AIR POWER

Journal of Air Power and Space Studies

Vol. 18 No. 4 • Winter 2023
(October-December)

Contributors

Colonel Gaurav Soni • Professor (Dr) W. Selvamurthy
• Air Marshal VPS Rana • Air Commodore Manoj Kumar
• Captain (Dr) Sunil Tyagi • Air Vice Marshal (Dr) Devesh Vatsa
• Ms Payal D. Dave • Mr Rohith Sai Narayan Stambamkadi

CENTRE FOR AIR POWER STUDIES, NEW DELHI

INCREASING CYBER ENIGMA FOR IAF: A WAY FORWARD

DEVESH VATSA

> Cyber-related risks are a global threat of bloodless war. India can work towards giving the world a shield from the threat of cyber warfare.
>
> —Prime Minister Narendra Modi

INTRODUCTION

Nothing comes close to set the tone for this journey of cyber warfare than the words by the prime minister of one of the largest democracies in the world, and home to innovations and technological prowess. India has, for decades, witnessed revolutions all around the world, but the time has come for the world to witness India taking the lead. History has shown that any new idea, product, or process had always been the fallout of a military requirement, which includes algorithms, weapons, aircraft and even today's internet and the cyber world. Hence, the Indian military in general and the Indian Air Force (IAF) in particular, are poised to usher in a new era of revolution and reorganisation of combat and associated

Air Vice Marshal (Dr) **Devesh Vatsa** VSM (Retd) is a former Commandant of Aviation Software Development Institute (SDI) of the IAF and Assistant Chief of Staff (Communication). Presently, he is working at DSCI, NASSCOM, as Advisor, Cyber Security & Critical Technologies.

operations. Welcome to the enigmatic world of cyber physical systems[1] and cyber warfare.[2]

Cyber power is the new soft power which is much more lethal than the conventional power achieved through military might. The primary reason for acknowledging the prowess of cyber power in domains such as the political, economic and military affairs is the ability of information and information technology to provide and support crucial elements of operational activities. The IAF has always been at the forefront to adapt new technologies and, at the same time, adapt to the nuances associated with them. With cyber systems making their way into every aspect of operational constructs, it is but natural for the IAF to gain insight into this domain and lead the cyber warfare game. The Chief of Air Staff (CAS), IAF, has rightly brought out the IAF's perspective during his interview with *SPS-AVIATION,* where he opined that cyber operations are an integral part of military operations and the organisation has been working towards enhancing and upgrading these capabilities.[3]

In order to delve further into this area, it is important to understand a few underlying aspects related to the cyber domain in general and its applicability to the IAF in particular, for administrative, maintenance and operational requirements.

CYBER DOMAIN: UNDERSTANDING THE ENIGMA

> They told you that you were safe. They told you lies. You are weak and defeated. For the price of one helicopter, we have brought you to your knees.
>
> —Thomas Waite, Legal Code

1. Radhakisan Baheti and Helen Gill "Cyber-Physical Systems", *The Impact of Control Technology* 12.1 (2011), pp. 161-166.
2. Md. Onais Ahmad, et al. "Cyber-Physical Systems and Smart Cities in India: Opportunities, Issues, and Challenges", *Sensors*, vol. 21, no. 22, November 2021, p. 7714.
3. "Excerpts from Interview of CAS", *SP's Aviation*, issue no. 2, 2022, https://www.sps-aviation.com/story/?id=3076. Accessed on December 25, 2022.

The cyber domain is an electronic information (data) processing domain where zeroes and ones transact at a very high speed in one or many information technology infrastructures.[4] The cyber environment, on the other hand, comprises various users, all kinds of government networks, corporate networks, home networks, both wired or wireless, devices such as Personal Computes (PCs), laptops, smartphones, tabs, all kinds of software, processes, information, both stored or in transit, various applications, services, and systems that can be accessed directly or indirectly to networks. Cyber space is the name given to the new global commons, created when we connect all the routers, switches, computers, fibre optic cables, wireless devices, satellites and other components of information technology which include the internet. The new hyper-connected world of the post-digital era has blurred borders, and provided new opportunities but also entails new challenges, risks, and threats because of its global reach. The cyber domain is a man-made domain of the 20th century, which is now accepted as the fifth domain of warfare, the other four being well-known, namely, land, sea, air and space. While these four domains are the components of the cosmos, the fifth is a human creation[5] – a pure on-going technological development with continuous and significant impacts on the whole universe. The cyber domain also differs from other domains in its unique characteristics which have a direct and great influence on the activities within the cyber domain.

Cyber space is the name given to the new global commons, created when we connect all the routers, switches, computers, fibre optic cables, wireless devices, satellites and other components of information technology which include the internet.

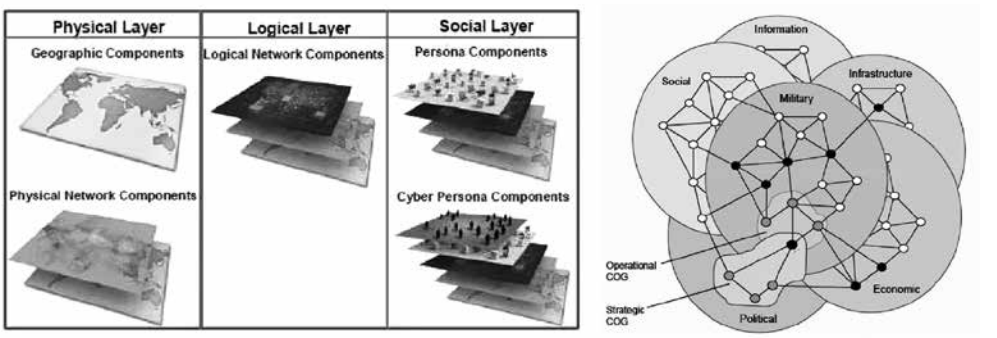
Organisations need to develop a deeper understanding of the various technologies and emerging threats existing in the highly dynamic cyber

4. Tim Maurer and Robert Morgus, "SPACE", JSTOR, October 1, 2014, pp. 18–24., https://www.jstor.org/stable/resrep10487.5. Accessed on January 11, 2023.
5. Dan Efrony, "The Cyber Domain, Cyber Security and What About the International Law?", https://csrcl.huji.ac.il/sites/default/files/csrcl/files/dan_efrony.pdf. Accessed on December 25, 2022.

domain to have an upper edge. The cyber domain can be broadly divided into five parts, as shown below:

- **The Physical Domain:** This includes the media, cables, optical fibres, intelligent or dumb components, devices, and endpoints like PCs, mobiles, tablets, or any other entity which occupies a physical space.
- **The Logical Domain**: This represents various functional, operational, and administrative entities that form part of a cyber ecosystem. It consists of those elements of the network related to one another in a way that is abstracted from the physical network, based on the logic programming (code) that drives network components. Workflows, control flows, services, processes, and software that runs on a computer system, including the Basic Input/Output System (BIOS), operating systems, applications, and data form the logical domain.[6]
- **The Data Domain:** This represents the collection of values that a data element may contain. Everything generated by the physical and logical domain in the form of system logs, error logs, and output becomes a part of the data realm.

Fig 1: Cyber Domain and its Interconnections[7, 8]



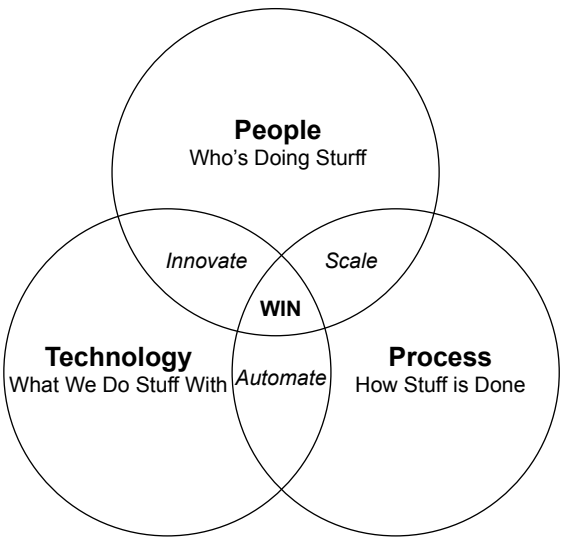
6. Akhil Bhadwal, "Cybersecurity Domains: A Brief Overview", knowledgehut, October 19, 2023, https://www.knowledgehut.com/blog/security/cyber-security-domains. Accessed on December 25, 2022
7. AcqNotes, s.v. "Cyberspace", https://acqnotes.com/acqnote/careerfields/cyberspace. Accessed on December 25, 2023.
8. Michael J. Weiskopff, Defence Technical Information Centre, "Effects-Based Operations in the Cyber Domain", 2017, p. 7.

- **The Application Domain**: This includes the application layer constructs which map the logical domain to the physical domain, with dependency on data domain features. All the applications available on a computer system form part of this domain.
- **The User Domain:** Last but not the least, the user domain is represented by a set of physical or logical entities which consume and generate data, thereby forming the other end of the cyber domain spectrum. In simple terms, all users and user information form part of the user domain. This is the part which makes "cyber" existence and experience good or bad, socially, politically, and operationally.

PILLARS AND TENETS OF CYBER DOMAIN

> Technology is destructive only in the hands of people who do not realise that they are one and the same process as the universe.
>
> —Alan Watts

Fig 2: The People / Process / Technology Framework



Source: Christopherspenn.com | @cspenn

- **People, Process and Technology:**[9] Any ecosystem comprising a product, a user of the product and a workflow is based on three important pillars, namely, People, Process, and Technology, popularly represented as the PPT concept. The PPT concept is all about how the three elements interact. In the domain of cyber, people are the users of networks as well as people who are responsible to protect the networks from cyber threats. Processes include the policies, instructions, directives, and advisories which need to be followed by the users of the network to remain safe and protected from cyber attacks. Technology helps people do their tasks and helps automate processes. Thus, organisational efficiency and protection from emerging cyber threats can be achieved by balancing the three and optimising the relationships among people, processes, and technology.
- **People:** People refers to the human resources available to any organisation. The people are the ones who need to follow the laid down processes to keep the workplace safe from cyber threats.
- **Process:** A process is the steps or actions that combine to produce a particular goal of cyber safety. The process in the PPT framework mostly defines the "how" aspect.
- **Technology:** The technology provides the necessary infrastructures for running the networks as well as the products which can be utilised extensively to protect them by applying control through processes. It also helps in the automation of some parts of the process.

As standalone components, people, processes, and technology are necessary for organisational transformation and management. To achieve organisational efficiency, there is a need to place the three in equilibrium and maintain good relationships among them. In the cyber domain, although the process and technology can be controlled to a certain extent, it is the people

9. Christopher S Penn, "Transforming People, Process, and Technology", April 7, 2021, https://www.christopherspenn.com/2021/04/transforming-people-process-and-technology-part-1/. Accessed on December 25, 2022

who are the ultimate users in every aspect, and, thus, define the outcome of any ecosystem.

CIA Triad: The letters CIA reminds us of the Central Intelligence Agency, popularised by innumerable Hollywood flims. However, it stands for more significant aspects closer home. Information security is not only about securing information from unauthorised access, but extends to preventing unauthorised access, use, disclosure, disruption, modification, inspection, recording or destruction of information. Information security programmes are built around three objectives, commonly known as CIA – Confidentiality, Integrity, and Availability. Apart from these, a few other concepts which govern information security include Non-repudiation, Authenticity and Accountability. Table 1 describes the basic information security constructs

Fig 3: CIA Triad[10]

10. Debbie Walkowski, "What is the CIA Triad", F5 Labs, July 8, 2019, https://www.f5.com/labs/learning-center/what-is-the-cia-triad. Accessed on December 25, 2022.

Table 1: Tenets of Information and Data Security[11]

Concepts/ Terminologies	Description/ Definitions
Confidentiality	Information is not disclosed to unauthorised individuals, entities, and processes.
Integrity	Accuracy and completeness of data are maintained. This means data cannot be altered in an unauthorised way.
Availability	Information must be available when needed and asked for.
Non-repudiation	Both receiver and sender cannot deny receiving a message or a transaction.
Authenticity	Verifying the users as who they say they are and that each input arriving at the destination is from a trusted source. This, if followed, guarantees valid and genuine messages received from trusted sources through valid transmissions.
Accountability	It should be possible to trace the actions of an entity uniquely to that entity.
Information Assurance	The act of ensuring correct information being transmitted, stored and transmitted to the right person when desired ensuring that information is not compromised in any way when critical issues arise.

EVOLUTION OF INFORMATION DOMAIN IN THE IAF

> If future generations are to remember us more with gratitude than sorrow, we must achieve more than just the miracles of technology. We must also leave them a glimpse of the world as it was created, not just as it looked when we got through with it.
>
> —Former US President Lyndon B. Johnson

11. Michael Nieles, Kelley Dempsey, and Victoria Yan Pillitteri. "An Introduction to Information Security", NIST Special Publication 800.12 (2017): 101.

As an organisation, the IAF had always been open to technological advancements and has gone ahead with strategic decisions that were seen to be revolutionary. The IAF's journey with respect to Information Technology (IT) is not new, in fact, it is as old as its existence. A few of the important units/establishments involved with computers, information technology, digitisation and information management are enumerated in the subsequent paragraphs.

- **AFCAO**: The IAF was way ahead in its thought process in terms of digitisation, as it was fully prepared to embrace the digital shift at a time, when others were looking at, and gauging, the quality of typewriters. Evolving a computerised process for disbursement of salaries was unheard of even by international standards. The Air Force Central Accounts Office (AFCAO) came to being when the accounts of the IAF were transferred from the Royal Air Force Base Accounts Office to the Air Force Central Accounts Office. The payslips were maintained manually which was tedious and error-prone. Hence, the need was felt to automate the process. Computerisation came to the fore with a humble beginning by rolling out voluminous data sheets for the Airmen Pay Wing. The task was carried out on a three-hour time-sharing basis from the computers of the Department of Statistics, Cabinet Secretariat, RK Puram, due to the paucity of the requisite hardware resources. AFCAO became one of the premier establishments of the IAF to initiate computerisation and led to the creation of a digitised financial entity exclusively for the IAF. The Officers Pay System in 1988; Airmen Pay System in 1991; and Civilian Pay System in 1993 are some significant milestones which were later integrated to generate the Intermediate Running Ledger Account (IRLA)-cum-Pay Slips.
- **AFRO:** All functionalities in the Air Force Records Office (AFRO) have been long computerised and an automated system has been put in place to perform the intended task. The postings of air warriors are now being managed through computers. Transparency and rationality in posting

The postings of air warriors are now being managed through computers. Transparency and rationality in posting without human bias is being achieved. This has brought a lot of satisfaction amongst the air warriors.

without human bias is being achieved. This has brought a lot of satisfaction amongst the air warriors.

- **AFGIS:** The Air Force Group Insurance Society (AFGIS) has long been registered for the welfare of the past and present members and their dependants. This establishment mobilises the savings of Air Force personnel, past, present and their dependents, and suitably invests the same and distributes the income so earned among its depositors. It is also involved in providing loans/grants for welfare activities. AFGIS operations have long been computerised for enhancing efficiency and effectiveness.
- **CSDO:** The Central Servicing Development Organisation (CSDO) is a premier institution in the maintenance hierarchy of the IAF. The Royal Air Force (RAF) and Army Aviation Corps, UK, addressed the aircraft maintenance management issue by constituting the Central Servicing Development Establishment (CSDE) under the functional control of the director general of engineering, Ministry of Defence (Air). The primary role of the unit, with respect to new inductions, is to continuously evaluate maintainability aspects by participating in Maintenance Evaluation Trials (MET) and the development of servicing philosophies. CSDO is also responsible for undertaking studies on technical aspects as directed by Air Headquarters (HQ) to improve the maintainability and availability of assets for operations. Presently, CSDO is engaged in studies to optimise the time taken for servicing so that more assets are made available for flying. With the implementation of project e-MMS(Electronic Maintenance Management Systems), CSDO can carry out a near real-time publication revision against the standard bi-annual amendments and five yearly revision cycles. This cycle has enabled centralised enforcement of lifing and servicing policies across the IAF in the barest minimum time. CSDO has adapted to the world of IT in a befitting manner.

- **IMMOLS:** Most units of the Indian Air Force have now been connected to the Integrated Material Management On-line System (IMMOLS), which was launched in the year 2006. IMMOLS has ensured transparency and improved logistics support in terms of procurement and provisioning. The IAF has given a unique code through a standard numbering system to every item of material that it requires. The information on the stock, location and consumption of every item is, thus, available at the fingertips of all the units. Personnel can know immediately when it is time to replenish the inventory of an article and can order it without delay. The IMMOLS software was developed to eliminate the problems of delay, ensure better coordination and improve efficiency.

AFNet has proven to be an effective force multiplier for intelligence analysis, mission planning and control, post-mission feedback and related activities like maintenance, logistics and administration. It is designed for high reliability with redundancy.

- **AFNet:** The Air Force Network (AFNet) is an Internet Protocol (IP) based Multi-Protocol Label Switching (MPLS) network which provides voice, video and message services to the personnel pan IAF. AFNet has proven to be an effective force multiplier for intelligence analysis, mission planning and control, post-mission feedback and related activities like maintenance, logistics and administration. It is designed for high reliability with redundancy built into the network design itself. AFNet is also capable of transmitting videos from Unmanned Aerial Vehicles (UAVs), and pictures from the Airborne Warning and Control Systems (AWACS) to decision-makers on the ground and providing intelligence inputs from remote areas. AFNet raised the bar towards the use of IT which led to near real-time information transfer, thereby making decisions easier and better.
- **DCMU:** The Data Centre Management Unit (DCMU) is a one of its kind specialist communication unit in the IAF responsible for all the

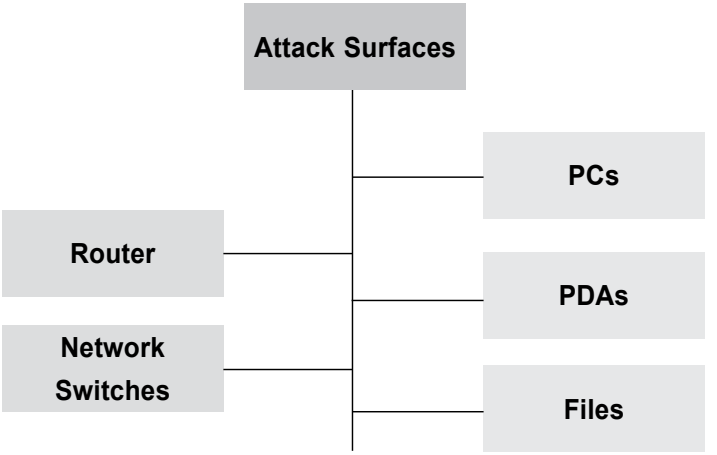
data services of the Indian Air Force. The unit has been set up in the HQ Training Command campus. DCMU exercises functional control of all Data Centres (DCs) spread across the IAF and addresses all data services-related issues of the entire IAF. It houses a variety of high-end hardware responsible for hosting services with respect to operations, maintenance and administration of applications pan IAF. DCMU hosts various data services on AFNet and manages all the five IAF DCs. Mission-critical communication equipment is installed in the DCs to ensure high availability of voice and data services. DCMU acts as a disaster recovery site for all the DCs in cases of eventualities. The latest developments in the data centre technologies like virtualisation, and storage management, have been already exploited for efficient management of data services.

- **IACCS:** The Integrated Air Command and Control System (IACCS) is an automated command and control system for Air Defence (AD). IACCS operations ride the AFNet backbone, integrating all ground-based and airborne sensors, AD weapon systems and Command and Control (C2) nodes. Integration with the other Services' networks and civil radars provides an integrated air situation picture to operators to carry out the AD role. IACCS offers connectivity for all the ground platforms and airborne platforms, as a part of the network-centricity of the IAF. It also facilitates real-time transport of images, data, and voice, amongst satellites, aircraft and ground stations. IACCS is expected to change the air defence facets and underlying paradigm in the times to come.
- **UDAAN:** The IAF Centre of Excellence for Artificial Intelligence under the aegis of the Unit for Digitisation, Automation, Artificial Intelligence and Application Networking (UDAAN) has now taken wings with its roots positioned at New Delhi. A big data analytics and AI platform has been commissioned for handling all aspects of analytics, machine learning, natural language processing, neural networks, and end computing

requirements. UDAAN AF has taken proactive steps to embed Industry 4.0 and AI-based technologies in its war-fighting processes.

Digitisation has given the required advantage from a functional perspective, but has also led to an increase in attack surfaces. The use of endpoints like PCs, printers, Personal Digital Assistants (PDAs), laptops, etc. are now an everyday affair and, hence, need to be handled carefully. Similarly, the AFNet backbone and its associated network components are also required to be protected and preserved. Information security in digital form is difficult to contain and maintain. Such attack surfaces need constant vigil and protection from emerging cyber threats. Cyber espionage and associated activities are required to be detected and stopped within an optimum time-frame.

Fig 4: Cyber Attack Surfaces (author's creation)



CYBER ATTACKS, MYTHS AND NEED FOR SECURITY

Passwords are like underwear: don't let people see it, change it very often, and you shouldn't share it with strangers.

—Chris Pirrilo

Cyber Attack: In the post-digital era of a hyper-connected digital world, the cyber related crimes are growing at an exponential rate, challenging the Law Enforcement Agencies (LEAs) to comprehend how to counter the growing shadow world of cyber crimes.[12] Various techniques and tactics are being applied by cyber criminals to fool people and information systems. Cyber attacks are steps, activities or actions performed by individuals/state or non-state actors/ organisations with a malicious and deliberate motive to breach information systems, computer systems, infrastructures, or networks. Some of the common types of cyber attacks include phishing, Distributed Denial of Service (DDS), malware based attacks, brute force attacks, Structured Query Language (SQL) injections, etc. A few of the common attack types are described in Table 2.

Table 2: Common Cyber Attacks[12]

S No.	Attack Type	Description
1.	Phishing	Phishing is a technique to fool people by sending malicious messages to innocent people to steal sensitive, personally identifiable information such as credit card and login information or to install malware.
2.	Denial of Service	A denial of service attack aims at interfering and compromising network availability, for instance, flooding a website with a huge amount of traffic, taking up the entire server bandwidth
3.	Malware-based Attack	Malware is a collective term used to describe different types of malicious software such as ransomware which blocks access to key components of the network, spyware which covertly gains sensitive information by transmitting data in the hard drive and different types of viruses disrupting certain components and affecting the system.

12. "7 Most Common Cybersecurity Threats and How to Mitigate Them", 10xDS, January 27, 2020, https://10xds.com/blog/common-cybersecurity-threats-and-mitigation/. Accessed on December 27, 2022.

S No.	Attack Type	Description
4.	Brute Force Attack	A brute force attack is simple in its approach to gain access to systems or online accounts, trying all the possible ways to crack the password using various algorithms and eventually finding the right one.
5.	SQL Injection	The SQL injection attacks the target's vulnerable websites to gain access to stored data. The attacker inserts the harmful code into a server using SQL and gains access to sensitive information such as user names, passwords and any amount of personal information stored in the database
6.	Man-in-the-Middle (MITM)	Man-in-the-middle attack, popularly known as eavesdropping attack, happens when an attacker manages to intercept and hijack a connection in a two-party transaction to eavesdrop.
7.	Cross Site Scripting (XSS)	A type of injection, in which malicious scripts are injected into otherwise benign and trusted websites
8.	Cross-Site Request Forgery (CSRF)	CSRF is an attack that forces an end user to execute unwanted actions on a web application in which they are currently authenticated

Cyber Myths: Issues with cyber security often stem from a lack of cyber security awareness as it is evident from the 2020 Cyberthreat Defence Report by the CyberEdge Group:[13] a lack of cyber security awareness has been identified as the biggest detriment to an organisation's cyber defences. No training on cyber security and persistent misinformation are the reasons for this lack of awareness. Since breaches, hacks, and attacks are evolving continuously, cyber security preparedness always remains behind and could result in a catastrophic outcome. It is, thus, important to be aware of the

13. Cyberedge Group, "2020 Cyber Threat Defence Report".

pitfalls, identify the attack surfaces and be aware of probable attacks on to identify and mitigate such attacks.

This will also lead to the formation of better cyber security policies. A few of the myths about cyber security are enumerated below:[14, 15]

- We're unlikely to experience a security breach.
- We've never experienced a cyber attack, so our security posture must be strong enough.
- Our passwords are strong enough to avoid a data breach.
- Anti-virus and anti-malware software are enough to keep us safe.
- Cyber threats only come from external actors.
- We've invested in sophisticated security tools, so we're safe.

CYBER SECURITY

If It's Smart, It's Vulnerable.

—Mikko Hyppönen

Cyber security is the collective process of protecting computer systems, networks, and programmes from cyber attacks. The ever-expanding cyber space has increased the incidents of cyber breaches for illicit gains. For an organisation like the IAF, the threat becomes manifold due to the involvement of state-sponsored actors. The field of cyber security is categorised into six main domains, namely, cyber-physical domain, information domain, network domain, cognitive domain, social domain, and transportation domain.

14. Barry O'Donnell, "5 Cybersecurity Myths and How to Address Them", WhatIS, March 16, 2022, https://www.techtarget.com/whatis/post/5-cybersecurity-myths-and-how-to-address-them. Accessed on December 25, 2022.
15. Craig Pollack, "14 Cybersecurity Myths and Conceptions", FPA, March 18, 2021, https://www.fpainc.com/blog/14-cybersecurity-myths-and-misconceptions. Accessed on December 25, 2022.

Table 3: Cyber Security Areas[16]

S No	Domain Name	Purpose in Function
1.	Cyber-Physical Domain	The cyber-physical domain is used to protect hardware, software, and important data or information. The cyber-physical system is used in several applications such as health care, military, transport, and industrialisation.
2.	Information Domain	The information security domain awareness exercise is used for correct teaching targeted at making computer users alert on information security. The information domain is used for monitoring, information storing, and conception.
3.	Network Domain	The network domain is used in sharing and communication. The network is one of the most important parts of protecting private records. The network must be ready with properties such as integrity, identification, non-rejection, and privacy.
4.	Cognitive Domain	The information must be property analysed and recognised and used in the field of cognitive decision-making. The cognitive domain is used in remote control applications in smart homes as well as in small commercial domains.
5.	Social Domain	The social domain in cyber security is important for assessments, executive side. It provides awareness on how organisations can be improved and arranged to react to cyber threats and protect data from cyber criminals who try to hack personal information.
6.	Transportation Domain	The transportation domain provides extraordinary quality or smart services to meet the customer's requirement. The Intelligent Transportation System (ITS) goals are improved reliability, accessibility, safety and efficacy of the transportation infrastructure.

16. Naik Bukht, et al., "Importance of Cyber Security and its Sub-Domains", *Journal of Information and Computational Science*, June 2020, pp. 473-485, https://www.researchgate.net/publication/342354467_Importance_of_Cyber_security_and_its_sub-domains. Accessed on December 25, 2022.

As part of ensuring policy generation/compliance checks/network monitoring (Process), and the creation of the required pool of manpower (People), the IAF formulated certain units/establishments to further the cause of cyber risk mitigation.

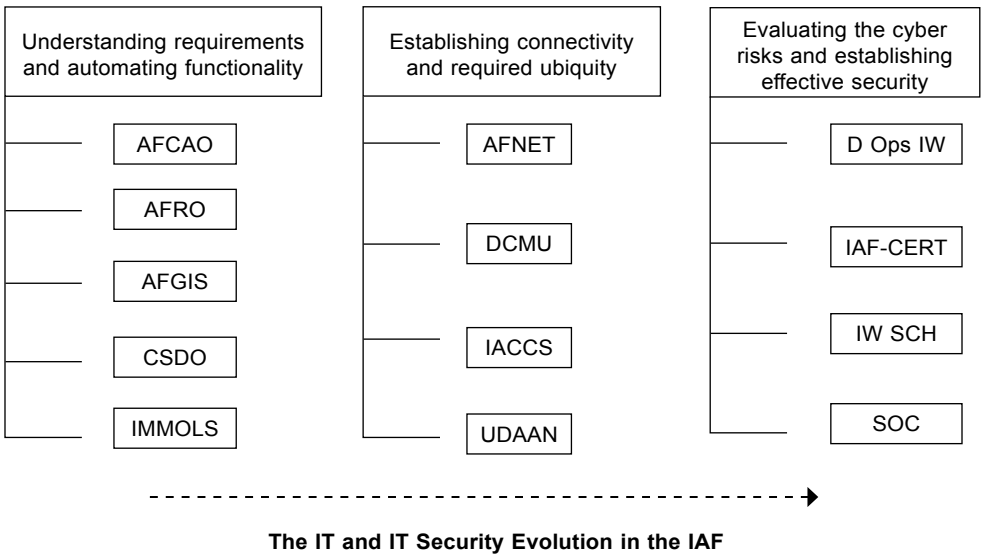
MITIGATION STEPS BY THE IAF

The digitisation journey for the IAF has surely given a platform for better administration and decision-making. The impetus on automation and efficient workflow has been achieved to a large extent by the use of IT. But as they say, "With great power, comes greater responsibility", and the power yielded by this digital and information revolution has also enhanced security issues related to data security, information pilferage and data tampering across all spheres. The IAF's data security policy, thus, gradually became the need of the hour, leading to the creation of various units/establishments involved in cyber security.

A comprehensive design with multi-layer security precautions for "Defence in Depth" was introduced by incorporating encryption technologies, intrusion prevention systems to ensure the resistance of the IT system against information manipulation and eavesdropping, as far as the AFNet connectivity is concerned. But, ensuring better technology covers only the "T" in the Process, People, and Technology aspects. The IAF was quick to realise, within the first decade of this century, that IT-enabled service and functionality is a double-edged sword. At one end, it provides the much-needed automation and connectivity, but that very boon, if unsupervised, may turn into a bane and haunt operations in the times to come. Thus, the "Process" and "People", along with the relevant "Technology" need to be brought in sync for effective operational advantage.

Establishment of Specialist Units for Mitigating Cyber Risks: As part of ensuring policy generation/compliance checks/network monitoring (Process), and the creation of the required pool of manpower (People), the IAF formulated certain units/establishments to further the cause of cyber risk mitigation.

Fig 5. Digital Journey of the IAF



Source: Author's Creation.

The agencies involved in cyber security in the IAF, at various levels and with different capabilities are enumerated below.

- **IAF-CERT:** The Indian Air Force-Computer and Emergency Response Team (IAF-CERT) was conceptualised in 2002. With the advancement of IT and computer power, information processing systems have become a force and efficiency multiplier for all organisations, especially the defence forces. With the spread of the internet an increasing rise of malicious programmes (worms, viruses, malwares, etc.) was observed. A need was felt to establish a specialist agency to deal with computer and network security and, hence, the birth of IAF-CERT. In the year 2000, Information Warfare (IW) activities were conceived by the Directorate of Conceptual Studies (DICOST), at Air HQ. Thereafter, in 2002, it started functioning as a cell of the Directorate of Operations Information and Electronic Warfare (IEW) at Air HQ. With the commissioning of the AFNet, the IAF moved towards Net-Centric Warfare (NCW). The importance of information security from the defensive IW perspective was realised. During the

year 2006, the requirement was felt for a dedicated agency to look after the defensive aspect of computer security in the IAF leading to the birth of the "IAF-Computer Emergency Response Team" (IAF-CERT). IAF-CERT gave the much-needed tool to the IAF for measuring its on-ground implementation of cyber measures vis-à-vis the policies given. Since then, IAF-CERT has grown into a robust establishment involved in cyber security audit, risk assessment, vulnerability evaluation and incident response.

- **Information Warfare School:** Information Warfare (IW) in the Indian Air Force has its genesis in the early 1990s. As an organisational element, it began functioning as a cell under the Directorate of Concept Studies, DICOST (Air HQ). Subsequently, it was brought under the Assistant Chief of Air Staff (ACAS) Ops Space in the Directorate of Information and Electronic Warfare and is now under the functional control of the Directorate of Ops (IEW) at Air HQ. The IW School started functioning as an independent unit from October 1, 2012. The basic roles and functions of the IW School are to conduct basic and advanced IW courses, conduct specialised capsules on information security, conduct IW exercises, conduct IW workshops and online IW familiarisation. The IW School is also involved in providing inputs to Air HQ on policy matters for formulating defensive and offensive strategies.
- **Security Operation Centre (SOC):** The SOC is an in-house team of IT security professionals that monitors the IAF's entire IT infrastructure, 24/7, to detect cyber security events in real-time and address them as quickly and effectively as possible. SOC is formulated to carry out tactical and real-time mitigation for a cyber threat detected. It is also responsible to create network monitoring rules and capturing logs for necessary analytics, as well as defining end-point security. SOC can be considered as the eye/ear/skin of AFNet, capable of sensing attacks, carrying out initial mitigation actions and informing IAF-CERT to deal with any eventualities.
- **Cyber Operation Centre (COC):** Formulation of the COC in the IAF takes the essence of IW operations to a whole new level. COC has been formulated

to provide a multi-faceted, technology-oriented but process-driven approach to certain specific elements associated with cyber security. It enables the IAF to carry out endpoint digital forensics, malware analysis and study nuances associated with exploits as a proactive measure. The addition of an Internet Security Operation Centre under the aegis of COC has provided the much-needed control for IAF internet machines and users.

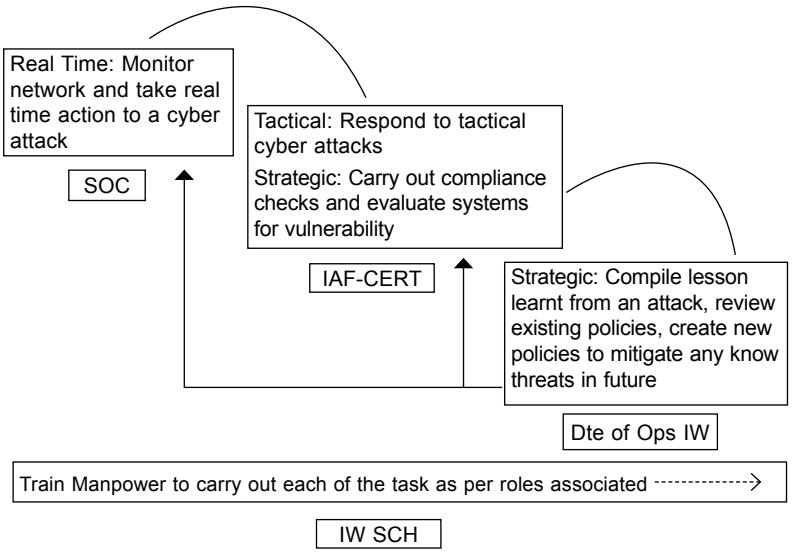
Since cyber warfare is an ongoing process, with no beginning or end, it is important to be prepared for every eventuality, so that, when the time comes, the IAF will be able to deliver the required results in the shortest possible time.

Awareness Programmes: The IAF has also been ensuring that knowledge about various cyber threats/risks and vulnerabilities is informed to its rank and file, irrespective of their direct involvement in the IW ecosystem. This is because IW is like breathing: everyone who intends to live, should know it.[17] Since humans are the greatest assets of any organisation, it is imperative that adequate briefing/information is provided to the air warriors to ensure better IW hygiene. This is done through the formulation of an Information Security Policy and regular release of Cyber Security Instructions (CSIs), Cyber Security Awareness (CSA), alerts, IW bulletins, etc. The cyber defensive posture of the IAF is depicted in Fig 6.

The IAF has also been investing time, effort, and human resources to ensure that offensive actions related to cyber can be performed as and when required. Since cyber warfare is an ongoing process, with no beginning or end, it is important to be prepared for every eventuality, so that, when the time comes, the IAF will be able to deliver the required results in the shortest possible time.

17. Md Mehedi Hassan Onik, Chul-Soo Kim and Jinhong Yang, "Personal Data Privacy Challenges of the Fourth Industrial Revolution", 2019, pp. 635-638. 10.23919/ICACT.2019.8701932

Fig 6: Cyber Defensive Process of the IAF



Source: Author's Creation.

CHANGING FACETS OF DIGITAL WAR

With the advent of new technologies, the Concept of Operations (CONOPS) related to war has taken a paradigm shift. In this increasing era of Network-Centric Warfare (NCW), the cyber attack surfaces have increased multifold. Information warfare now has gone "airborne". Smart Line Replaceable Units (LRUs)/ components being used in modern-day aircraft have a full-fledged software stack, along with data transfer protocols. If compromised, anyone can behave as a network member and jeopardise the whole operational mission. The effective marriage of Electronic Warfare (EW) and Information Warfare (IW) is very disruptive in nature and is likely to bring about a strategic level decision change when dealing with digital data.

Cyber space being a boundaryless, faceless and timeless entity, is capable of affecting all aspects of the war-waging capability of a nation. Cyber Psychological Operations (PsyOps) through available social media platforms, mails, notifications, etc., can demoralise the troops in peace as

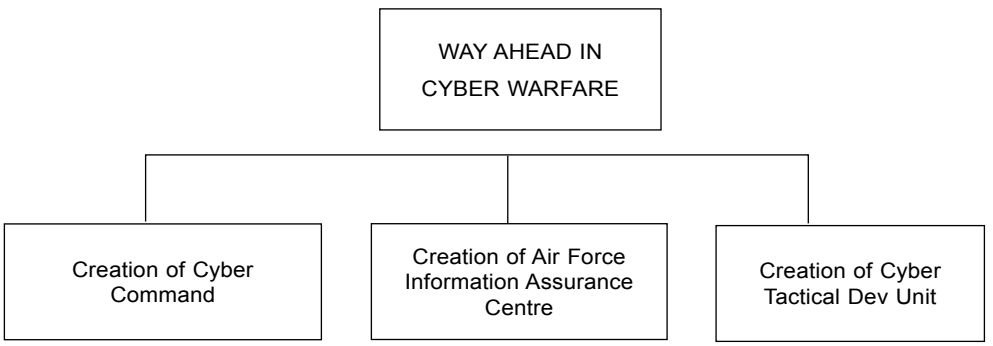
well as during an active operation. Cyber Influence Operations or CIOs by adversaries need to be curbed while developing our capability to undertake the same when needed. It is important to deal with each aspect of the cyber domain in a professional manner.

In order to mitigate such threats, it is important to segregate the technological aspects vis-à-vis the procedural ones and generate a framework for response and mitigation.[18] A cyber threat with respect to an information flow can be arrested provided that source, sink and underlying media are known and under control, along with the protocol being employed. Just like "Rome was not built in a day", it is important to generate strategic policies and tactical implementations, to counter the cyber security issues of the future.

ROADMAP: A WAY FORWARD

In order to control the narrative in the future and the outcome of a cyber war, it is important to have foresight and work upon building executable deterrence. The following is proposed as part of a policy decision, which will allow us to control the environment, actors and process involved in an effective manner.

Fig 7: Cyber Warfare: A Way Ahead



Source: Author's Creation.

18. Edward R. Griffor, et al., *Framework for Cyber-Physical Systems*, Vol. 1, "Overview", 2017.

- **Creation of a Cyber Command:** Formation of a full-fledged Cyber Command in place of the existing Defence Cyber Agency (DCyA) will provide the much-needed power to control all aspects related to cyber warfare. The formation of a Cyber Command will also bring India at par with the Western world, in terms of war-waging capability through cyber means.
- **Creation of an Air Force Information Assurance Centre:** This will take care of the strategic policies and defensive postures in cyber and information warfare in a dynamic environment. NCW will entail entities from all three Services and, thus, it is of utmost importance to ensure that the information asset is available under all conditions, whether it is peace or war-time.
- **Creation of an Air Force Cyber Tactical Development Unit:** Such a unit will be useful in short-term measures. It should be capable of creating cyber weapons as per the requirement and associated intelligence available. Such cyber weapons can be limited by time or space or both. Hence, it is important to have a unit which can keep track of all related incidents and identify a loophole (or bug), which can be turned into a vulnerability and exploited.

CONCLUSION

Organisations are under the constant pressure of being forced to react quickly to the ever-evolving and increasing number of cyber security threats. Since the attackers have been using an attack life cycle for cyber attacks, organisations have also been forced to evolve and create a vulnerability management life cycle. This article is an attempt to make the readers understand the cyber domain, along with its pillars and fundamentals. It also runs through various cyber security concepts and attempts to bust some of the myths associated with the cyber domain. The adoption of IT in the IAF has been showcased, along with the thought process of cyber security that is embedded in the organisation which has fuelled the establishment of cyber security agencies within the organisation.

The cyber domain and cyber physical systems are here to stay. One cannot remain oblivious to their presence, more so at the organisational level. The IAF's journey and history prove that the organisation has always been a leader in adopting technologies, as per requirement and availability. We should strive for a better, more resilient and secure cyber environment for achieving our functional and operational goals.

> Every worthwhile accomplishment, big or little, has its stages of drudgery and triumph: a beginning, a struggle, and a victory.
>
> —Mahatma Gandhi