COMBINING CYBER WITH AIR FORCE OPERATIONS

RAMESH RAI

INTRODUCTION

Cyber technology has made its impact in the battle space, much as the technology of flight had a century ago, and evolved as a new domain. Cyber is now well acclaimed and established as the fifth domain of warfare, at par with the land, sea, air and space domains. We can safely postulate that any future conflict will have a large component of cyber warfare which may gain predominance as the years go by as no nation would resist the temptation to destroy, disrupt or confuse the enemy leadership, population, armed forces or the decision-making loops using cyber space.[1] Whether cyber would bring about a paradigm shift in the conduct of warfare or change the fundamental character of war will depend on how its doctrine and operational concepts get developed and integrated with the war-fighting concepts of the other domains. Conceptually, each domain develops and prepares to operate independently and collectively to use its prowess when called upon to do so, and it is certain that the cyber domain would follow a similar contour. Irrespective of its construct, cyber warfare is poised to emerge as a significant component of a future war.

Air Marshal **Ramesh Rai** VM (Retd) was AOC-in-C Training Command when he retired in July 2015 after serving in the Indian Air Force (IAF) for 39 years.

1. http://airpower.airforce.gov.au/APDC/media/PDF-Files/Pathfinder/PF211-Future-Wars-and-Air-Power.pdf.

Since a wide range of social, economic, political and military functionalities depend on computers, networks, the internet, electronic technologies and the electro-magnetic spectrum – in other words, on 'cyber space' – it is preordained that cyber warfare will be used to exploit this dependency to meet political and military objectives.

Broadly speaking, cyber warfare is the use of technology to penetrate another nation's/enemy's computers or networks for the purpose of causing damage or disruption.[2] Since a wide range of social, economic, political and military functionalities depend on computers, networks, the internet, electronic technologies and the electro-magnetic spectrum – in other words, on 'cyber space' – it is preordained that cyber warfare will be used to exploit this dependency to meet political and military objectives. Thus, the predominance of cyber warfare in a future conflict, which is deemed to be hybrid, is connatural. Computers and networks are embedded in every system of a nation's being, enabling administration, banking, business, industry, logistics, electric grids, communications, air traffic control, air space management, smart cities and much more, to function efficiently each day. It is the vulnerability of this very actuality that the enemy will exploit through cyber warfare and which a nation would have to guard against. The threat is real and a cyber attack on a government's Information Technology (IT) network could bring an entire nation to its knees. In April 2018, the small independent Caribbean nation of Saint Maarten faced a total public shutdown for an entire day when its IT network was hacked for the third time over a year.[3] A coordinated cyber espionage campaign was run by a group called "Turbine Panda" from 2010 to 2015 to help China acquire intellectual property needed to design and build its own C-919 airplane. The group successfully breached IT networks of many companies, including

2. Lt Col Steven J Anderson, USAF, "Air Power Lessons for an Air Force Cyber Power Targeting Theory", *The Drew Papers.*

3. https://www.weforum.org/agenda/2018/06/how-organizations-should-prepare-for-cyber-attacks-noam-erez/ https://securityaffairs.co/wordpress/71236/hacking/sint-maarten-cyber-attack.html.

Safran, Capstone Turbine, Ametek, Honeywell, General Electric, and others.[4] These examples highlight the extent and severity of cyber attacks. It is imminent that cyber forces could operate around the globe and with a much wider connotation than the battle space of the militaries, and would need to be addressed at the national level. The onus of protecting the nation from such cyber attacks will lie solely on the national leadership.

In the future, cyber space will pervade every conventional war-fighting domain more and more as our armed forces get increasingly dependent on computers, networks and information technologies to enhance their efficacy. This will create new and ever-increasing vulnerabilities.

CYBER SPACE AND ARMED FORCES

Since the armed forces will also be in the ambit of cyber space, the military element of cyber warfare will have to be culled out from within the national framework. The armed forces would have to protect not only their platforms, weapons, information, networks and capabilities but also conduct offensive cyber operations in the respective domains. In the future, cyber space will pervade every conventional war-fighting domain more and more as our armed forces get increasingly dependent on computers, networks and information technologies to enhance their efficacy. This will create new and ever-increasing vulnerabilities. The onus will be on those heading these conventional domains to be prepared to defend their cyber space from intrusions and prevent disruptions in their operations. At the conceptual level, integration of both non-kinetic and kinetic operations emerges as the key doctrinal concept for fighting a future war. Accordingly, the Indian armed forces will have to position themselves to develop cyber warfare capabilities to be employed independently or in support of their domain operations. This would entail developing both defensive and offensive cyber forces to counter the enemy's cyber capabilities. Irrespective of whether cyber operates independently or in support, it will have to connect with

4. https://www.computing.co.uk>ctg>news>china-espionage-c919.

operations in other domains as future wars would have a multi-domain connotation and combining the war-fighting tenets of each would be imperative.

CYBER AS PART OF THE FUTURE BATTLE SPACE

A future war in our context will have a pronounced cyber threat from China as it consolidates on its new operational concept of fighting an informationalised war. In the last decade, China has made considerable progress in developing cyber warfare capabilities in terms of its policies, restructuring organisations, building human expertise, and raising new establishments. China and Pakistan are known to be developing cyber warfare capability to deter a physically and technologically superior military adversary.[5] Given the above, and the operational character of the battle space as it obtains today, it is certain that a future two-front war will have a hybrid construct. The hybridity could be with a mix of regular forces using conventional weapons intermeshed with irregular forces using irregular tactics with the support of terrorists, insurgents, cyber intrusions, and possibly some dimension of social and political warfare. While the cyber intrusions with political, economic and social connotations would need a whole of nation approach, the armed forces would have to tackle intrusions into their cyber space so that their operations are not constrained or inhibited.

CYBER AND AIR FORCE OPERATIONS

The cyber space is a physical phenomenon that serves to host the Electro-Magnetic (EM) spectrum, computers, networks, flow of digital data and information, much in the same way as air hosts airborne systems (fighter aircraft, drones, missiles, etc.). Air forces in particular rely heavily on cyber space since most of their operations are synchronised, coordinated and integrated through the flow of information via computers, sensors, datalinks, information systems and information technology. The air force

5. https://usiofindia.org/publication/usi-journal/chinas-cyber-warfare-capabilities/.

will need to factor its cyber space uniqueness and control this domain to retain its freedom of action. This aspect assumes greater significance and relevance for the future, as its reliance on cyber space would be increasingly heavy as it transforms itself to a 5th Generation (Gen) force in the years to come. The Indian Air Force (IAF) is at the threshold of configuring an Operational Data Link (ODL) and translating to network-centric operations. It already has a secure encrypted Air Force Network (AFNET) operational since 2010, facilitating enhanced communications and data transfer for the Air Defence (AD) set-up. The Integrated Air Command and Control System (IACCS), connecting the data of all ground-based radar sensors and Airborne Warning and Control System (AWACS) rides on the AFNET. With the ODL configured, all its 4.5 Gen (Mirage, SU-30, Tejas and Rafale), 5th Gen manned (Advanced Medium Combat Aircraft – AMCA) and unmanned (Autonomous Unmanned Research Aircraft - AURA) platforms, Intelligence, Surveillance and Reconnaissance (ISR) systems, surface-based weapons systems would ride on the ODL to transfer data to and from the IAACS, between platforms and Communication and Control (C2) centres to complete all elements of the net-centric set-up. Networking primarily links all sensors, systems, weapon platforms and C2 centres for data to flow to create enhanced situational awareness and then to bring to bear the most appropriate weapon on the target, enhancing the efficacy and tempo of operations. The implication of becoming a 5th Gen air force is the vulnerability of the cyber space to intrusions by the enemy that could restrict, disrupt or inhibit air force operations. Hence, it would be imperative for the IAF to cultivate capabilities to defend or protect its cyber space.

From the above discussion, it emerges that the key doctrinal update for the air force would be to integrate the cyber domain into its war-fighting doctrine and operational concept. Air forces exploit the third dimension of the operational environment using combat and support systems to leverage speed, range, flexibility, precision, tempo, and lethality, and create the desired effects within and from the air. This will now require an intermesh with the cyber domain in both the defensive and offensive sense. Cyber defensive

The networked system is at risk owing to its construct and configuration, primarily at the points of interconnection and interaction with its clients. Any weakness even in a single system or its connect could disrupt the entire network and the results would be catastrophic.

capabilities would be required to defend cyber space and ensure mission execution, even when under a cyber attack. This cyber attack could be in the form of denial-of-service attack from outside a firewall, manipulating data from within a firewall, interrupting communications, taking control of a system, and others. In a networked arrangement, the vulnerabilities would be far too many since most combat, combat support, sensors and information systems would be connected with the ODL. The IAF must defend these to ensure assured access to cyber space.

DEFENSIVE CYBER OPERATIONS

Defensive cyber space operations are intended to preserve the ability to utilise own cyber space capabilities for projecting air power. The IAF's network-centric set-up would comprise a very complex mix of an encrypted data link, software controlled systems, 5th Gen manned and unmanned platforms, AWACS, space and airborne ISR, ground-based radars, AD systems, C2 centres, a host of mainframes to personal computers, modems, interfaces of Local Area Networks (LANs) to the IAF's intranet, the world wide web, civilian and military communication systems, navigation systems, and radios in all frequency ranges. The networked system is at risk owing to its construct and configuration, primarily at the points of interconnection and interaction with its clients. Any weakness even in a single system or its connect could disrupt the entire network and the results would be catastrophic. Hence, not only the entire system but each individual client has to be cyber protected and defended. This would be extremely critical. At risk is not only the external arrangement of the network, but also the software within individual systems and platforms which could be controlled or damaged to disrupt air operations.

In the future, manned and unmanned platforms would be increasingly dependent on software. These platforms would carry out internal communication through an internal data bus for various functionalities like fly-by-wire, auto throttles for engine control, computers for navigation, weapons aiming, threat management and many other solutions. The Jaguar, Mirage-2000, SU-30, Tejas, Rafale and AMCA fall in this category. The data bus, though primarily meant for internal communication within the platform or any system, would also serve for the integration into the IAF's network arrangement. It is through these external exchanges that the basic software of a system, including an aircraft, could get vulnerable to a cyber attack. The SU-30 that crashed on the Indo-China border on May 23, 2017, killing two pilots, is presumed to be the victim of such an attack from some foreign nation, which could include China.[6] Thus, the communication connections of the network and its clients, inherently serve as the conduit for breach of security. All such connections would have to be controlled and monitored to prevent cyber infiltration. The IAF's doctrine would have to account for these vulnerabilities and provide appropriate methods in its approach to cyber defence.

Cyber intrusions exploit system weaknesses, engineering techniques of computers, and human limitations to steal and bypass signal defences like firewalls and physical defences like passwords and machine-to-machine authentication which are primarily based on identification and authentication codes.

CYBER INFILTRATIONS

Cyber intrusions exploit system weaknesses, engineering techniques of computers, and human limitations to steal and bypass signal defences like firewalls and physical defences like passwords and machine-to-machine authentication which are primarily based on identification and authentication codes. Fundamentally, cyber systems can be infiltrated in

6. https://www.cybersecurity-insiders.com/china-cyber-attacks-indian-sukhoi-30-jet-fighters/

two ways, i.e. by physical and signal inputs. Physical infiltrations are made through the system hardware via the keyboard, mouse, cockpit controls, flight control, weapon system controls and removable media that provides physical inputs into a system. The first line of defence, therefore, would be to secure the physical inputs and outputs of a system. If these are not secure, the system is not secure.

Signal infiltration comes through existing indirect or direct connections to the network. These connections are typically LANs, infrared (IR) devices, Radio Frequency (RF) connections (radios), and modems (phone lines) wherever they may be in the entire geographical spread or layout of the IAF. This includes various Command Headquarters (HQs), bases, squadrons, radars, Surface-to-Air Missiles (SAMs), control rooms, etc. Any system, including a network with external connections, can theoretically be infiltrated. The number of potential entry points is limited only by the number of direct and indirect connections into the system. For instance, a system with an internet server is vulnerable to cyber infiltration from any computer connected to the internet. An isolated network with a modem is vulnerable to any computer that can call into it. Defence mechanisms to prevent signal infiltrations would have to be incorporated within the software and hardware by way of passwords, coded signals, firewalls, terminal identification, isolation, and system monitors. Every software system would need to have proactive and effective virus protection in place. To provide the best defence, these techniques must be customised, combined, and layered with one another.

CYBER DEFENCE: LAYERED APPROACH

Our cyber defence mechanism would, thus, need a layered approach. The first layer would be to ensure the integrity and security of the information environment from an Information Technology (IT) perspective to keep the physical and signal intrusions at bay. This layer would include designing, building, configuring, securing, operating and maintaining the information environment with IT security aspects fully in place, i.e. physical security, password protection, password encryption, data protection, data encryption,

firewalls, virus scanner, virus protection, etc. as discussed in the preceding paragraphs. This must be done in a proactive manner across the entire IT spread of hardware, software, data, individual users, system administrators, etc. without exception. The concept is to focus on the security from an IT perspective when configuring every part of the information sphere, particularly the ODL, IACCS, AFNET, data storage, LANs, L3 switches at our bases and Command and Air HQs, with emphasis on the security of data at rest and in motion within and across the IAF's information environment. This layer can be thought of as an umbrella protection against an agnostic threat. Our IT security measures must serve as a baseline to mitigate known vulnerabilities from within and from outside, covering a broad range of external threats. Unfortunately, even a perfect IT security baseline would not provide complete security. Defensive cyber space operations would be required to deal with the full range of cyber space threats.

The next layer would be to create defensive forces to defend own cyber space capabilities from active threats, specifically for the protection of data, networks, software-enabled platforms/devices and other designated systems by defeating cyber space intrusions as they occur. Defensive cyber space operations must be seen as active cyber space defence activity that would allow us to interdict an adversary after he penetrates the first layer.[7] Accordingly, this layer would involve creating abilities to detect, analyse, and mitigate threats that cross over. As opposed to the first layer which was threat agnostic, this layer would be threat specific. Defensive cyber operations in this layer are executed against specific threats with malicious capability and intent to affect our cyber environment that have outsmarted the first layer. Since such outmanoeuvring of the outer layer could happen across the entire information sphere, defensive cyber operations must be prioritised to occur first at the most critical part of the environment so that our operations are not disrupted. In the air force jargon, these operations could be said to be akin to defensive counter-air operations, wherein air power takes on the intruding enemy forces with own defensive forces.

7. n. 2.

EVOLVING DEFENSIVE CYBER FORCE

In evolving a defensive cyber force, the IAF would have to identify key parts of the information environment that are vital for its operations. For example, if the IACCS system is a priority for the defence of the nation, then, perhaps, this is the priority. Step two in this example would be to technically map the key elements from the sensor-to-shooter, the network and systems over which data would move to the command centres for attack assessment and then to the entity directed to respond. Mapping defensive operations would involve determining the systems in play with their own vulnerabilities and those at the points where one system connects to another and then by linking vulnerabilities with adversary capability and intent, the priority risk areas on which to focus our defensive effort get identified.

Defending the IACCS or any other key cyber environment would involve a run of cyber ISR functions to detect and analyse the kind of threat and the defensive measures that need to be employed. These defensive measures could be taken internally within own cyber space or preemptively taken outside our information environment to stop or block the attack (offensive counter air). The essential task would be to hunt the friendly cyber arena for intruded threat/s and direct an appropriate internal response in almost real time. Cyber ISR capability would be the key to this function. Conceptually, it calls for a robust cyber ISR scan capability over the entire network, along with the capacity to create the defensive cyber forces capable of mitigating a detected threat. This would be a tough call and the core aspect of cyber defence, requiring cyber experts with knowledge on each individual system and component that makes up our cyber space. This capability emerges as the key determinant of our ability to provide freedom of manoeuvre in own cyber space. We must, however, optimise the employment of forces across both layers of defence as each would affect the other, but that discussion is beyond the scope of this article.

Potential vulnerabilities are not limited to the network and its clients but would also include the entire 'ecosystem' of which maintenance, engineering, logistics, spares management, fuel management, gases, etc. would be

essential parts. Measures to protect the Integrated Material Management Online System (IMMOLS), Electronic Maintenance Management System (e-MMS) are equally important as these may provide a bridge for malware to jump from the IAF's intranet to the aircraft platform. Beyond aircraft related systems, there are systems at the airfield that rely on the cyber space and EM spectrum that directly support air operations, i.e. air traffic management, meteorology, provisioning electricity, command and control centre at the base, etc. Cyber space will remain a contested domain, as our enemy would know our dependability, and it is unlikely that we will ever have continuous or uncontested cyber space superiority; however, in the same way as we approach operations in the air domain, we must have enough control of the cyber space at the time and place of our choosing to get our operations through.[8] While cyber defence is the lynchpin to providing freedom of movement in the cyber space, offensive cyber capability is where the cyber domain offers targeting payoffs for employment of air power. Developing offensive cyber forces would be equally important.

NEED FOR OFFENSIVE CYBER FORCES

A discussion on offensive cyber operations is based on the premise that these operations would have the potential to meet the security challenges by combining with the offensive operations of the air force. In doctrinal terms, it calls for culling out a cyber-air targeting philosophy that would adequately meet the mission objectives.[9] Given the lack of warfare experience in the offensive cyber arena, one could approach the cyber-air integration by adopting the air power targeting philosophy as a start point and then determine the extent to which cyber combines in neutralising the plethora of the IAF. Over time and as integration of the cyber and air domains pick up momentum, clarity will emerge on its operational utility and efficacy. Perhaps, and more importantly, offensive cyber weapons would match or even better the versatility of the air domain targeting, as they would also

8. Ibid.
9. Ibid.

A sound doctrine for targeting would have to be established, based on the capability of cyber forces that the IAF is able to develop, and the technology, expertise available, employment philosophy and experience gained.

have the potential to address targets across the full range of operations, i.e. from the strategic to the tactical and from the conventional to irregular war. The aim at all levels would be to deny, disrupt, or degrade enemy capabilities, either directly or indirectly (through deception), either by acting alone or in concert with air power. At the strategic level, cyber could target the larger nodes of enemy systems whose disruption would provide an outsized leverage for coercion, while, at the tactical level, support local actions, depending on the demands of the tactical situation. For example, a cyber attack on an AD radar or Surface-to-Air Missile (SAM) system on the ingress route of a strike as part of Destruction of Enemy Air Defence (DEAD) or Suppression of Enemy Air Defence (SEAD) operations would typically meet the air force's tactical requirement in what could be termed as a localised issue. But at some point, a sound doctrine for targeting would have to be established, based on the capability of cyber forces that the IAF is able to develop, and the technology, expertise available, employment philosophy and experience gained.

INTEGRATION OF OFFENSIVE CYBER AND AIR OPERATIONS

Integration of offensive cyber space operations could follow the approach described above for integration into the offensive actions of the air force. The existing Air Operations Planning Process (AOPP) could be applied to cyber space operations as well when analysing targets and evolving a campaign plan. Such an approach would be easy to comprehend and implement since our war planning cells are familiar with the process. Irrespective of which targeting philosophy is applied while evolving the Concept of Operations (CONOPS), i.e. Warden's idea of "enemy as a system" or the "centre of gravity approach", at the analysis phase, and to arrive at the best weapon

to be employed, the planners ought to consider cyber as another tool/weapon in their arsenal. Such an approach would require little adaptation in integrating offensive cyber forces with offensive air action. The key element would be for the commander to articulate his preference for engaging the target and the extent of employment of the offensive cyber forces to achieve the desired effect. Whether the target is to be engaged by cyber alone or a combined cyber-air action, would be his call. The role of cyber in every conceivable aspect, i.e. shaping operations by deception or disruption of the enemy's information sphere or creating uncertainty in the opponent's decision matrix or a destructive effect or whatever else is to be conceived by the commander, would need to be clearly spelt out. Some unique cyber effects that could be employed are paralysing enemy AD and communication systems using malware, executing feints, selective computer destruction of combat systems through online manipulation and invading C2 systems of the enemy, to mention a few. In Operation "Orchard" the Israeli Air Force had used offensive cyber forces by employing electronic warfare technology like the "Suter network attack system" of the US Air Force and had fed false targets to manipulate the Syrian radars during its aerial strike on a suspected nuclear plant at the Al Kibar site in the Deir ez-Zor region of Syria on September 6, 2007. This example elaborates on the type of cyber effects that could form part of the commander's CONOPS and decided fairly early during the planning, as preparation of cyber forces is a long and arduous task. It involves penetrating the enemy cyber space to exfiltrate data, model the target and evolve the attack malware. While it can be imagined that offensive cyber operations could play a key role in the early

While it can be imagined that offensive cyber operations could play a key role in the early stages of the war to shape the battle space since it can be developed during peace-time, it is expected that the role of offensive cyber will increasingly provide opportunities for a significant impact throughout the air campaign as experience is gained.

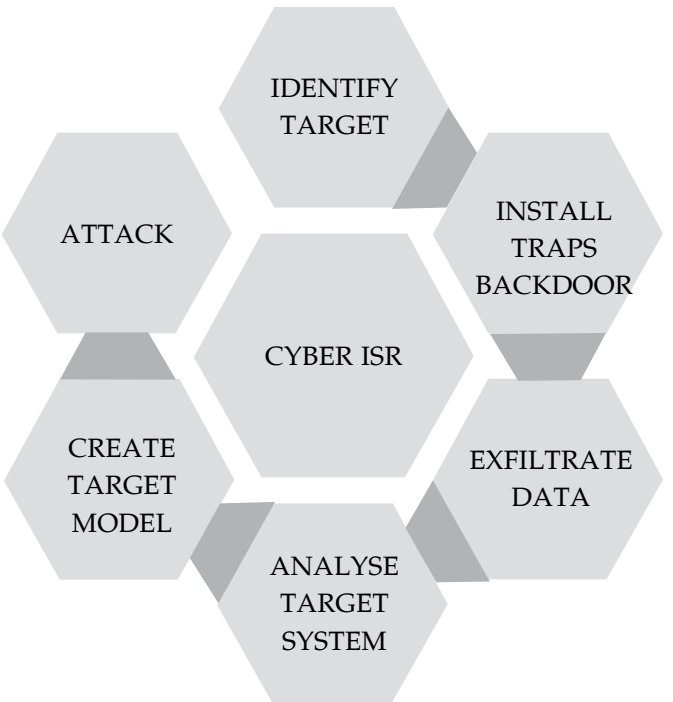
stages of the war to shape the battle space since it can be developed during peace-time, it is expected that the role of offensive cyber will increasingly provide opportunities for a significant impact throughout the air campaign as experience is gained.

EVOLVING OFFENSIVE CYBER FORCES

The ability to deliver offensive cyber space effects requires three critical elements i.e. target identification and characterisation; access to the target; and, tools to deliver the intended effects. This process entails a long preparation time and, therefore, cyber targets need to be determined early in the planning process. The first step is to carry out cyber intelligence of the enemy cyber space and get a sense of the information that travels and is stored on the digital and computer networks to map the operating environment.[10] Thereafter, it is broken down into various layers for determining the hardware through which the information flows, its e-mail address, Internet Protocol (IP) address, detailing of information flow paths (links) and routing and storing digital information (nodes) to name a few.[11] In this manner, after prolonged surveillance and reconnaissance activities, the target is identified. After the target is identified, cyber personnel install cyber traps in the form of malware to enter its defences through the backdoor, i.e. penetrate the firewalls, etc. Thereafter, exfiltrate the data for subsequent analysis of its algorithms, protocols, codes and structure to create a target model in terms of its software architecture and then evolve the requisite cyber tools (techniques and procedures) for an attack. Fig 1 captures the essence of the process involved.

10. https://www.airuniversity.af.edu/CyberCollege/Portal/Article/Article/1238539/isr-and-cyberspace/
11. Ibid.

Fig 1



This description is not meant to oversimplify the process of evolving cyber forces or integrating cyber space operations into planning and execution. In fact, the whole process of evolving cyber forces is highly complex and technically challenging. The targets have to be worked upon for a long time and developed years in advance to be kept ready for launch. At the end of such activity, the preparation of cyber space target folders giving the details of targeting solutions developed for use to make mission plans is involved. The true genius of this entire effort and ability is the human operator. The availability of adequately trained and capable manpower emerges as a challenge. Presently, there is no cyber branch in the IAF, and officers with knowledge of the tactical planning aspects would have to be professionally developed to learn enough about cyber space and then integrate cyber space and air operations. Alternatively, the aeronautical engineering (electronics)

branch officers or airmen could carry out the cyber portion to be married by the operations branch officers into campaign planning. The second challenge is the technical capability of developing cyber forces as described above. Since target configuration and software are constantly upgraded, these cyber forces have to be modified or updated on an almost continual basis to prevent collateral damage or fratricide.[12]

DEVELOPMENT OF FULL SPECTRUM CYBER POWER

Having broadly discussed the need for defensive and offensive operations and how these may be integrated into our air operations, it clearly emerges that for a full spectrum cyber power, we would need to develop robust cyber ISR, cyber defence and cyber offence capability. Evolving cyber forces and a doctrine for their employment would depend on how the cyber-air capability is employed to accomplish the mission. The air force would need to work out tactics, techniques, procedures in the cyber space for its operations. In terms of targets, the air force could consider C2 centres, communication nodes, computers, ISR, logistics networks, maintenance networks, critical information storage systems, navigation and guidance systems of platforms like aircraft, ships, missiles, drones and precision-guided munitions, and assets in outer space and their supporting infrastructure. The list is endless and the task is daunting, but must start in earnest.

The IAF has an extensive cyber security policy in place since 2007 which was revised in 2012 and 2018. The policy covers the entire gamut of cyber activity including the AFNET, LAN, internet and weapon systems. It lays down in detail the various procedures to be adopted in the IAF's cyber space. This policy would form the first layer of security, as per the discussion in this article, as it elaborates on the cyber security posture that the IAF needs to adopt with respect to technology and emerging threats. Our cyber space would be a contested arena in any future war, as stated earlier, hence, developing cyber defensive forces as the second layer of defence would be imperative. The aim of cyber space defence is not only to obtain freedom to

12. Ibid.

operate in own cyber space but to protect the entire information environment to mitigate threats and vulnerabilities. The IAF ought not to be content in merely defending its cyber space, but must also, as a policy, employ cyber offence to support its own operations by manipulating, degrading, disrupting and destroying enemy infrastructure and/or capabilities. It must recognise that a cyber space attack, like all forms of attack, can be designed to generate effects in the physical domains.

CONCLUDING THOUGHTS

The intent of this article is to highlight the need for cyber space operations to be integrated with IAF operations, since availability of freedom to manoeuvre in cyber space would be imperative to win a future war. The IAF has laid out a security policy which serves well as the first layer of defence. It could now look forward to developing the entire gamut of actions to exploit cyber power in its entirety. For this, creating defensive and offensive cyber forces, along with robust cyber ISR emerges as the key operational construct. A way forward has been discussed. Cyber-air operations can create powerful synergy and there lies huge benefit in combining existing air concepts with cyber as a starting point. The availability of trained and qualified manpower would be a challenge that will have to be overcome. While this article has focussed on cyber space operations in support of air operations only, there is a broader implication of cyber security at the national level for which developing a policy, organisation and authority would be mandated to tie it all together. The armed forces play a key role in defending national security within their sphere and must, thus, be prepared to defend it in all domains, including cyber space. This implies creating situational awareness of the cyber space, cyber forces and a mechanism to integrate cyber space operations within the national framework to accomplish the assigned missions. The Indian Air Force would do well to take the lead, as its dependence on cyber space is absolute.