OFFENSIVE AND DEFENSIVE CYBER OPERATIONS IN THE MULTI-DOMAIN BATTLE SPACE

ABHINAY SHUKLA AND VSV CHAITHANYA

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

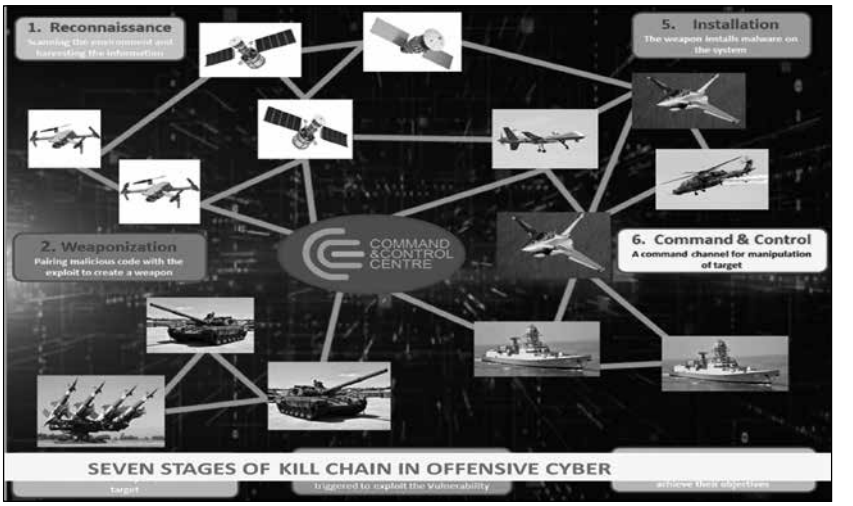
INTRODUCTION

Multi-domain battle operations are undertaken to exploit the advantages of employing the joint combat capabilities of all the forces participating in the conventional domains i.e. land, air and sea for a common operation. Our forces are entering a new era of theatre commands. Inclusion of two new domains i.e. the cyber and space domains, will function as a force multiplier for enhancing the competence, ability and endurance of our forces.

Group Captain **Abhinay Shukla** was commissioned in the Indian Air Force (IAF) on January 5, 2004. He is presently posted at an Air Force Station in the Eastern Air Command (EAC), IAF.

Squadron Leader **V S V Chaithanya** was commissioned in the Indian Air Force (IAF) on July 9, 2012. He is presently posted at an Air Force Station in the Eastern Air Command (EAC), IAF.

Fig 1: Cyber Space in Multi-Domain Battle



Source: T*he Cyber Defense Review 2017*.[1]

According to FM 3-12 Cyber Space and Electromagnetic Warfare, 2021, in the near future, cyber space will be increasingly utilised in congested environments where friends, allies and adversaries will transmit and process large amounts of data or information.[2] In such a dynamic cyber space, the vulnerabilities of own forces can be exploited and, therefore, having a strong cyber defence system in place is mandatory.

A country's armed forces can be operating in one of the three situations i.e. peace, No War No Peace (NWNP), and war. During peace-time, adversaries' actions may include planting an insider for espionage activities, gaining access to critical infrastructure and planting zero-day vulnerabilities for offensive operations during heightened situations. During NWNP, according to Nadiya Kostyuk, Scott Powell and Matt Skach, cyber aggression is expected which may include targeted harassment to military infrastructure.[3] Similarly,

1. Lieutenant General Paul M. Nakasone and Major Charlie Lewis, "Cyberspace in Multi-Domain Battle", *The Cyber Defense Review 2017*.
2. FM 3-12, Cyber Space and Electromagnetic Warfare, August 2021, Headquarters, Department of the Army, USA.
3. Nadiya Kostyuk, Scott Powell and Matt Skach, "Determinants of the Cyber Escalation Ladder", Spring 2018.

during war, an existential attack is highly likely. Therefore, it is essential to define the escalation ladders for offensive and defensive cyber operations during peace-time, NWNP and war-time.

Our forces are entering a new era of theatre commands. Inclusion of two new domains i.e. cyber and space domains will function as a force multiplier for enhancing the competence, ability and endurance of our forces.

Artificial intelligence (AI) is also now showing its presence in the Indian armed forces. AI, with deep learning features, may be used to defend own cyber space, as it can help timely detection of threats and anomalies in the systems. The powerful features of AI can be used by the adversary towards the creation of malwares or zero-day attacks or launching offensive cyber actions.

INDIAN SCENARIO

Cyber space operations are full of ambiguities, as they do not fit into the category of conventional wars fought in the air, on land and at sea. Secondly, the cyber attacks during peace-time can easily be construed as war. Unlike airspace, territorial borders and maritime boundaries, there is no defined cyber space. It is, therefore, essential to formulate a cyber security framework and escalation ladder that can be followed by all elements during a war. But to do that, it is important to appreciate the cyber security posture of our country.

CYBER ATTACK TRENDS

In October 2022, Tata Power, which, is a major power producer in India, reported a cyber attack on its systems. The malware attack on the All India Institute of Medical Sciences (AIIMS) in November 2022 lasted for more than 15 days, wherein approximately three to four crore patients' data was compromised and 1.3 terabytes of data was encrypted. These incidents tested the efficacy and preparedness of our cyber security agencies. In another incident, six major airports of India were targeted with

According to the Checkpoint 2023 mid-year cyber security report, India continues to be in the higher risk zone in the Global Threat Index Map.

Distributed Denial of Services (DDoS) attacks in April 2023, disrupting airport services for more than nine hours. Based on the above incidents, it is evident that Indian government agencies and critical infrastructure may regularly experience cyber attacks in the future too. According to the Checkpoint 2023 mid-year cyber security report, India continues to be in the higher risk zone in the Global Threat Index Map.[4]

As per the Mandiant Report 2023, the Russia-Ukraine War is one of the first wars where cyber power to conduct "disruptive attacks, espionage activities and information operations was used, along with the kinetic military operations."[5] No nation in this world can guarantee that it is immune to cyber attacks. However, the confidence level of a nation against cyber attacks is largely based on the offensive and defensive capabilities of that nation.

INDIA'S RANKING IN CYBER CAPABILITIES.

India ranks 10th in the global cyber security index as per the Global Cybersecurity Index (GCI), International Telecommunication Union (ITU) 2020.[6] According to the International Institute for Strategic Studies, the cyber capabilities of different countries were assessed based on their doctrine, command and control of governance, core cyber intelligence, resilience of cyber security standards, and offensive cyber capabilities. Some 15 countries were assessed based on the above mentioned criteria in three tiers. The countries and their standings are tabulated below.

4. "Checkpoint 2023 Mid-Year Cyber Security Report", https://pages.checkpoint.com/2023-mid- year-cyber-security-reprot.html.
5. "M Trends 2023", https://www.mandiant.com/resources/blog/m-trends-2023
6. "GCI by ITU 2020", https://www.itu.int/dms_pub/itu-d/opb/str/D-STR- GCI.01-2021-PDF-E.pdf.

Table 1: Comparison of Cyber Capabilities of Major Nations

Tier 1	Tier 2	Tier 3
USA	Australia	India
	Canada	Indonesia
	China	Iran
	France	Japan
	Israel	Malaysia
	Russia	North Korea
	UK	Vietnam

Source: International Institute for Strategic Studies, 2021.

The attacks on India's infrastructure and its low global ranking, clearly show India's lack of preparedness in cyber capabilities. There is, thus, a need to carry out the Strengths, Weaknesses, Opportunities, and Threats (SWOT) analysis of Indian cyber capabilities to understand how we can improve. But before that, there is a need to compare India's capabilities in the cyber domain with those of major nations (the USA, Russia and China), that are performing better in the cyber arena. This has been summarised in the succeeding tables

SWOT Analysis of India's Cyber Posture: Having compared India's cyber capabilities, the SWOT analysis is important to understand our strengths and weaknesses. Table 2 brings out these details:

Table 2: Comparison of Cyber Capabilities of Major Nations

Capabilities	China	India	USA	Russia
Strategy and Doctrine	Emphasises on sovereignty and information dominance, developing indigenous technology, and use of AI.	Emphasises on secure and dependable cyber space for individuals, companies and government and indigenous cyber security technologies.	Emphasises to achieve and maintain cyber space superiority, preventing intellectual property threats, foreign interference and working with allies.	Emphasises on sovereignty, cognitive and psychological aspects of cyber conflict and indigenous Information Technology (IT) production.
Governance, Command and Control	Formation of the Cyber Space Administration of China for civilian infrastructure and Strategic Support Force (SSF), to combine attack functions in cyber and space under a single commands.	Formation of the National Critical Information Infrastructure Protection Centre and Defence Cyber Agency (DCyA) .	Cyber Mission Force for centralised command and control for military and national critical infrastructure.	Federal Service for Technical and Export Control (FSTEK) tasked to lead defensive measures against foreign technology.
Core Cyber Intelligence Capability	Deployment of Skynet for video surveillance network. Deployment of Sharp Eyes , AI for social control. Golden Shield Project , technologyto collect, analyse and transmit information.	The National Intelligence Grid (NATGRID) provides intelligence on data sources. Intelligence Bureau (IB) and Research and Analysis Wing (RAW) monitor the internet traffic, includingthe social media.	National Security Agency (NSA) designated for military cyber capability. Central Intelligence Agency (CIA) for civilian cyber capability. Federal Bureau of Investigation (FBI) for domestic cyber capability.	Internal security moonitoring using SORM 1 - Responsible for meta data, mobile content and land line. SORM 2 – Monitoring internet traffic. SORM 3 – Other media.
Cyber Empowerment and Dependence	Reliance on foreign companies like CISCO, IBM, Intel and Microsoft for formulating national cyber security standards.	India also heavily relies on imports from the US, Japan and China.	Gathers civilian information using PRISM, and UPSTREAM from **Google, Apple, and Microsoft**.	Recruiting of patriotic hackers to launch offensive cyber operations.

Capabilities	China	India	USA	Russia
Cyber Security and Resilience	China has implemented the **Multi-Level Protection Scheme** to impose a heightened regulatory framework on network operators.	The National Critical Information and Infrastructure Protection Centre (NCIIPC), has been assigned the role of promoting policies across the nation		Russia relies on protection of critical infrastructure through a system known as GoSOPKA which comprises a public-private partnership.
Offensive Cyber Capability	China has proven its offensive capabilities by compromising the US government and commercial network on multiple occasions.	No available evidence on open sources regarding offensive capability.	The US possesses huge capabilities for offensive cyber action more than any other country.	All Russian intelligence agencies, namely, FSB, GU and SVR possess offensive cyber capabilities.

Source: International Institute for Strategic Studies,[7] 2021.

7. "Cyber Capabilities and National Power: A Net Assessment", International institute to Strategic Studies, 2021.

Table 3: SWOT Analysis of Indian Cyber Capability

Strength	**Weakness**
Cyber security and resilience. Strong defensive network. Isolated network for critical and military infrastructure keeping pace with technology advancement.	Governance, command and control Non-availability of national cyber security database. Public-private partnerships. Lack of defined risk matrix and cyber escalation ladders. Limited strategic alliances with allies and major nations.
Opportunities	**Threats**
Offensive cyber capability. Cyber empowerment and dependence. Artificial intelligence-based cyber offensive attacks Research and Development (R&D) involving academia, cyber security experts. Employment of cyber operation tools in weapon systems. Theaterisation will enhance synergy during joint operations between the armed forces.	Foreign vendor dependency and limited indigenous products. Limited capability for handling zero-day vulnerabilities or AI based attacks. Supply chain disruption. Inadequate measures to identify and detect insider threats.

The analysis shows that India has opportunities to enhance its cyber capability if there is a coherent policy and synergy of various elements, including Research and Development (R&D) and academia. To chalk out a way forward in this regard, understanding the challenges in cyber operations is important.

CHALLENGES IN CYBER SPACE

The biggest challenge in cyber space is to find the key factors that can be encountered during cyber operations. Once the challenges are understood in detail, risk assessment and mitigation can be put in place to achieve cyber deterrence. This section dwells on these challenges at the national and defence forces levels.

The challenges in respect of the national pursuit include:

Cyber space is highly dynamic and defending borderless cyber space is a big challenge. Also, it is very difficult to keep track of Tactics, Techniques and Procedures (TTPs) of the potential adversaries, their skills, and the resources available to them.

- Cyber space is highly dynamic, and defending borderless cyber space is a big challenge. Also, it is very difficult to keep track of the Tactics, Techniques and Procedures (TTPs) of the potential adversaries, their skills, and the resources available to them.
- Efforts required in tracing the source of an attack, as the attackers can use servers and resources from other countries.
- The swiftly evolving security and threat landscape. Advancements and complexity in the Information and Communication Technology (ICT) ecosystem in the country.
- Dependency on foreign vendors for electronic and Information Technology (IT) hardware and software.
- Putting in place optimised mechanisms for reduction in cyber security risk exposure to our critical ICT infrastructure.
- Integrating and coordinating the efforts of various cyber security agencies of the country for effective defensive and offensive cyber operations.
- Lack of international consensus.

The challenges in respect of the Indian armed forces in cyber space are:

- The art of conducting cyber war is a new arena as there have been no wars fought integrating the cyber space in the multi-domain battle space.

In the case of cyber space operations, the detection of malicious activity is known only when it is happening, as it does not provide an early warning before the activity begins.

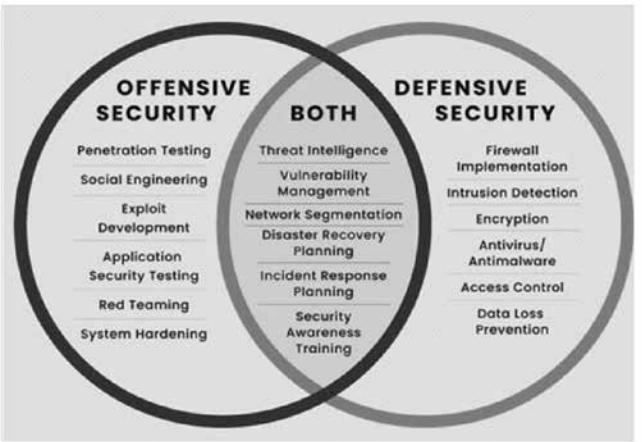
- The cyber weapon has to remain anonymous and unidentified by the adversary. The same depends largely on efficient and optimal use of the latest technology, tools and skills which are not readily available.
- One of the biggest challenges is the life-cycle management of our weapon systems. While the weapon systems have a life-cycle of 15-20 years, the ICT devices and software in general have a life-cycle of 5-6 years and the same are required to be upgraded periodically.
- Identification of skilled cyber security experts from various sectors including academia, private sector, security researchers, civil society, etc.
- Lack of infrastructure and R&D to secure the cyber space.
- Measures for ensuring technical cooperation and building international confidence.
- Efficacy of our security controls against severe/most advanced attacks like zero-day, DDoS, AI-based attacks, etc.
- The ease with which an adversary will be able to create malware and accelerate malicious activities by the use of AI-based tools like Chat GPT.
- To achieve a confidence level of 95 percent with respect to the capabilities of our deployed cyber security tools and our cyber security experts, to differentiate between false positives and false negatives.
- In the case of cyber space operations, the detection of malicious activity is known only when it is happening, as it does not provide an early warning before the activity begins.
- The situational awareness is hugely dependent on timely analysis of data from cyber sensors and the skill level of the cyber trained personnel including coordination between multiple cyber apex agencies.

- The challenge of maintaining cyber silence while passing on crucial information without interception is a key to attaining cyber defence supremacy.
- It is not practically possible to standardise a single benchmark / document for all the weapon systems due to varied functionalities. Therefore, the cyber protection team has to develop skills with respect to each weapon system.

CYBER OPERATIONS CLASSIFICATION

Cyber operations can be broadly classified into two major categories i.e. defensive and offensive cyber operations. The various processes/ activities involved in cyber operations are illustrated in Fig 1 below.

Fig 2: Offensive Cyber Security



Source: https://www.fortra.com/solutions/data- security/offensive- security[8]

DEFENSIVE CYBER CAPABILITIES AND SECURITY CONTROLS FOR CYBER RESILIENCE

Every nation develops its defensive cyber capabilities with the aim to safeguard its critical ICT infrastructure and military assets, including

8. "Offensive Cybersecurity, Fortra", https://www.fortra.com/solutions/data- security/offensive-security

various weapon systems, from the adversary's actions/attack so as to ensure continuity of operations at all times, including during heightened situations. This can be achieved only by ensuring the effectiveness and sufficiency of security controls for defence in depth.

Effective security controls are the key for defensive operations. It is, therefore, important to understand the important security controls categories and their deployment.

Cyber Security Controls for Cyber Resilience

In order to ensure cyber resilience, it is necessary that effective and efficient security controls are deployed. Some of the mandatory security controls that need to be incorporated are given below:

- **Segmented Network:** To isolate the threats from the adversary's actions/ cyber attacks from the integration points of own network with the outside world.
- **Continuous Monitoring and Situational Awareness:** Continuous monitoring using advanced tools, a skilled workforce for timely detection of anomalies and threats, and taking the desired mitigation actions.
- **Patch Management:** Automated patch management for the latest patches is to be done centrally for efficient remediation of vulnerabilities.
- **Asset Management:** To maintain an exact inventory of ICT infrastructure, including hardware and software.
- **Access Control Management:** To ensure secure access of data, application and resources to authorised personnel only, with controlled administrative privileges.
- **Configuration Management:** It is to be centrally managed to ensure, base lining, configuration version control, configuration changes, etc.
- **Audit:** Regular internal and external audits are to be conducted for comprehensive analyses and assessments of the security posture. This also aims at reviewing policies, procedures and security controls. It is primarily aimed at vulnerability assessment and threat analysis.

- **Log Management:** It is a continuous process which involves centralised log collection, analysis and event reporting to detect cyber attacks and security gaps.
- **Recovery:** In the case of a disaster/adversary action, recovery to a known (trusted) state in the shortest possible time for ensuring continuity of operations.

In the case of disaster/ adversary action, recovery to a known (trusted) state in the shortest possible time for ensuring continuity of operations.

DEFENSIVE CYBER SECURITY STRUCTURE

A recommended defensive cyber security structure for network security could comprise two teams i.e. Blue Team and Red Team.

- **Blue Team:** This team could comprise security professionals who are responsible for ensuring the overall security posture of an organisation. The Security Operations Centre (SOC) performs most of the roles of the Blue Team, as mentioned below:

  Incident Response and Management
  Auditing and Implementing Controls
  Security Monitoring
  Threat and Gap Analysis
  System Hardening and Configuration Management
  Digital Forensics
  Patch and Anti-Virus Management

- **Red Team:** This team could be responsible for simulating the adversary's actions/ attacks by carrying out operational security checks, penetration testing, black box testing, etc. on own network/ ICT infrastructure to assess the efficacy of the deployed security controls.

Unsupported software/ applications must not be used as they make the system vulnerable to cyber attacks. Only authorised and trusted personnel should be permitted to perform data transfer activities on/from the aircraft.

DEFENSIVE CYBER OPERATIONS FOR AIR POWER

According to Ball and Bryant, defensive cyber operations in air power must include the following:[9]

- **Real-Time Situational Awareness and Early Warning:** Regular monitoring with automated security tools of own systems, especially at ingress and egress points. There are commercially off-the-shelf available tools that monitor and analyse the flight safety critical avionic systems and their network, and provide real-time alerts about potential anomalies or cyber attacks. One such example is the cyber aviation tool named Spectris by the Israel Aerospace Industries (IAI) ELTA system.
- **Signature Reduction:** Stealth aircraft are not detected by air defence sensors due to their reduced signature. Similarly, it is important that the cyber signature/ footprint is reduced to the minimum by using air-gapped data links/ network. It is also important that the data being transmitted to or from the aircraft is encrypted for data protection.
- **Cyber Hardening and Protection of Avionic Systems:** All sub-systems of the aircraft must be hardened and base lining needs to be undertaken. Necessary security controls must be ensured at the integration points i.e. data ingress and egress. No patches/ updates are to be loaded to any sub-system without proper security testing. Unsupported software/ applications must not be used as they make the system vulnerable to cyber attacks. Only authorised and trusted personnel should be permitted to perform data transfer activities on/from the aircraft.
- **Decoys/Honeypots:** Akin to the use of decoys in defensive air operations, the use of honeypots in the form of fake networks and fake data will help in detecting the adversary's action without any impact on the actual

9. Ball and Bryant, https: //www.ndia.org/-/media/sites/ndia/divisions/combat-survivability/2022-webinar-slides/accs- short-ndia-15-mar-2022-bryant.ashx.

system. This can be used as a deception measure for the adversary's surveillance.

- **System Override Facility:** The aircraft must be provisioned with the override facility for use in the case of a cyber attack on avionics. This will enable the aircraft to recover and perform the intended function.

OFFENSIVE CYBER CAPABILITIES FOR CYBER SUPREMACY

Offensive cyber security operations aim at disrupting, denying, degrading and destroying the ICT infrastructure/ weapon systems of adversaries with the aim to incapacitate their war-fighting capability. The offensive actions that can be undertaken on an adversary are:

Espionage
Sabotage
DDoS /DoS (Distributed Denial of Service/Denial of Service)
Propaganda Attacks
Surprise Attacks
Data Exfiltration
Attacks on the nation's critical infrastructure like power grid, nuclear power plant, transportation, research establishments and government agencies.

In order to launch an offensive cyber operation, the armed forces need to follow the steps of kill chain process which are given below:

Reconnaissance
Weaponisation
Delivery
Exploitation
Installation
Command and Control
Action on Objectives

OFFENSIVE CYBER ACTIONS IN MULTI-DOMAIN OPERATIONS

In order to achieve the best offensive posture in cyber warfare, the intelligence support must be strong. A clear, defined policy on whether to use cyber weapons preemptively or during retaliation or covertly and overtly during the periods of cyber warfare must be available.

Offensive cyber operations can be undertaken on the adversary's weapon systems that are deployed in the land, air or sea domains. The stages of offensive operations will remain the same for all the domains. However, for the purpose of better understanding, an example of a possible cyber offensive that can impact air operations is discussed in the succeeding paragraphs.

As per the Alpha White Paper, 2017, offensive cyber operations that can be carried out on an aircraft include the following:[10]

- **Spoofing:** To modify data fed in the aircraft with an intention to steal the information. This can be done using the weakness of a the security controls or compromised avionics.
- **DoS:** Launching service disruption attacks during the aircraft's mission.
- **Counterfeiting:** Insertion of a malicious code with the intention to disrupt the mission. Insertion of bogus flight plans or fake messages.

Interference with following systems can also take place:

- **Communication Systems:** Enabling radio frequency channels to connect with rogue elements for information. Injection of false data through data link communication.

- **Navigation Systems:** Degradation of the Global Positioning System (GPS). Corrupting the navigation instruments to disorient the pilot.

10 "Aircraft Cybersecurity: The Pilot's Perspective", Alpha White Paper, 2017, https://www.alpha.org/-/media/ALPHA/Files/pdfs/news-events/white-papers/white-paper cybersecurity.pdf?la=en.

- **Flight Control Mechanism:** Injection of wrong inputs to the aircraft's flight controls. Limiting or the stopping the response to the fly-by-wire systems.

- **Safety Warnings:** Initiating wrong safety warnings to confuse the pilot. Disrupting the safety warnings.

- **Air Traffic Control (ATC):** Transmission of wrong information to pilots or traffic controllers.
  Issuing fake weather reports.

IMPLEMENTATION OF CYBER ESCALATION LADDER

In order to develop coherent and practical solutions in response to attacks, the militaries and cyber agencies must have a similar thought process for a particular type of threat from an adversary. Having an escalation ladder would bring the agencies involved in cyber warfare to a common platform, thereby initiating a logical and proportional response to a threat. As explained in the previous section, to achieve decisive results during the cyber space operations, a clearly laid down framework needs to be put in place in the form of escalation ladders for peace, No War No Peace (NWNP) and war.

The expected activities to be carried out during the NWNP and war situations are given below:

Peace (Preparatory Phase)

Defensive Cyber Operations

Risk assessment of own critical national and military infrastructure through vulnerability evaluation and auditing.

Preparation of a risk management framework. Deployment and validation of the necessary security controls. Mitigation of known risks.

Preparation of a Crisis Management Plan (CMP) and validation of the same for its efficacy.

Building cyber defensive capabilities.

Coordinating activities and conducting joint cyber exercises with allies in the form of supporting nations, academia, private sectors and other apex cyber agencies.

Research and development activities for indigenous cyber hardware and software.

Offensive Cyber Operations

Risk identification and assessment of the adversary's critical national and military infrastructure.

Reconnaissance for target identification and selection.

Intelligence gathering of the enemy's cyber capabilities. Planting actors for cyber espionage activities.

Creation of a skilled workforce to undertake offensive operations.

Penetrating the adversary's network in the stealth mode and persisting.

Creation of cyber weapons.

Weapon delivery using the supply chain management and other methods.

No War No Peace (Unstable Phase)

Defensive Cyber Operations

Reviewing security controls.

Increasing periodicity of vulnerability assessment of critical Infrastructure.

Stringent security controls to be implemented.

Close monitoring of all network integration points and revalidation of configuration checks on all perimeter security devices.

Intensive log analysis for detection of anomalies and network behavioural changes using automated tools and manually.

Deployment of experts (registered in the national security database) earmarked for undertaking cyber defensive actions.

Offensive Cyber Operations

Exploitation, installation and command and control stages of the kill chain to be extensively used for all systems.

Controlled DoS attack on government websites.

Targeted military interference.

Exfiltration and destruction of non-critical data for deterrence.

False propaganda using website hacking techniques.

Strategic cyber espionage.

Deployment of experts (registered in the national security database) earmarked for undertaking cyber offensive actions using the services of allies for controlled offensive actions.

War (Catastrophic Attacks)

Defensive Cyber Operations

All activities during NWNP will be performed extensively.

Recovery of national critical and military infrastructure with the support of cyber security experts from academia, private sector and other apex cyber agencies.

Offensive Cyber Operations

All activities performed during NWNP will be performed extensively.

Existential attacks on the adversary's military infrastructure and critical national infrastructure aiming at data exfiltration, network spreading and system disruption, etc.

Launching multiple DDoS attacks with the support of allies, including other nations.

Having seen all aspects of offensive and defensive cyber operations in the Multi-Domain Operations (MDOs), there are certain areas where we can work as a country and as Indian defence forces to strengthen cyber capability. These are:

The national critical infrastructure and armed forces' infrastructure is one of the centres of gravity in the war-fighting capabilities and the same needs to be safeguarded from external and internal threats.

Protection of Critical Military and National Infrastructure

The national critical infrastructure and armed forces' infrastructure is one of the centres of gravity in the war-fighting capabilities and the same needs to be safeguarded from external and internal threats. This can only be achieved if our defensive measures are a step ahead with regard to actions by threat actors, perpetrators and hacktivists.

Need for Real-Time and Close Monitoring of Our Cyber Boundaries

In order to ensure cyber supremacy, it is very important that we define our cyber space, consisting of physical, logical and cyber boundaries in order to isolate threats at integration touch points with untrusted networks. It is important that these integration points are closely monitored and stringent security controls are deployed to counter any cyber attacks, including zero-day, DDoS and AI-based attacks.

We need to continuously check the efficacy of our security controls based on Tactics, Techniques and Procedures (TTPs) of the Mitre Attack framework which defines the likely offensive actions by the adversary to compromise the systems/networks.

Cyber Capability Building

We need to build a cyber resilient force with a dedicated Purple Team that brings in the Blue and Red Teams together to improve the overall cyber security posture. Our cyber security teams should also participate in international exercises for exposure to enhance the skill building of own forces.

Creation of a National Security Database (NSD), comprising security experts with respect to offensive and defensive capabilities who can be utilised for launching cyber missions during hostilities is necessary.

To strengthen our defensive capabilities, our cyber protection agencies need to incorporate mechanisms for real-time detection and speedy prevention of cyber attacks by deploying the necessary security controls that are based on Artificial Intelligence (AI) and Machine Learning (ML) to combat the increasing cyber attacks.

At present, we are largely dependent on the security tools which are technology driven for detection and control of cyber attacks which are susceptible to compromise. Therefore, it becomes important that during heightened situations, our teams should be able to manually validate the events independently.

Developing Indigenous Cyber Capability

It is important that we reduce our dependency on foreign vendors. Towards this, we need to devise a mechanism for utilising the expertise of academia, apex agencies of cyber security and private partners for R&D activities which should primarily aim at developing indigenous hardware, software, cyber weapons, cyber security tools, and a hardened operating system and anti-virus capability to create multiple stealthy offensive teams distributed geographically that are capable of undertaking offensive actions in heightened situations.

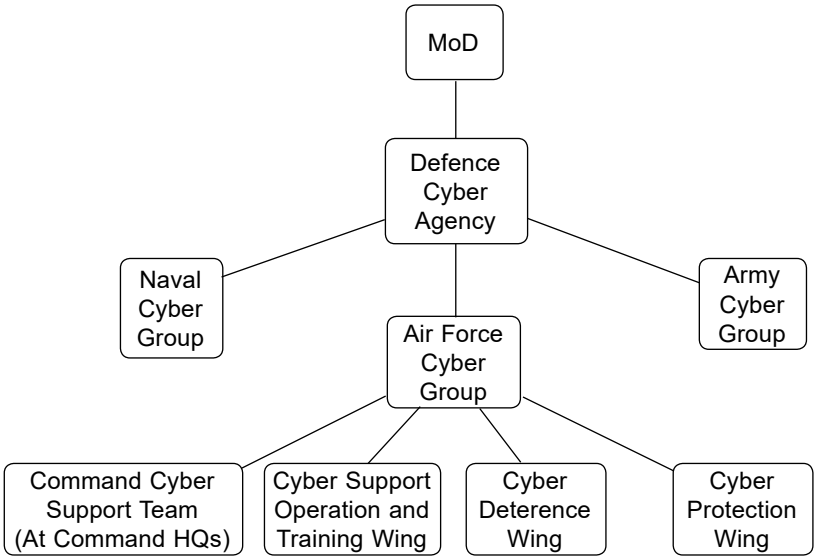
Offensive and Defensive Cyber Solutions for the Air Domain

We need to incorporate the cyber security solutions in our aircraft by providing cyber hardening/ production of avionics system, real-time awareness and early warning system, securing onboard networks and computer systems, threat modelling and remote cyber forensics. ELTA's Spectris is one such tool that provides avionics cyber security solutions.

There are modular cyber payloads like Pit-Viper Air which can be used for cyber missions, especially for offensive cyber operations. We also need

to explore the capabilities of launching offensive cyber operations during air campaigns.

Fig 3: Defence Cyber Agency Structure



It is important to ensure that we follow the security by the design approach for the weapon systems so that they are reasonably protected against cyber attacks.

Formulation of the common escalation matrix and policies that can be utilised by the armed forces and civilian agencies which clearly define the roles and responsibilities during the escalation is required. Also, we need to develop stringent policies with respect to generation, storage and transmission of classified data.

Coordination Between Various Cyber Security Agencies

India's National Cyber Security Policy (NCSP) was formulated in 2013. As on date, multiple agencies are responsible for protecting national infrastructure, businesses and individuals from cyber threats. However,

leveraging responsibilities on multiple agencies lacks peace, war and NWNP coordination during scenarios.

The responsibility of safeguarding the military ICT infrastructure lies with the Defence Cyber Agency (DCA) which comprises the Air Force Cyber Group (AFCG), Army Cyber Group (ACG) and Naval Cyber Group (NCG). The structure is as depicted above (Fig 3). The present groups will be able to undertake offensive and defensive operations. However, they need to be complemented with a skilled workforce. It is also recommended that their modules be attached to each Command Headquarters (HQ) for integration and decentralised cyber operations.

Unlike the Indian cyber organisation structure, the Department of Defence, of the USA has brought all the national and military cyber agencies under one head. The cyber mission force has allowed military commanders to plan cyber space operations in coordination, with other cyber agencies, thereby providing better situational awareness to execute operations successfully.

CONCLUSION

The participation of cyber space in the multi-domain battle space is a futuristic approach of major militaries across the spectrum. The United States has already formed a well-structured framework to align all the conventional forces towards this paradigm. China has also formed a Strategic Support Force to achieve cyber supremacy in multi-domain operations. India has started looking at cyber space operations from a national and military perspective, however, it is important to use cyber space operations as force multipliers for defending our critical ICT infrastructure and ensuring cyber supremacy. We need to continuously enhance our offensive and defensive cyber capabilities for an overall cyber security posture.