, we are faced with the daunting task of defending everything in our "house/fort" without the ability to prioritise specific efforts, such as those which will likely have the greatest effect on our ability to complete the duty**.**

3.3 Network Security in Army Force

As previously stated, the Armed Forces' current role is confined to defence cyberspace security, with a limited mandate for offensive cyber operations in support of their operational responsibilities. According to the author, this role should be expanded to include a single point of contact for all offensive cyber operations (including active defence) at the national level, as well as the protection of our National Critical Information Infrastructure (NCII) when faced with threats with strategic implications. Although both the restricted and expanded roles need the development of capabilities for both defensive and offensive cyber operations, the personnel required to complete the expanded function would be orders of magnitude bigger, especially for offensive cyber operations **[18]**.

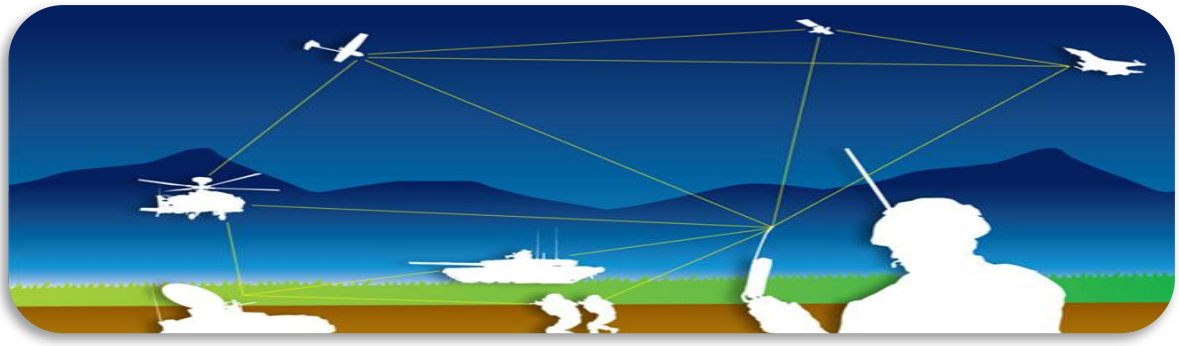

Figure 3: Graphical Representation of Army Force.

5.1 Network Security Risks

During the epidemic, remote labour became the new normal. Working from home enabled businesses to continue functioning as usual, but it also opened the door to internet criminal behaviour. Cyber assaults, hacking, and data breaches are becoming increasingly common. However, many firms might have avoided these dangers with little risk management and a proactive approach to digital security **[18]**. Whether you're through a digital transformation or concerned about data security, these are the growing cyber risks you should be aware of.

- Malware – a mix of the terms mischievous and programme — is a collective name for software that harms desktops, laptops, servers for websites, and networks. While malware isn't a new problem, hackers are always looking for new ways to exploit it. Ransomware, malware, spyware, and trojans are examples of such threats.
- Ransomware is a sort of software that extorts money. Hackers restrict user access to data, threatening to publish or erase it until a ransom is paid.
- Crypto jacking is the use of a computer to covertly "mine" cryptocurrencies such as Bitcoin and Ethereum. While it is not a direct risk, it may severely slow down your gadgets.
- This sort of malware, named after the famous Trojan horse, employs useful software as a backdoor to obtain access and exploit a machine or network. Credit card information is frequently stolen using Trojans.
- Worms are self-contained malware that spreads by itself across additional documents and programmes. Worms, as opposed to viruses, are autonomous programmes that may "wiggle" around your network.
- Wipers, often known as wiper malware, do harm to organisations by erasing as much data (if not all) as possible. Unlike ransomware, which is motivated by money, wiper assaults are motivated only by disruption. Wiper assaults may also be used by criminals to cover up the trails of several data thefts.
- Man-in-the-middle (MitM) operations are a sort of "shoulder surfing" in which hackers listen in on your internet connection. In order to steal data and modify congestion, criminals intercept communication between a server and a client.
- Brute force attacks are a sort of cryptography attack in which hackers use software to guess your login credentials repeatedly. One in every five networks has been subjected to a brute force assault.

- SQL injection attacks (SQLI) are common on websites that utilise databases. SQL attacks occur when an attacker injects code into a website or server database with the intent of stealing money, changing data, or erasing web activity.

5.2 Developing Network Security Policy in Defence Environments-

A more comprehensive idea known as national security policy or national security strategy includes defence policy. defensive strategy covers everything from real command and control to defensive planning and administration, which are related stages towards putting that policy into practise. In practise, the distinctions between each of these notions or phases are frequently hazy. Defence policy is often governed by norms and principles that are ingrained in national security policy and encompasses everything from purposes to tactics and means of attaining national defence objectives.

- **Access Management:** To prevent unauthorised access to sensitive data and systems, put rigorous access control mechanisms in place. Give users just the rights required for their responsibilities while adhering to the least privilege concept. To improve authentication security, use multi-factor authentication (MFA). Defence acquisition networks must be protected by access control methods. By implementing robust authentication solutions such as multi-factor authentication and adopting the concept of least privilege, access to essential systems and information may be closely restricted. This reduces the potential of insider assaults and aids in the prevention of illegal access.
- **Control of access based on role (CABR):** Use CABR to allocate permissions based on job roles and responsibilities. Determine the amount of access required for each role and provide permissions accordingly. CABR mitigates the risk of insider threats and assists in the prevention of unauthorised access.
- **Management of Least Privilege (MLP):** MLP solutions are used to control and track privileged accounts, such as administrator or super user accounts, which have additional access permissions and are more susceptible if compromised. They incorporate session recording and auditing capabilities, strict access controls, account activity monitoring, and session recording and auditing capabilities.
- **Segmentation of a Network:** Network segmentation is used to divide a network into isolated pieces or zones. This limits attackers' lateral movement in the event of a breach. Access controls can be put in place at each segment to guarantee that only those with authorization are granted entry to certain network regions.
- **Protected remote management:** If remote access is required for defence acquisitions, use secure remote access alternatives such as VPNs, which are virtual private networks, or secure desktop remote access protocols. Make ensuring that only those with authorization have remote access, and that adequate authentication processes are in place for remote connections.
- **Monitoring and Recordkeeping:** Activate logging and auditing features to keep tabs on user actions and access attempts. To spot any unusual or unauthorised access attempts, routinely monitor and verify audit trails. this assists in the detection of potential insider threats or security breaches.
- **Evaluation of Credentials on a Regular Basis (ECRB):** Conduct access evaluations on a regular basis to confirm and verify user access privileges. Check that entry credentials are consistent with employment roles and responsibilities. Eliminate any superfluous or obsolete access rights as soon as possible.
- **Professional Learning and Instruction (PLI):** Employees should be trained on the importance of access control as well as their duties in maintaining safe access. Instruct them on best practises for creating strong passwords, detecting phishing attempts, and reporting any strange behaviour or potential security problems.
  The Department of Defence (DoD) and national security initiatives rely heavily on network security. It is vital for safeguarding sensitive information and key infrastructure, as well as assuring data integrity, availability, and confidentiality.

5.3 Implication of Network Security

Here are some of the most important implications of network security in these situations:

- **Protection from web threats:** Network security measures help to protect against a variety of cyber risks, including as hacking attempts, malware infections, data breaches, and advanced persistent threats (APTs). These threats pose major risks to national security because they have the potential to jeopardise sensitive information, military operations, and critical infrastructure.
- **Protecting sensitive data:** The Department of Defence and national security agencies handle highly sensitive and classified information. Encryption, access controls, and data loss prevention (DLP) technologies, for example, help protect this data against unauthorised access, interception, or leakage. It ensures that sensitive data is only accessed and altered by allowed individuals.
- **Protection from insider threats:** Network security aids in reducing insider risks, which are caused when trusted persons with authorised access abuse their powers or do hostile acts. Suspicious activity may be found and possible insider attacks can be avoided with the use of effective network monitoring, user access limits, and behaviour analytics.
- **Maintaining operations:** Network security within the DoD and national security institutions ensures operational continuity. By protecting critical systems and networks against disruptions caused by cyberattacks, network security measures help to preserve critical operations, communications, and command-and-control capabilities even in the face of potential threats.
- **Collaboration and information transaction:** Effective network security enables secure collaboration as well as sharing of data across numerous divisions, agencies, and partners involved in national security initiatives. By building secure means of communication and implementing safe data exchange protocols, network security allows secure information sharing. This improves awareness of the situation and reaction time.
- **Protection of infrastructure:** Critical infrastructure, including power grids, transportation networks, and communication networks, is essential to maintaining national security. Network security measures aid in defending against network attacks that can threaten public safety, impair critical services, or give adversaries unauthorised access to delicate systems.
- **Capabilities for offensive and defensive cyber warfare: N**etwork security is essential for providing these capabilities. To detect, evaluate, and combat cyber threats, the DoD and national security organisations rely on cutting-edge network security technologies and methodologies. This involves acquiring intelligence, analysing vulnerabilities, conducting penetration tests, and creating advanced network security tools. In order to secure sensitive data, important infrastructure, and operational capabilities from network attacks, the DoD and national security initiatives must prioritise network security. It improves cooperation, increases data integrity, availability, and secrecy, and increases the resilience of the country's defence and security systems.

  Major Finding-The remaining section of this research includes an overview of the literature on recent network attacks that have taken place .The current investigation offers updated research on the CVE, or Common Vulnerabilities Exposures in order to report on the most recent developments.[41]

  The scope of this investigation prevents us from knowing more at this time about other countries' cyber and network warfare capabilities. Future study involving more researcher with network security experts could provide more in-depth details on the specific dangers that security professionals deal with on a regular basis.

Major problem-What network security best practises and techniques can we use from the operations and polices of defence environment to strengthen the network security of Department of Defence? These recommended network security procedures and techniques can be thought of—or categorized—as countermeasures to a network attack.

- **Infrastructure** – The country's capacity to develop and put in place a network security policy, as well as to strengthen its cyber defence, incident management, tools, expertise, and Technology security assets.
- **Learning and awareness**—Knowledge and skills look at the effectiveness, affordability, and uptake of policies by people, governments, and enterprises. It also has to deal with official network security instructional resources, professional training, and awareness initiatives for network security in DOD.
- **Guidelines and approaches**- Develop and keep up-to-date processes, operations, and tools for gathering, examining, and utilising state, data, and summaries from other disciplines to put up operational operating network security scenarios in defence department.
- **Regulations and norms** - Adopt and develop national network security laws and standards, both direct and indirect, with an emphasis on regulatory requirements for statutes and regulations that are relevant to network crime.
- **Administration** - Handle a network security programme that consists of a planning procedure, administration, and network security activities that are in line with the national strategic goals and the danger to the infrastructure.
- **Legislative innovation** – Network security regulations should be flexible, ever-evolving, and customised to address new issues and demands.
- **Specialisation** - A professional team in charge of upholding a certain network security legislation or act.

Key Finding

1. The AFIWC monitors operations, providing a global view of the Air Force network's security posture and recommending actions to base and regional commanders based on this global view [18] (1997).
2. The website of a hazardous chemical emergency command system in Qingyang is verified by the new risk value calculation formula, and the validity and reliability of the results are obtained [33] (2002).
3. The rise of contentious politics based on sectarian, ethnic, linguistic or other divisive criteria, is primarily responsible for the many communal and secessionist movements flourishing [57] (2004).

4. Techniques for detecting malicious code bring us back to general computer security issues and methods. Analysis of network activity associated with problems such as worm infections could complement other system security work in determining which machines are infected. Based on both traffic analysis and system behavioural analysis, for example, sufficiently suspicious machines might be isolated from their peers via (perhaps new) security protocols until administrators took steps to secure them [32] (2005).
5. Air Force pursue research in quantum encryption and security, and continue to examine computer security techniques for the mid-term and beyond. The Air Force should continue future planning efforts to anticipate and develop countermeasures to emerging threats in order to proactively protect and dominate the cyberspace domain of the future [35] (2007).
6. Military Field Data Network; Security Leak; Country Case Study; Human Resource Management, Cyber Offense [19] (2011).
7. Security policies should be designed first before its implementation in such a way, so that future alteration and adoption can be acceptable and easily manageable. The security system must be tight but must be flexible for the end-user to make him comfortable, he should not feel that security system is moving around him. Users who find security policies and systems too restrictive will find ways around them [31] (2011).
8. Environmental defence and material item integrity [17] (2014).
9. to evaluate the current state of the art in terms of research tracks, publications, methods, trends, and most active research areas and findings for consolidating the areas of past and current research on the examined application domain, and propose directions for future research [36] (2018).
10. This Particular paper initiative to present a state of matters associated with the Indian Defence subsequently illustrates the global circumstances associated with defence and tries to recognize their possibilities as well as the obstacles for the Make in India strategy for the defence sector [53] (2019).
11. The Army Unified Network Plan provides the strategic framework to guide the development of the Unified Network that the Army requires to realize its transformation to an MDO-capable force by 2028. The Unified Network modernization must be more than just developing and fielding capabilities. it must be a holistic approach that addresses our people, training, organizations, policies, and processes [56] (2021).
12. The naval combat system is a software-centric complex weapon system integrated with the network and computer software. The core performance and function of this system are influenced by software. Recently, the use of commercial software has significantly increased. However, systematic software security testing has not been applied to the real testing process in the system development stage during the combat system development, restricting the development of a robust combat system against cyberattacks [46] (2021).
13. There are many models for SDLCs, including waterfall, spiral, agile, and – in particular – agile combined with software development and IT operations (DevOps) practices. Few SDLC models explicitly address software security in detail, so secure software development practices usually need to be added to and integrated into each SDLC model. Regardless of which SDLC model is used, secure software development practices should be integrated throughout it for three reasons: to reduce the number of vulnerabilities in released software, to reduce the potential impact of the exploitation of undetected or unaddressed vulnerabilities, and to address the root causes of vulnerabilities to prevent recurrences [49] (2022).
14. To address this limitation, the paper discusses the development of current military and security mechanisms and compares their differences based on various reasons using different case studies.)rough the analysis of factors on the impacts of military and security mechanisms, the paper hopes to provide new perspectives that can help understand this issue and explores ways to distinguish the effectiveness of military and security mechanisms in reality [43] (2022).

15. Define cybersecurity goals for military systems within the Air Force around desired outcomes while remaining consistent with DoD issuances Realign functional roles and responsibilities for cybersecurity risk assessment around a balance of system vulnerability, threat, and operational mission impact, and empower the authorizing official to integrate and adjudicate among stakeholders. Hold individuals accountable for will full infractions of cybersecurity policies [55] (2023).
16. The unique nature of this domain has required some restructuring on the part of the military. This has led to its own set of complications when it comes to re-alignment of organisation, recruitment of personnel, and working with other actors in the civilian space. This paper looks at the cyber force structures in a number of countries to draw out the underlying logic behind the creation and modifications that the military in particular has gone through over a period of 10 years. It looks at the initial approaches, the expectations behind those approaches, and the eventual outcomes [54] (2023).
17. Focus in on advanced RF and digital EW simulations, threat models, sensor evaluations, and cutting-edge technology development in the RF domain [52] (2023).
18. While there are numerous CC/S/A efforts, initiatives, and pilots ongoing; a single, overarching view of how cyber protection activities in the DoD Space Enterprise could, or should, relate or be prioritized does not exist. The DoD is one of the largest owners of real estate, buildings, and industrial control systems (ICS) in the Federal Government with more than 500 installations, 300,000 buildings, and an estimated 2.5 million unique ICSs Cross domain technology is a key component of NSM-8 and includes inventory and reporting requirements. Results of the linked Binding Operational Directive (BOD-2022-001) will inform the CSRA about threats and vulnerabilities that need to be addressed at the enterprise level [51] (2023).
19. Open source was in nearly everything we examined this year; it made up the majority of the codebases across industries, and it contained troublingly high numbers of known vulnerabilities that organizations had failed to patch, leaving them vulnerable to exploit. In addition, BDSAs include temporal metrics in scoring considerations, whereas sources like the NVD do not. Our aim is to provide the most finely tuned and accurate scores possible, helping customers prioritize triage activities accurately [50] (2023).
20. IoT is having an evolving era as the technology is growing uninterruptedly and IoT is connecting devices as well as humans. With this rapid growth of technology, the IoT is becoming more vulnerable and the center of attraction for hackers. Attackers exploit the network to gain access to it. Among a variety of attacks, a DDoS attack behaves contrarily as it does not reveal any signs of device failure and is hence hard to avoid [48] (2023).
21. The purpose of this research is to look into the applications of DISM policies in terms of practices and implementation in academic libraries. identifies the challenges faced by academic libraries in applying these DISM practices regarding policy [47] (2023).
22. Security professionals and leaders need to align their strategies and best practices incrementally with their business objectives to establish advanced threat protection and improve cyber resiliency [45] (2023).
23. This study investigates how knowledge in network operations and information security influence the detection of intrusions in a simple network. This research paper also reviewed different strategies used by different researchers to prevent cyber-attack in different areas of work and also exposed the most recent used cyber security attacks, preventions, future threats and prospective ways to avoid cyber-attacks [44] (2023).
24. Cyber-attacks are increasing on daily basis, so we want to ensure we are applying security patches when they are due and anti-virus signatures are up to date, train our employees about security, and ensure our organization is up to date with compliances. Configure your network firewall to allow only the required ports and hosts; use secure and strong passwords, and do not forget to use the principle of

the least privilege model in your IT infrastructure. perform frequent backups and a continual audit of your IT environment [34] (2023).

6 Discussion and Analysis

We explored Network Security for Defence (NSD) in this study. NSD is the preventative along with to a lesser extent, proactive component of Network Security Operations (NSO). We examined how NSD fits into a broader group of defending activities and how non-nation states may lack the capacity to defend against a full-fledged attack by a nation state. We discussed what we are attempting to safeguard in terms of data and information. We also discussed the CIA trinity of confidentiality, integrity, and availability, as well as AAA, which stands for authentication, authorization, and auditing.

These basic concepts serve as the framework for the protection of our information assets. We discussed security awareness and training initiatives in order to safeguard the weakest link in our defences: people. We discussed the security attitude and what we can do to attempt to in still some of it in the users for whom we are accountable. Then we discussed security training for our users in order to educate them on the right answers to some of the instances in which they may possibly jeopardise our security footing. We also highlighted the necessity for varying degrees of security training for the various levels of technical skill that we may need to address. We must be effective in Network Security Defence all of the time and every time. Our opponents can strike at any moment and with whatever method they have available, and they only need to be successful once. We must be vigilant and respond to any attack. This is true for every system, network, and organisation. You are a part of the continuous war as a member of the military, key infrastructure, or even company structures.

7 Conclusion

The fast development of several network paradigms has led to the widespread sharing and efficient use of information resources. As a result, cyber security issues become worse. Moving target defence and mimic defence are being looked into as solutions to this problem in order to enhance the effectiveness of the defence. Additionally, enhancing network security has significant theoretical implications and practical significance for enhancing network active defence capabilities. Network security for defence is described as "actions taken through the use of computer networks to protect, monitor, analyse, detect, and respond to unauthorised activity within Department of Defence information systems and computer networks." In the worlds of the military and government, exposing sensitive information may have far-reaching ramifications beyond monetary loss. Such information can include Operations Orders (OPORDERS), war plans, troop movements, technical specifications for weapons or intelligence collection systems, the identities of undercover intelligence agents, and a variety of other items critical to the military and government's operations.

When such information is accessed in an unauthorised manner, many lives can be lost and the balance of power can be substantially affected. There are laws in place to safeguard this sort of information, but they are often still in the works. The inherent imbalance of network security defence makes reduction and annoyance in general much the more critical. The enemy only has to locate one of the accessible services to exploit to be effective, but the defence must equally maintain all of them. In order to appropriately defend their own national cyberspaces, key global actors have developed national cyber security plans and reorganised their security organisations. The military has often been given a key position in these reorganised entities.

References

1. Kizza, J. M. (2017). Guide to Computer Network Security. Springer

2. Harrington, J. L. (2005). Network Security: A Practical Approach (The Morgan Kaufmann Series in Networking). Morgan Kaufmann.
3. K. Beck, M. Beedle, A. van Bennekum, A. Cockburn, W. Cunningham, et al., 2001. "Manifesto for agile software development." http:// agilemanifesto.org/ (accessed Jul. 19, 2018).
4. Tzagkarakis, N. Petroulakis, S. Ioannidis Botnet attack detection at the Iot edge based on sparse representation 2019 Global IoT Summit (GIoTS), IEEE (2019), pp. 1-6
5. M. Crouse, B. Prosser, E.W. Fulp Probabilistic performance analysis of moving target and deception reconnaissance defenses Proceedings of the Second ACM Workshop on Moving Target Defense, ACM (2015), pp. 21-29
6. Y. Liu, W. Peng, J. Su A study of ip prefix hijacking in cloud computing networks Secur. Commun. Network., 7 (11) (2014), pp. 2201-2210
7. Wool, IEEE Computer, 2004.
8. Ranathunga D., Roughan M., Nguyen, H., Kernick P. and Falkner N., SCADA Firewall Configurations and the Implications for Best Practices, IEEE Transactions on Network and Service Management, 2016, 13(4), p. 871-884.
9. Policy Brief on "Internal security," Institute for Defence studies and analyses, New Delhi, June 2009.
10. Prime minister's speech at the chief minister's meet on Naxalism, april 13, 2006, New Delhi, available at http://pmindia.nic.in/speech/content.asp?id=311.
11. Importance of Network Security, found at http://www.content4reprint.com/computers/security/importance-of-network-security-system.htm
12. "India's National security: Internal and External Threats", at www.livemint.com.
13. Shrivastava, R.K.; Bashir, B.; Hota, C. Attack detection and forensics using honeypot in IoT environment. In Proceedings of the International Conference on Distributed Computing and Internet Technology, Bhubaneswar, India, 10–13 January 2019; pp. 402–409.
14. Zhuang, R.; DeLoach, S.A.; Ou, X. Towards a theory of moving target defense. In Proceedings of the ACM Workshop on Moving Target Defense, Scottsdale, AZ, USA, 7 November 2014; pp. 31–40.
15. Wu, J. *Cyberspace Mimic Defense*; Springer: Cham, Switzerland, 2020.
16. Qin, Z.; Denker, G.; Giannelli, C.; Bellavista, P.; Venkatasubramanian, N. A software defined networking architecture for the internet-of-things. In Proceedings of the IEEE Network Operations and Management Symposium (NOMS), Krakow, Poland, 23–27 May 2014; pp. 1–9
17. Y. Liu, W. Peng, J. Su A study of ip prefix hijacking in cloud computing networks Secur. Commun. Network., 7 (11) (2014), pp. 2201-2210
18. Approved for public release; distribution unlimited. © 1997 The MITRE Corporation. All rights reserved
19. 2011 3rd International Conference on Cyber Conflict C. Czosseck, E. Tyugu, T. Wingfield (Eds.) Tallinn, Estonia, 2011 © CCD COE Publications
20. D. Wang, J. Yu, B. Liu, C. Long, P. Chen, and Z. Chong, "Integrated energy efficiency evaluation of a multi-source multi-load desalination micro-energy network," *Global Energy Interconnection*, vol. 3, no. 2, pp. 128–139, 2020.

View at: Publisher Site | Google Scholar

21. Y. Tang and M. Elhoseny, "Computer network security evaluation simulation model based on neural network," *Journal of Intelligent and Fuzzy Systems*, vol. 37, no. 3, pp. 3197–3204, 2019.

View at: Publisher Site | Google Scholar

22. L. Deng, D. Li, X. Yao, and H. Wang, "Retracted article: mobile network intrusion detection for IoT system based on transfer learning algorithm," *Cluster Computing*, vol. 22, no. S4, pp. 9889–9904, 2019.

View at: Publisher Site | Google Scholar

23. C. Zhou, H. Wang, C. Wang et al., "Geoscience knowledge graph in the big data era," *Science China Earth Sciences*, vol. 64, no. 7, pp. 1105–1114, 2021.

View at: Publisher Site | Google Scholar

24. S.-P. Wang and D.-M. Zhao, "A hierarchical power grid fault diagnosis method using multi-source information," *IEEE Transactions on Smart Grid*, vol. 11, no. 3, pp. 2067–2079, 2020.
25. Australian Government media release, Stronger cyber defences for deployed ADF networks, 12th August 2020; Available from: https://www.minister.defence. gov.au/minister/lreynolds/media-releases/strongercyber-defences-deployed-adf-networks
26. Wardrop, C., Victory in the Age of Cyber-Enabled Warfare, 11th March 2021; Available from: https:// theforge.defence.gov.au/publications/victory-agecyber-enabled-warfare#ftnt30
27. https://www.theguardian.com/ australia-news/2020/jun/19/australia-cyber-attackattacks-hack-state-based-actor-says-australianprime-minister-scott-morrison
28. Available from: https://www.homeaffairs.gov. au/cyber-security-subsite/files/cyber-securitystrategy-2020.pdf
29. Ranathunga D., Roughan M., Nguyen, H., Kernick P. and Falkner N., SCADA Firewall Configurations and the Implications for Best Practices, IEEE Transactions on Network and Service Management, 2016, 13(4), p. 871-884.
30. Braue, D. Defence Consolidates cyber capabilities, Information Age, August 2020; Available from: https://ia.acs.org.au/article/2020/defenceconsolidates-cyber-capabilities.html
31. Shailja Pandey et al. / International Journal of Engineering Science and Technology (IJEST) Vol. 3 No. 5 May 2011 ISSN : 0975-5462
32. Marin, G.A. (2005), "Network security basics", In security & Privacy, IEEE, Issue 6, Vol. 3, pp. 68-72, 2005.
33. L. Wang, A quantitative computer system and network security risk assessment method[D] (Harbin Institute of Technology, 2002)
34. Computer Engineering and Intelligent Systems ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online) Vol.14, No.2, 2023 https://www.researchgate.net/publication/369739760
35. Center for Strategy and Technology, Air War College, 325 Chennault Circle, Maxwell AFB, AL 36112, or on the CSAT website at http://www.au.af.mil/au/awc/awcgate/awccsat.htm. The fax number is (334) 953-6158; phone (334) 953-6150.
36. Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Gjøvik 2815, Norway; hakon.gunleifsen2@ntnu.no (H.G.); goitom.weldehawaryat@ntnu.no (G.K.W.) * Correspondence: vasileios.gkioulos@ntnu.no; Tel.: +47-61135162 Vasileios Gkioulos *,†,‡, Håkon Gunleifsen ‡ and Goitom Kahsay Weldehawaryat ‡
37. Lal, C.; Petroccia, R.; Conti, M.; Alves, J. Secure underwater acoustic networks: Current and future research directions. In Proceedings of the 2016 IEEE Third Underwater Communications and Networking Conference (UComms), Lerici, Italy, 30 August–1 September 2016; pp. 1–5.
38. Bader, A.; Alouini, M.S. Mobile Ad Hoc Networks in Bandwidth-Demanding Mission-Critical Applications: Practical Implementation Insights. IEEE Access 2017, 5, 891–910. [CrossRef]
39. Bor-Yaliniz, I.; Yanikomeroglu, H. The new frontier in RAN heterogeneity: Multi-tier drone-cells. IEEE Commun. Mag. 2016, 54, 48–55. [CrossRef]
40. Demirors, E.; Shankar, B.G.; Santagati, G.E.; Melodia, T. SEANet: A software-defined acoustic networking framework for reconfigurable underwater networking. In Proceedings of the 10th International Conference on Underwater Networks & Systems, Arlington, VA, USA, 22–24 October 2015; p. 11.
41. : https://www.researchgate.net/publication/313804253
42. ARCIC. 2016. "Army Warfighting Challenges." Accessed January 17, 2016. http://www.arcic.army.mil/Initiatives/army-warfighting-challenges.aspx.

43. Security and Communication Networks Volume 2022, Article ID 8208892, 11 pages https://doi.org/10.1155/2022/8208892
44. Eze et al INOSR Scientific Research 9(1):13-24, 2023. 13 ©INOSR PUBLICATIONS International Network Organization for Scientific Research ISSN: 2705-1706 https://www.researchgate.net/publication/367742804
45. PurpleSec (2023). Cyber Security Statistics – The Ultimate List Of Stats, Data, & Trends For 2023. Retrieved from purplesec: *https://purplesec.us/resources/cyber-security-statistics/#Cybercrime*
46. CHEOL-GYU YI 1 , (Student Member, IEEE), AND YOUNG-GAB KIM 1,2, (Member, IEEE) Received February 3, 2021, accepted April 23, 2021, date of publication April 30, 2021, date of current version May 10, 2021. Digital Object Identifier 10.1109/ACCESS.2021.3076918
47. Journal of Information Science 1–15 The Author(s) 2023 Article reuse guidelines: sagepub.com/journals-permissionsDOI:10.1177/01655515231160026 journals.sagepub.com/home/jis
48. Computers & Security Volume 127, April 2023, 103096 https://doi.org/10.1016/j.cose.2023.103096
49. National Institute of Standards and Technology Special Publication 800-218 Natl. Inst. Stand. Technol. Spec. Publ. 800-218, 36 pages (February 2022) CODEN: NSPUE2https://doi.org/10.6028/NIST.SP.800-218
50. 2023 Open Source Security and Risk Analysis Report
51. DoD CIO Cybersecurity Architecture Division Version 5.0 January 30, 2023
52. https://sam.gov/opp/5695b1e77e624d3fa850ada7fba25a0d/view.
53. International Journal of Management, IT & Engineering Vol. 9 Issue 5(2), May2019, ISSN: 2249-0558 Impact Factor: 7.119 http://www.ijmra.us
54. Manohar Parrikar Institute for Defence Studies and Analyses Journal of Defence Studies, Vol. 17, No. 1, January–March 2023, pp. 5–24
55. Elżbieta Hodyr, PhD Student, War Studies University in Warsaw, ORCID: 0000-0001-5045-093X. Cybersecurity and Law 2022;8(2):56-59 DOI: https://doi.org/10.35467/cal/157124
56. LTC Tonya S. Robinson, DANI-NSP, DCS, G-6 Plans and EIEMA Portfolio Management Division latonya.s.robinson.mil@mail.mil
57. First Edition of October 2004 Published By Headquarters Army Training Command Headquarters Army Training Command Shimla – 171003 India