Seminar Report

CYBER WARFARE: CHANGING CONTOURS OF WARFIGHTING

Seminar Coordinator: Colonel Subhasis Das
Rapporteurs: Debasis Dash, Ameya Kelkar and Anushree Dutta

Centre for Land Warfare Studies
RPSO Complex, Parade Road, Delhi Cantt, New Delhi-110010
Phone: 011-25691308; Fax: 011-25692347
email: landwarfare@gmail.com; website: www.claws.in

The Centre for Land Warfare Studies (CLAWS), New Delhi, is an autonomous think tank dealing with contemporary issues of national security and conceptual aspects of land warfare, including conventional and sub-conventional conflicts and terrorism. CLAWS conducts research that is futuristic in outlook and policy-oriented in approach.

Printed in India by
Bloomsbury Publishing India Pvt. Ltd.
DDA Complex LSC, Building No. 4, 2nd Floor
Pocket 6 & 7, Sector – C
Vasant Kunj, New Delhi 110070
www.bloomsbury.com

CONTENTS

EXECUTIVE SUMMARY

- The constants of the cyber domain are the speed of operations, the factor of uncertainty and the complete lack of indicators. War fighting doctrines will require adapting to these constants.
- Models or simulations pertaining to the effect of concerted cyber attacks on critical infrastructure like power grids, air traffic control, financial systems, railways and transportation networks etc, do not exist. Hence, it is difficult to predict the effect of such disruptions on national war fighting capability.
- Cyber warfare is driven by individuals. The threat posed by such individuals and small groups has been demonstrated time and again in digital space. This can turn into a battle winning factor for any nation which can ensure the consolidation of effort, centralized planning, and collective execution.
- The governance of cyber space is getting extremely complex because of the mix of international and local stakeholders.
- Cyber weapons are the new weapons of mass destruction/ disruption, where the mass is made up of assets and information.
- The theories of deterrence which have stood the test of time through the era of nuclear brinkmanship fall flat in the cyber context because there is complete obfuscation of attribution.
- In the context of cyber offensive operations, there is a need to evolve a common understanding of the targeting philosophy between the military and non-military sectors.
- Future wars may be fought largely in the human mind. Since this constitutes a paradigm shift in the art and science of warfare, there is a need to examine afresh the methodologies to fight this war. The primary aspect which needs to be is the content and media of communication in cyberspace.
- Cyber space, in the current form, is not suitable to be subjected to national laws or policies. The Indian government agencies

including the Armed Forces should first invest in mapping the real players in cyber space.

- The Government needs to move fast towards the establishment of regulatory agencies which can draw out statutory terms and conditions, disclosure agreements etc, for companies/developers to operate in the country.
- A secure knowledge management system and a common human resource (HR) management system for the cyber space would be a positive endeavour to achieve integration and availability of skilled manpower. Training for cyber warfare has to be an incentive driven national mission and cannot be left to a few agencies or organisations.
- The level of sophistication used even by terror outfits such as Al-Qaeda and ISIS in their overall cyber operations are more complex than most countries can handle at present. Precision targeting and stealthy cyber weapons are being used in the field of espionage and other disruptive activities. Such advanced threats to national security will require technical deterrence capability in addition to other forms of deterrence.
- National Information Infrastructure is continuously under attack. The problem is further exacerbated since almost all the Indian information infrastructure including the critical ones are running on imported software, hardware, chipsets, etc.
- The vulnerability of satellites spans across the kinetic, electronic as well as the cyber domain. Increasingly satellite systems, are getting connected to the internet and use more generic commercial standards and protocols, thereby increasing their vulnerability.
- To evolve a working public private partnership in cyberspace, formal working groups should be created with representation from the Government, private companies and users.
- Amendments to the Information Technology (IT) Act needs to be put into place to keep it updated with the current information sharing scenario.

- In the current security scenario of disorder and conflict, intelligence holds a high priority for the Armed Forces. Intelligence gathering is rapidly shifting to cyber space.
- A numbers of agencies are carrying out cyber intelligence activities in India; however currently, they suffer from a shortfall in data handling capabilities, translation services, cryptanalysis and automation.
- Buying technology is not a long-term solution in the cyber domain. Comprehensive indigenisation is the only way forward.
- In the operational and tactical battle space, widely networked systems like communications, logistic networks, and information systems are highly vulnerable. Few nations are working on cyber injection attacks at the tactical scenario using mobile and aerial platforms–hence, the threat is real and near.
- Responsibility and ownership of networks which constitute cyber space must be clearly defined, and agencies/sectors have to be made fully accountable and legally responsible. Service providers should also be made to compensate for any breach in their security arrangements, which also include any theft or loss of information.
- Military grade standards should be extended to cyber hardware and software.

DETAILED REPORT

A National Seminar on '*Cyber Warfare–Changing Contours of War Fighting*' was conducted at Manekshaw Centre, Delhi Cantonment on 14 July 2017. The Seminar was conducted by the Centre for Land Warfare Studies (CLAWS) under the aegis of the Army Management Studies Board – Army Training Command.

Aim

The Seminar was aimed at analysing *existing laws and policies, associated shortcomings, threats, challenges and recommend a way forward*. It was also aimed at *evaluating capabilities,* with a specific focus on the *role of various agencies*.

Modalities of Conduct

A one day Seminar was conducted at Ashoka Hall, Manekshaw Centre, Delhi Cantonment on 14 July 2017. The participants were from different government departments and agencies, three services, strategic community, veterans, industry, Research and Development (R&D) organisations and academia. Selected army officers dealing with cyber aspects in policy formulation, planning and training from Command and Corps HQs also participated.

Speakers

- Lieutenant General DR Soni, VSM, GOC-in-C, HQ ARTRAC
- Dr Gulshan Rai, National Cyber Security Coordinator
- Alok Joshi, Chairman National Technical Research Organisation (NTRO) and ex-Chief Research and Analysis Wing (R&AW)
- Captain Raghu Raman (Retd), Reliance India Limited
- Arun Sukumar, Head Cyber Security and Internet Governance Initiative, Observer Research Foundation
- Brigadier Manjeet Singh, DACIDS(DIARA), HQ IDS

- Lieutenant General Davinder Kumar, PVSM,VSM** (Retd) former Signal Officer in Chief
- Amit Sharma, Additional Director, Defence Research and Development Organisation (DRDO)
- Major General Ajeet Bajpai (Retd), DG National Critical Infrastructure Information Protection Centre (NCIIPC)Colonel Deepak Puri, DG Sigs
- Colonel KPM Das (Retd), CISCO
- Major General SK Pillai, VSM (Retd), Tata Power SED
- Marc Kahlberg, CEO, Vital Intelligence Group, Israel
- Major General MU Nair, ADGSI & ACIDS(Int), HQ IDS
- Colonel Dinesh Kumar, Military College of Telecommunication Engineering, Mhow

The aspects covered and the salient observations/recommendations of the Seminar are given in the following paragraphs:

Inaugural Session

While setting the tone of deliberations to follow, Director CLAWS indicated that the dimension of cyber warfare was distinct and unique because the security agencies of a nation are expected to operate in a zone of ambiguity and darkness. Accurate information and intelligence about the enemy is a prerequisite of successful military operations; however, in the cyber domain, offensive and defensive operations have to be carried out against shadowy adversaries, rapidly emerging technologies and vague targets. It is as much a cognitive war, as a war of ascendancy in capacity and capability. The other area where cyber is distinct is because it has a significant effect on the other traditional dimensions of warfare like land, sea, air and space. This relative zone of grey, however, provides a unique opportunity, where the genius of a few dedicated operators can disrupt the adversary in all dimensions and can have a force multiplier effect. Director CLAWS pointed out the constants of the cyber domain which are the speed of operations, the assurance of uncertainty and the complete lack of indicators. The

speaker also highlighted that cyber warfare can easily spill over into the civil space and cause collateral damage. This aspect has not been understood and negligible models or simulations exist pertaining to the effect of concerted cyber attacks on critical infrastructure like power grids, air traffic control, financial systems, railways and transportation networks, etc. The merging of the military and non-military space also creates challenges in the response mechanisms; hence, there is a pertinent need to earmark roles, develop capabilities, assign responsibilities, and accountability amongst the various stakeholders.

The Keynote Speaker highlighted that cyber warfare continues to be a subject of intense discussion and debate. It cannot be denied, that in the present context, enhancement in capability and capacity has taken place, but most of it has been haphazard and discrete. There is a pertinent need to take stock as to where the nation stands, where we would like to reach, and what needs to be done to achieve the same. The modern connected world offers a unique paradox. While digital connectivity is enhancing the quality of life of global citizens, it is also making everyone vulnerable. Nothing seems to be safe as long as it is connected to the ubiquitous digital space because in some part of the world there will be a young brilliant mind working towards hacking and cracking the network. There is a natural propensity of such individuals to act against powerful organisations like a state department or a nation. In some cases, the adventurism is replaced by the need for monetary reward or ideological indoctrination. The threat posed by such individuals and groups has been demonstrated time and again in digital space. This can turn into a battle winning factor for any nation which can ensure the consolidation of effort, centralised planning and collective execution. The acme of skills would be a cyber attack which can bring the adversary nation to a standstill, without a shot being fired. Unlike traditional warfare in which the adversaries are much likely to be forewarned and forearmed prior to the launch of the hostilities, in cyber warfare the target is not likely to be aware that it is under attack, which makes it lethal and destructive. Even though the effect of these attacks may not be immediately visible, they have the capability to bring entire

cities and nations to a standstill, instilling chaos and confusion in the population and weakening the resolve of the nation.

China has reportedly raised a specialised cyber warfare unit called Unit 61398 manned by razor sharp IT whiz kids with a single point agenda. Such units can continue to operate even during peacetime with complete anonymity. They also bring in an element of control while at the same time contribute to messaging and signaling to the adversary. India's Cyber Security Policy 2013 covers a wide range of topics ranging from the institutional framework and emergency response to the indigenous capability building. However, the key would be to translate this Policy into sound strategy, which would require coordination among different agencies and institutions, overriding turfs and comfort zones. The need of the hour is a detailed roadmap specifying the base capabilities desired to combat threats, the schedule of acquisition, the associated economics, and the future development roadmap. The cyber domain of warfare cannot remain open-ended any longer. The Policy should also lay down the terms and conditions for launching India's offensive cyber operations, the key to future national security and war effort. A realistic and pragmatic introspection is needed regarding the Indian organisations, capabilities, technological expertise, secrecy and security of systems, requirement of motivated human resource, mastermind(s) to steer offensive capabilities, and economics. If need be, a government decree needs to be issued for the overarching coordination, control and accountability to achieve the overall objective of national security. Unlike the attack by kinetic weapons, cyber warfare may not yield immediate visual effects with bloody results, which can motivate and spur the victorious and probably disheartened and destroy the vanquished. Hence, the degree of motivation required amongst cyber warriors needs to be very high as they would remain anonymous, unsung heroes, with only their small teams aware of their successes and failures. From the technology standpoint, India needs to invest and develop hardware and software tools indigenously, so that capabilities remain up-to-date. The legal net must also be expanded to cyber space so that the horrors of cyber warfare don't affect the hapless population. Laws must be collaborative in nature so that

nations must adhere to them, failing which they would incur penalty, embargo or sanction. In the military context, fully Network Centric Warfare (NCW) is the requirement of the day; however, in reality, we are operating in a broad mix of technologies, manpower and equipment, some of which are of older generations. However, with time, most ground/air/satellite based sensors, navigation systems, battle field management systems, target designation and tracking systems amongst others have become connected and dependent on cyber space, which makes them vulnerable to attack. Hence, effective military strategies and concepts are needed to counter cyber attacks as also define rules of engagement, tactics and low-level drills to empower system operators and commanders adequately.

The National Cyber Security Coordinator highlighted the symbiotic relation between technology and risk. While the complete absence of risk would be utopian, we may attempt to mitigate the same through governance. However, the governance of cyberspace is getting extremely complex because of the mix of international and local stakeholders. The connectivity and applications (cloud and virtualisation) on the internet is largely international while content is predominantly local. There is a unique formula of evolution playing out between the state players and cyber criminals. While cyber crime is leading on to new technologies, the states are countering the same through newer technologies leading to a continuous development cycle. Today, cyber weapons should be termed as the new weapons of mass destruction/disruption, where the mass is made of assets and information. Malicious malware like Stuxnet affected limited numbers of machines in 2010, while the June 2017 WannaCry attack affected an estimated 8,00,000 machines in 150 nations. This trend of mass attacks is only likely to grow. Discussions on the adaptation of the Laws of Armed Conflict to the cyber domain, is still in its infancy. There is a Budapest Convention for Cybercrime but there is no such law for cyber war or cyber terrorism.

The requirement to develop indigenous capability is paramount. The Speaker highlighted certain instances where niche expertise on certain key technology areas is not easily available in the nation. The availability of funds is not a plaguing problem any longer. What is

the need of the hour is a holistic and collaborative effort from the Government, defence, the vibrant civil sector and industry.

Session I: Emerging Challenges in the Cyber Domain

Cyber threats are both existential and real. However, it would not be prudent to approach the same as we have been attuned to in conventional warfare. The existence of an identified enemy, intelligence of enemy buildup and mobilization, own countermeasures and counter maneuvers have no relevance in cyber war. The manifestations of cyber war are primarily in the cognitive domain. This may include propaganda, false news and influencing of public opinion to create social divisions in the run up to the hostile engagement. The social media itself has the power to gauge the national mood which is quite evident today as we are witnessing a standoff with China in the area of Doklam. The theories of deterrence which have stood the test of time through the era of nuclear brinkmanship fall flat in the cyber context because there is complete obfuscation of attribution. In addition, any flag or indication of players is likely to be fake; hence, national escalation control mechanisms should be robust. A number of positive steps have been taken in the Indian context, which includes the establishment of the office of the National Cyber Security Coordinator, the framework of information exchange between major stakeholders like the NCIIPC, CERT-In, etc. The Standard Operating Procedures for the Public Private Partnership model is also in place. However, resources will always be limited and there is a pertinent need for partnership, especially in cyber defence. In the context of cyber offensive operations, there is a need to evolve a common understanding of the targeting philosophy between the military and non-military sectors. Targeting which has not been thought through, could well be at cross purposes to the national objective. Hence, there may be a requirement to evolve guidelines and delineate targets into the military and non-military domains.

The Sixth Dimension of Warfare

Cyber warfare and its effects need to be examined entirely differently from what is being done today. When war changed its theatre of

operations, for eg from land to sea, entirely new doctrines emerged. Today, cyber warfare is shifting from disruptions, denials and kinetic effects (the physical dimension) to a completely different space. We could possibly be left behind in a time warp if we do not study its effect on the sixth dimension – The Human Mind. Our reluctance to accept that future wars may be fought largely in the human mind may result in trying to fight the war of the future using tools and techniques of the present or the past. Since this constitutes a paradigm shift in the art and science of warfare, there is a need to examine afresh the methodologies to fight this war. The primary aspect which needs to be addressed is the content and media of communication. Terrorist organisations like ISIS have graduated into high technology modern platforms and disseminate professionally prepared content which has succeeded in influencing the target population. On the other hand, the government and law enforcing agencies are trying to reach and influence the same target population using archaic methods and old world media. Mere pumping in of funds, training programmes and education will not serve the purpose unless the methods to address the mind are altered. Even with huge monetary budgets, dedicated resources and intrusive actions like the PRISM programme, the United States of America was unable to solve the problem(s) of Chinese hacking or ISIS indoctrination. One way of addressing the challenge of communication would be to address the subliminal mind of the target audience rather than the conscious mind. Experiments all over the world have proven that addressing the subliminal plane is more effective in conveying messages. Drafting of new laws and policies simply will be of limited use as the adversaries have no respect for such laws and regulations. We need to accept that it is a paradigm shift and doctrines need to be changed completely. Slow, incremental changes will not yield the desired results. The way forward is to acknowledge the challenge, leverage the national capability as against government capability, collaborate and cooperate with multiple disciplines and rebuild delivery capacity.

Cyber Laws, Policies and Regulatory Mechanisms

The fundamental question which needs to be addressed is: whether cyber space, in the current form, suitable to be subjected to national

laws or policies? In 1996, MasterCard and Visa along with a consortium of information technology (IT) companies developed what is called the Secured Electronic Transaction (SET) protocol, to ensure the security of Card based financial transactions made over the non-secure internet. The main feature of the SET protocol was that it was dependant on the collaborative effort between the consumer, merchant and the service provider. While server-to-server communication operated by the financial companies was secure and safe, it required the users and merchants to carry out security requirements including installing special software, use of personal identification number (PIN), etc. SET could not achieve the goal of its developers who had visualised its acceptance as the de-facto standard for e-commerce transactions. Some financial frauds were reported which could be attributed to lack of adherence to the security requirements at consumer or merchant level. This further led to the development of 3D secure by VISA and MasterCard which is in today across the globe and is the global standard. What is important in this example is that neither governments or consumers or merchants had any role in deciding the standards or protocols, success or failure notwithstanding. The laws and policies for e-commerce have been decided by small consortiums, groups or companies mainly within North America and Western Europe. This model of control is likely to continue and organisations like the Internet Engagement Task Force will decide the rules of the game keeping most nations, governments and users out of the loop. The shift from IPv4 to IPv6 has been on similar lines and most national governments were not stakeholders to the decision.

Typically cyber space is made of a number of pipes, tubes and devices that are interconnect with each other, about which there is a fair degree of information and shared stake. But, unfortunately, no attempt has been made to map the actors behind the scenes who form the crucial layer called 'App layer'. In India, the top five smart phone players are Korean (Samsung) or Chinese (ViVo, Oppo, Lenovo and Xiaomi). The top five Apps in India are Whatsapp, Facebook Messenger, SHAREit, UCBrowser and Truecaller which are from foreign players. The government, military, common users or the law

enforcement agencies are unaware as to the terms of agreement based on which the license of the Android mobile operating system has been provided to the smart phone manufacturer. Neither is the user completely sure about the end user/privacy agreement which is the contract between a user and the App developer. Hence, it would be naïve for us to really believe that in a country dominated by Chinese and foreign players, it would be easy to protect or regulate the Indian cyber space.

Indigenous manufacture would be an ideal solution; however, the reality is that the nation is decades away from self-sufficiency. Hence, in the current context, the Indian government agencies including the Armed Forces should recognise the problem and invest in mapping the real players in cyber space. They will include the players in the hardware and the App space. The Indian government needs to move fast towards the establishment of regulatory agencies which can draw out statutory terms and conditions, disclosure agreements, etc., for companies/developers to operate in the country. The rules of the game need to be evolved by the regulatory agencies and users made aware of the same. This would be the first step towards more effective regulation in cyber space and to ensure security of the nation. Once the ecosystem has been mapped out and the actors have been made part of the partnership with the nation, laws and policies dealing with the humanitarian, economic and social fallout of cyber warfare can be evolved.

Synergy between Organisations and Delineation of Tasks

Cyber organisations around the world are witnessing transformative changes. The United States of America has a well-established and inclusive structure backed by an information operations strategy. In 2010, the US raised a cyber command (the status of the United States Cyber Command, has since been raised to that of a Unified Military Command in August 2017), with 27 agencies under its ambit and a personnel strength of around 25,000. At the apex level, there are about 103 teams with 6,200 personnel which augment the resources of the individual service components. China, on the other hand, has revamped its structure with the creation of the People's Liberation

Army (PLA) Strategic Support Force, which has under its ambit the Network Information and Operation force, amongst others. The Information and Operation force is further divided into the 2nd, 3rd and 4th departments with the former looking after traditional military espionage, the 3rd department looking after cyber-attack and code breaking operations and the 4th department looking after Electronic Warfare and Electronic Intelligence. This force has a strength of around 7,000 to 10,000 personnel. On the other hand, the non-governmental forces dealing with the cyber domain is around 60,000 personnel. Israel has a specialised cyber arm called Unit 8200 and the strength is estimated to be around 3,000 with a budget of around US$ 1.5 billion. On a comparative index, India's investment in human resource and its budget allocation is minimal. The office of the National Cyber Security Coordinator has taken a number of initiatives including dialogues with stakeholders. The interim National Cyber Coordination Centre (NCCC) which is under establishment as the Threat and Situational Awareness Project (TSAP) will eventually develop it into a full-fledged central executive body. This organisation will look into the internet at Meta data level and assess the threats in the Indian cyber domain. We already have the NCIIPC which has been looking into the critical infrastructure and functions under the aegis of NTRO. NCIIPC has come out with standard operating procedures for various critical sectors. In the context of the Armed Forces, the Defence Cyber Agency that has been approved as an interim measure will get converted into fully-operational Command. This will eventually bring the critical numbers and capability to the operational formations.

An immediate area of concern which needs to be addressed is the cyber response structure in the states and sectors such as industry, transportation, etc. Multiple stakeholders are a natural fallout of the basic nature of cyber space, and India's approach towards the challenge has also been similar, which has now resulted in a multitude of agencies with similar agenda. What is the need of the hour is the synergy between these stakeholders, resolution of overlapping responsibilities, breaking down of silos and generation of mutual trust. A secure knowledge management system and a common HR

management system for the cyber space would be a positive endeavour to achieve integration.

Session II: Cyber Warfare – Tools/Techniques and Future Trends

The cyber threat envelope is galloping forward at an unprecedented pace while the response mechanisms are always playing catch up. Even an air gapped network does not provide security today. Cyber malware can now be injected into a system using a drone or radio waves. The US reportedly has two squadrons of C-130s specifically for injecting viruses through airwaves. The future battle is going to be fought increasingly in the electronic and cyber domain; hence, there is a need to align India's offensive and defensive capabilities likewise.

Cyber Weapons and Advanced Threats to National Security

The weaponisation of cyber space is characterised by increasing levels of sophistication both technically and cognitively. The levels of sophistication used by terror outfits such as Al-Qaeda and ISIS in their overall cyber operations are more complex than most countries can handle at present. Precision targeting and stealthy cyber weapons are being used in the field of espionage and other disruptive activities. Modern cyber weapons can primarily be classified into two major categories, ie the survivability class and the confidentiality class of weapons. The survivability class consists of weapons which are designed to attack the computer systems that control dams, power grids, etc., and the confidentiality class consists of remotely activated trojans, zero-day exploits or exfiltration payloads. The US PRISM programme is an integrated confidentiality class weapon programme. Modern cyber weapons consist of a delivery vehicle like emails/websites/firmware, navigation unit which can achieve a high degree of targeting and the payload which defines the nature of the weapon. What adds to the nature of threat is that these systems are modular and it is possible to interchange these subsystems to create a new type of weapon in real time/a short period of time. Commercial anti-viruses are unable to detect such malware. An example of modular weapons would be the Stuxnet, DUQU, FLAME

series which were released one after the other. Stuxnet and DUQU had the same delivery and navigation system while the payload was completely different. The incorporation of kill switches and accurate fingerprinting also makes the detection of the weapons difficult. Terrorist organisations and cyber criminals are using four specific and readily available techniques to evade law enforcing agencies. These are the Dark Web, Crypto Currencies, The Dark Net Market Places and advanced Encryption. Ingenious methods of utilisation of these techniques enable terrorists and cyber criminals to wipe out their traces and data. Such advanced threats to national security will require technical deterrence capability in addition to legal deterrence. Trust and responsibility at the individual, organisational and global levels are needed, else cyber space will continue to be in danger.

Securing of National Critical Information Infrastructure

For information infrastructure to be termed as 'critical', it needs to satisfy any of the four parameters, i.e. it should affect national security, national economy, public health or public safety. Presently, information infrastructure may include the networks used exclusively by the military, the non-critical information infrastructure and the critical information infrastructure. In 2014, the need for a specialist agency examining and defending India's critical information infrastructure was felt in the government and the NCIIPC was established with a clear mandate and the associated authority, resources and budgeting. CERT-In continued with the role of protection of non-critical information infrastructure and the military was responsible to protect its own networks. Typically zero-day vulnerabilities, spear phishing attacks, compromise of sensitive systems and documents are reported on a regular basis. This is further exacerbated since almost all the information infrastructure including the critical ones are running on imported software, hardware, chipsets, etc. The data regarding infected systems is alarming. It would not be an understatement to say that most of the Indian systems are affected or the user is unaware that his/her system is affected. Fixing of detected vulnerabilities is a continuous process involving time and money. However, the patched systems are safe only till the next round of exposure to new

vulnerabilities. NCIIPC attempts to gather inputs from the Security Operation Centers (SOCs) of various sectors in terms of detected cyber vulnerabilities and disseminates it to the other entities along with some value addition, to prevent these entities from falling prey to cyber threats. As part of mitigation strategies a proactive control on the execution of malware code by disabling cookies, disabling script execution are useful methods. Containing the infected network population by stopping east-west network traffic is also effective in networks which have the controls built as part of the design. The next logical action is the isolation of systems to ensure that exfiltration of data does not take place. The NCIIPC has also undertaken the Responsible Vulnerability Disclosure Program, a voluntary programme which has yielded significant results. A programme has also been set in motion to use AI based predictive analysis, to detect an abnormal network traffic pattern in real time and predict a threat. A need has also been felt for developing experimental cyber ranges to simulate threats, so that threat assessment can be conducted without shutting down live systems. A set-up to check and issue certification for critical components is also being established. The evolving technology of Quantum Computing is being closely watched by the professionals involved in the task of protecting information infrastructure, as this can enhance security capabilities manifold. On the flipside, this technology in the wrong hand may also create havoc. While a number of actions are in the pipeline, the establishment of the NCIIPC has undoubtedly given the desired direction and impetus to the quest to protect critical information infrastructure. There is a need to build in a security mindset within the decision makers in the sectors with such critical assets.

Cyber-Space Convergence: Securing Assets and Services

Today, we are noticing a cyber space convergence which is largely unregulated and extensively exploited. Satellites typically spend two to three years in the making and around a decade or two in space. They are a more vulnerable than the systems on the ground as they cannot be physically accessed. The vulnerability of satellites spans across the kinetic, electronic as well as the cyber domain.

Increasingly satellite systems, which traditionally were niche products with proprietary protocols and serving limited users, are getting connected to the internet and use more generic commercial standards and protocols. Wireless attacks on networks are a growing trend, which makes satellite networks extremely vulnerable. With miniaturisation and multiple payload carrying capacities, the target value of satellites is increasing by the day. Even indigenous satellites have a significant dependence on imported components including firmware. With the opening up of the space sector, privately owned and operated satellites are likely to see fructification soon. Since most satellites have dual use role, economic considerations tend to overshadow military and security concerns. Modern satellites provide a single point hub for multiple services and many of the functions are software controlled; hence, a disruption in even a minor subsystem can have catastrophic effects. Vulnerabilities like sensor manipulation, antenna misalignment, the effect on thrusters, compromise of telemetry signals and data downlinks, etc., cannot be denied using purely cyber means. Mitigation mechanisms would include the use of end-to-end encryption for all processes, including cyber vulnerability as part of the design process, early patching of vulnerabilities, establish a trusted player ecosystem and legally binding agreements and terms of use.

Public Private Partnership Model for Cyber Security in India

The main players in the cyber security triad are the government, the private companies (both Indian and multinational) and the common citizen. While the purpose of all players may be similar, there is a huge dichotomy in thought between the players. The dichotomies may be appreciated and justified, but this divergence is also the primary reason why India, in spite of its advantages is far from being a fully-reliant, knowledge-based nation. Unlike in the US and Western Europe where the large IT companies and consortiums are in the forefront, in India, the government is always the primary stakeholder in the cyber security domain. We may define two types of Public Private Partnership (PPP) models. The Horizontal or the non-hierarchical model which is implementable in case there is

complete trust between all parties and the Vertical model where the central government is at the apex and the rest of the players perform a subordinate, guided role. The Vertical model is the de-facto model in India which is also the sub-optimal model. In spite of very large private sector footprints in the sector, the role play of these companies/working groups is very limited. There may be a case to reverse or alter the Governance model. The private sector is equally responsible for the impasse as it is reluctant to share information about its own breaches for the sake of protecting its professional reputation. The success of a PPP model would depend largely on sharing of accurate information in a timely manner. Large private companies need to go beyond mere business interests and Small and Medium Enterprises (SMEs) need to be brought into the system. The entire SME ecosystem is extensive and can deliver the goods if supported and nurtured by the Government and the departments of the armed forces like the Army Design Bureau, etc. It can now be reasonably deduced that post the establishment of the NCCC; there will be a defined and well-articulated policy to achieve commonality of purpose between the private sector and the Government. In the context of the defence sector, a major vulnerability remains the fact that all systems and networks are delivered by system integrators who may have a tendency to cut corners at every stage due to financial considerations. The solution would be to have an in-house system integration capability like has been attempted successfully by the National Informatics Centre. Some recommendations for the PPP model could be enumerated as follows:

- Formal working groups should be created and it should be representative of all the departments, private and government.
- A carefully crafted and examined template for the cyber security of a particular sector (for eg power) needs to be designed and implemented so that, if successful, it can be implemented in other sectors.
- Cyber education and awareness needs to be present at all levels of formal education.
- Amendments to the IT Act need to be put into place to keep it updated with the current information sharing scenario.

Session III: Cyber Warfare and the Indian Armed Forces

Cyberspace and Intelligence Acquisition in the Military Domain

In the current security scenario of disorder and conflict, intelligence holds a high priority for the Armed Forces. Intelligence needs to be examined in the context of the 'Intelligence Enterprise' and 'Intelligence Gathering in Cyberspace'. The term 'Intelligence Enterprise' is borrowed from the US Army. The Intelligence Enterprise comprises people, the processes, the infrastructure and the national intelligence efforts. It is aimed to develop a high level of situational understanding at the national, strategic, operational and tactical levels in a complex environment against determined and adaptive adversaries. The architecture of this Enterprise should ideally extend from the national to the tactical level, have robust linkages to other agencies and have linkages with industry and academia. This Enterprise needs to be multi-domain, converged and have capability in the entire spectrum of SIGINT activities. The scope of SIGINT has over time expanded beyond the traditional COMINT and ELINT and now includes Imagery, Open Source and Cyber Intelligence. The enterprise has to be technology driven with sensors, automation, cloud and big data implementation, cryptanalysis systems and analytics software. The personnel involved in the enterprise need to have a suitable skill set including leaders with suitable cognitive skills and ability to work in an overwhelming data environment.

Intelligence acquisition in cyber space is a new avenue for the intelligence community. It involves new data sources and new methods of data collection. It includes lawful intercepts, open source information both from the surface web and the dark web, from social media and most significantly through computer network exploitation (CNE) operations. The CNE operations are highly sophisticated operations which is a totally new domain for signal intelligence. It consists of reconnaissance, research, identification and selection of targets, followed by weaponisation, delivery, exploitation of vulnerabilities, installation of weapons, taking over control and lastly, carry out the desired actions at the target system. This may include exhilaration, destruction of data or intrusion of

another target. The main implication of intelligence acquisition in cyber space is the massive data available today. Data is no longer limited to documents as it includes audio, videos, logs, structured and unstructured data, etc. Numbers of agencies are carrying out similar tasks in India; however, currently, they suffer from a shortfall in data handling capabilities, translation services, cryptanalysis and automation capability including analytics. The automated analytics toolbox which can carry out audio, video, imagery, text and link analytics, etc., is gradually becoming central to intelligence organisations.

Militaries around the world have realised that cyber warfare cannot be treated in isolation. The PLA has placed SIGINT, CND and CNE with the third department of the GSD. Language translation, high-performance computing and cryptanalysis are already available within the third department. The US Cyber command and Unit 8200 of Israel have similar synergised organisations. A striking example of a synergised and converged operation involving SIGINT, CNO, EW and HUMINT is Operation Orchard allegedly attributed to Israel. In April 2004, a massive explosion took place on a North Korean freight train. In this explosion, 18-20 Syrian scientists died and their bodies were received in Damascus in coffins lined with lead. This set the Mossad operations into motion, to get to the bottom of the story. SIGINT operations also indicated multiple communications between North Korea and Syria, which were traced to a place called 'Al-Kibar', located in a remote desert region in western Syria. Cyber operators of Mossad also broke into the personal computer of a top Syrian atomic energy official while he was visiting London and uncovered a treasure trove of information including photographs of nuclear installations. An Israeli special force HUMINT operation was able to collect water and soil samples from the area of Al-Kibar which confirmed traces of radioactivity. In September 2008, the elite 69 squadron of the Israel Air Force destroyed the target after employing EW and possibly a sophisticated computer hack to feed a false air picture to the Syrian Air Defence network, bringing an end to Operation Orchard.

Realistic Training for Cyber Warfare

Frontiers of the modern war have shifted to disinformation warfare. In this kind of warfare, there is a need to have a mix of physical security with cyber security. Tackling these aspects in isolation will be disastrous. The integration of cyber specialists and legal experts is also a natural progression since the cyber weapons are now emerging out of the secret domain to the open domain. Cyber warfare and its tools/techniques are being discussed openly and many of the tools are easily accessible over the internet and social media. A country like India, which is an IT super power is more vulnerable as it becomes a lucrative target. Hence, the educational and training programmes for countries like India cannot be run off the mill, but highly specialised and focused. Buying technology is not a long-term solution in this field, especially for democratic and process based countries like India which have a relatively long procurement cycle. The selection of the right category of people with the right background is the first and primary task. It can be tackled in a three pronged manner. First, running special programmes in schools and higher institutes of learning where talent scouts can identify candidates with special skills. Second, the Armed Forces can focus on their captive manpower who can be selected and shifted to cyber intelligence roles. Third, the candidates working in the industry and other government agencies can be incentivised to shift either full time or part time to cyber militia role. Above all, training for cyber warfare has to be an incentive driven national mission and cannot be left to a few agencies or organisations. Cyber warfare should be a compulsory part of the curriculum in schools and colleges, just like languages or mathematics. Cyber is a global language which every child should learn. While some may excel in the same, others will contribute by being aware and knowledgeable. At the more advanced level, there is a requirement of technicians, investigators, agents, spies and leaders in the cyber domain. Once the requisite manpower base is available, the responsibility of such training can be assigned to specialist units both military and non-military. The process could be termed as Educational Intelligence (EDINT), where education can be turned into a source of Intelligence in the cyber domain.

Cyber Warfare in the Operational and Tactical Domains

The Indian defence forces are still progressing towards the goal of Net Centricity. In fact in certain areas, it is a distant objective. Consequently, cyber warfare in the tactical and operational battle space is not yet a matter of critical concern of commanders. Seldom does this aspect get discussed in formation war games and exercises. However, certain classes of equipment used by the Indian fighting forces like surveillance equipment, the sensor to shooter links, integrated command and control systems, etc., are certainly vulnerable. However, due to a very low degree of networking, cyber vulnerability is of a low order. Widely networked systems like communications, logistic networks and information systems which have a wide reach from the strategic level to the forward edge of the battle field are more vulnerable. Applications that are currently riding the Army data networks have an additional vulnerability due to lack of certification for hardware and software vulnerabilities. The simultaneous access of military personnel to the defence networks on one hand and the ubiquitous internet and social media on mobile devices on the other hand, is a criticality. Cyber hygiene has its importance, however technical measures to prevent any kind of network overlap or breach is the need of the hour. Automated solutions which can prevent a breach in military networks is more important in the Air Force and the Navy since the dependence of the platforms on various kinds of networks is paramount and any disruption may cause a virtual blinding effect.

While the vulnerability of tactical and operational systems can vary, what cannot be denied is that there is a far greater requirement in awareness about the possibilities amongst our commanders, system operators and network users. The technology exists for breaching air gapped networks; however, this methodology has practically proved effective for military networks and is likely to be adopted even in future. Setting-up of cyber/social media surveillance cells can be tried out at formation level in Counter Terror operations, to increase awareness as also focus on local content.

Cyber Warfare as Part of Security Strategy and Doctrine

Cyber warfare was conceived perhaps as an alternative to a conventional war but in today's scenario, even a serious cyber crime or a cyber attack can escalate into a war. Cyber warfare offsets conventional capability. In cyber warfare, even smaller nations or groups including non-state actors can acquire disproportionate capability using minimal resources. In the context of such groups, once the capability is in place, the intent to use such weapons may not be guided by reason or rationality. Non-attribution makes the problem more complicated. In this complex environment, the formulation of comprehensive security strategies and doctrines by responsible nation states, to address the threats of cyber threat is a challenging proposition. However, certain recommendations are enumerated as follows:

- A Cyber Commission needs to be formed under the Prime Minister Office (PMO) with legislative sanction. The agencies including the Armed Forces should derive their authority both defensive and offensive from the Cyber Commission. It should ideally have representation from the military and non-military domains.
- The cyber forces consisting of the military and non-military component should be used as aids to civil authority, especially in peace time. Therefore, the cyber capabilities of all agencies including the Armed Forces should be used to counter attacks and threats. During a war, while the agencies may remain the same, the leadership role could be assigned to the Armed Forces.
- The supply chain aspects including research, development and testing will need to be addressed at the national level.
- Accountability, certification and terms and conditions should be built into commercial agreements between the national government and private companies, both Indian and foreign. Fines, penalties and black listing should be used whenever security is at stake.

- Responsibility and ownership of networks which constitute cyber space must be clearly defined, and agencies/sector have to be made fully accountable and legally tenable. Service providers should also be made to compensate for any breach in their security arrangements, which also include any theft or loss of information.
- Specifically for the Armed Forces, the Defence Cyber Agency sends a weak signal and a proper cyber command needs to be put in its place. This is as much a matter of signaling as a matter of capability.
- As defense forces, the merging of physical and information domain including cyber should be clearly a part of the doctrine and capabilities built accordingly.
- The existing scope of Information War (IW) could be extended to social media, as part of the IW doctrine.
- Generation of an army of skilled manpower in cyber techniques needs to be addressed as part of the strategy and doctrine. Issues like the utilisation of NCC Cadets, Cyber Territorial Army and other in-house manpower needs to be addressed.
- The training of a cyber leader is infinitely more challenging than training a cyber warrior. This aspect needs to be addressed.
- Military Grade Standards should be extended to cyber hardware and software.
- Cyber deception is a major component of warfare of the future which needs to be considered as part of the doctrine.

Conclusion

The contours of cyber warfare are unique in the sense that the Blue team starts with a handicap. The advantages are heavily weighed in favour of the Black, Grey and the Red teams. Hence, the effort required to be put in by legitimate governments and agencies entrusted with the security of the population should be focused, synergised and coordinated. The establishment of the office of

the National Cyber Security Coordinator under the PMO was a seminal decision in our quest. Other organisations like the CERT-In, Regional CERTs, the NTRO amongst others are doing remarkable work in securing national interests. What emerges however, is the sheer dimension of the problem and the lack of resources including the trained 'Cyber Army' foot soldier. It is in this context that the Armed Forces of the nation could be given a definite mandate, like in many advanced nations of the world. What the Armed Forces bring in is discipline, expertise, screened manpower, training infrastructure and undisputed nationalism, all critical components of this fight. Particularly intriguing is the quest between the so called Old World and the New World intelligence acquisition techniques for battle. Information is easily available in the cyber domain, what is important is to realise the usable intelligence component. Actual battle situations will invariably offer much more in the traditional realms of HUMINT, COMINT, ELINT, etc.,which tends to dry up in peace time. Hence, there is a need to strike a fine balance between the Old and the New. The future battle field scenario remains ambiguous and speculative. Hence, training also needs to be futuristic and adaptive, which is a critical challenge for designers of the curriculum. Effects of cyber warfare in the operational and tactical domains are not in the active list of concerns today; however, there is a need to address this aspect adequately. Like electronic interference, soldiers must be ready to work through cyber interference. Few nations are working on cyber injection attacks at the tactical scenario using mobile and aerial platforms; hence the threat is real and near. Once the Joint Doctrine has accepted that the cyber domain is a valid domain of warfare for the Indian Armed Forces, all stakeholders must tackle the doctrinal aspects adequately for the cyber domain, followed by requisite capability development.

CONCEPT NOTE

Introduction

The Joint Doctrine of the Indian Armed Forces was released by the three service chiefs on 25 April 2017. The Joint Doctrine 2017 is a revised version of the first document released in 2006 and addresses the current realities. As a significant change to the existing procedures, the Document was released as an unclassified document for unrestricted circulation. The Doctrine recognises the five domains of modern warfare, ie land, sea, air, space and cyber space. It lays due emphasis on the development of the triad of the Defence Cyber Agency, Defence Space Agency and the Special Operations Division. The nucleus of the Defence Cyber Agency, which will have both offensive and defensive cyber warfare capability is already in place and is functioning under the HQ Integrated Defence Staff (HQ IDS). This is a positive step towards the creation of the Cyber Command and the evolution of potent cyber warfare capability.

Since 2014, the term Cold War 2.0 has been a matter of intense discussion in international forums. Respected commentators and leaders have written that the world is well and truly at war, albeit undeclared and being conducted indirectly or through proxies. Apart from media and social media, the most exploited arena of the Cold War 2.0 remains the cyber domain. Recent news reports have highlighted the 2016 Democratic National Committee (DNC) email leak as a possible fallout of this undeclared war. The consequence of the leaked emails and attachments which were published by WikiLeaks in July 2016, has been of mega proportions including the alleged effect on the US Presidential elections. The source of the leaks has not been fixed; however, fingers have pointed to Russian hackers. Cyber war however, goes much beyond Cold War 2.0. Small nations like North Korea have demonstrated their capability to take on technologically superior nations like the United States. Stuxnet and Flame attacks against Iran and Estonia have proved the power of cyber warfare to shift focus from conventional to the 'virtual'

domain. Access to the Internet and easily available cyber tools also enable 'Non-State Actors' to launch cyber attacks. Cyber attacks are characterised by deniability and non-attributability; hence, traditional and physical boundaries are not relevant in this kind of warfare. It is characterised by extreme speed, lack of warning or indicators, ambiguity regarding the specified areas of battle, and lack of posturing. Traditional deterrence strategies are ineffective in this form of warfare. USA, Russia, Israel and China have been known to have demonstrated advanced capability in the field of cyber warfare. USA has been concerned with the attacks on their 'Intellectual Property' and has created a new synergy between the security agencies and the industry. China has gained considerable success in this field and is now considered one of the foremost players. Role of Chinese hacking units has been detected in a large number of breaches that have been reported in different parts of the world. India continues to be a prime target of the Chinese cyber warfare effort.

The term 'cyber warfare' has been used loosely along with other activities prevalent in cyber space like cyber terrorism, cyber espionage, cyber crime, etc. While it is commonly accepted that the tools used to achieve ascendancy in cyber space are essentially similar in nature, cyber warfare is a military function aimed at the overall aim of securing the Nation and its interests. However, this military function can be performed jointly by military personnel, cyber militia, scientific community or academia. What is required in an integrated approach, training and access to suitable resources and tools. Cyber warfare, which has both offensive and defensive components, is also a subset of the overall gambit of Information Warfare(IW). In the net enabled world of today, it is arguably the most important component of IW.

Indian Context

At the national level, the defensive component, i.e. cyber security is loosely governed by the National Cyber Security Policy which was promulgated in 2013. The CERT-In under the Ministry of Communication and Information Technology is the national nodal agency for responding to computer security related incidents as

and when they occur. There are however more than 35 different agencies operating under the PMO, Ministry of Human Affairs (MHA), Ministry of External Affairs (MEA), MoD, MCIT and non-governmental organizations (NGOs) which have a role in the overall national response to cyber incidents. There are six different Apex Level agencies for management, coordination and supervision. The ambiguity in the protection of critical infrastructure emphasises the case for synergy. CERT-In, formed in 2004, vide the IT Act 2000 (section 70B) under MCIT, was initially mandated to ensure cyber security of critical infrastructure, which was later limited to only non-critical structures. The National Critical Information Infrastructure Protection Centre (NCIIPC) formed under NTRO vide IT Amendment Act 2008 (section 70A) was later mandated with the protection of critical infrastructure. Now the NDMA which is under MHA has also been assigned the responsibility for the protection of cyber critical infrastructure. Hence, three different agencies under different ministries are operating towards the singular objective of securing critical infrastructure. While the lead agency in formulating national policy is the DEITY/MCIT, this Ministry does not have jurisdiction over influential ministries and departments like the MoD, MHA and NSCS/NTRO. It emerged that the interaction, sharing of information, earmarking of specific roles and assignment of responsibility is nebulous. The appointment of the National Cyber Chief under the PMO is a positive development and expected to give the desired thrust towards integration and synergy. There appears to be a deliberate effort by the agencies concerned to ensure ambiguity regarding the *offensive* component of cyber warfare. The aspect is presently being handled by multiple agencies and there is a need for further integration of purpose, delineation of roles and the assignment of the lead agency role.

Data extracted from the CERT-In website depicts an alarming rise of cyber attacks and incidents on Indian websites and information infrastructure. According to a written reply given by the Minister of Home in the Lok Sabha on 7 February 2017, more than 700 websites of central ministries/departments and state governments were hacked between 2013 and 2016 (199 in 2016, 164 in 2015, 155 in 2014 and

189 in 2013). Both Pakistan and China have been targeting India in the cyber domain. Pakistan agents have used social engineering for espionagerelated tasks. Pakistani hackers have also been active on the internet and incidents of defacements, vandalism and cyber espionage have been identified. China is indulging in cyber activities which have a long gestation period and targeted at the strategic level. The role of Chinese communication and IT multinationals is implicit in the Chinese quest to achieve military and economic advantage. Instances of attacks on the MEA, MoD and the Tibetan government in exile have been attributed to Chinese actors. China is approaching cyber warfare by means of the organised sector as well as the unorganised sector, according to the tenets of the people's war. However, the role of the PLA is central to the Chinese cyber warfare effort.

Cyber Laws, Policies and Challenges

- *International Laws and Response to Cyber Conflicts*. The nature of conflicts in the cyber domain is an emerging phenomenon and is presently unregulated by international laws. The role of the United Nations in such conflicts is also non-existent. A critical challenge in regulation and adjudication in the cyber domain is the inherent difficulty of attribution and assignment of responsibility. It is evident now that the fallout of a serious cyber attack can easily affect the social and economic infrastructure of a nation and consequently have humanitarian ramifications. There is a case in point to include cyber attacks as part of the Laws of Armed Conflict and International Humanitarian Law. The Tallinn manual 1.0 published in 2013 was the first attempt to codify the rules and laws pertaining to cyber space and overt cyber warfare. The Tallinn manual 2.0, published in February 2017 by a team of legal experts has extended the scope to the applicability of international laws to cyber operations, which is presently a constant phenomena in peace and faced by peacetime legal regimes. This is expected to be the seminal document around which international laws and international response are likely to further develop and mature. As of now, the Tallinn manual 2.0 has not been released as a free to download document. However,

it is available as a book published by the Cambridge University Press.

- *National Laws and Policies*. The National Cyber Policies and Laws are limited to the IT Act 2000 (duly amended from time-to-time) and the Cyber Security Policy 2013. They are associated with numerous shortcomings. There is a pertinent need for revision so that the legal structures are robust enough to counter challenges from state/non-state actors and new domains like the Cloud and social media.
- *Challenges to a Unified National Response Mechanism*. The ubiquitous nature of cyber space has resulted in multiple stakeholders with no clear cut distinction of roles. Multiple players pursuing a loosely similar agenda in a common domain is likely to result in sub-optimal response and lack of accountability. There is a distinct need to address the synergy between organisations, delineation of roles and consolidate recommendations for consideration by the Government and the Services.

Cyber Warfare – Latest Tools and Techniques

- Cyber warfare is primarily technology driven; hence, the tools and methods employed in this form of warfare are constantly evolving. Defacement of website attacks, denial of service attacks, etc., are techniques of the past and have given way to intelligent malware attacks as evident from the cyber incidents which have occurred post the Stuxnet attack(s). This period has also seen the development and use of autonomous cyber weapons. The inter-connections between cyber attacks like ransom ware, cyber crime, the dark web, illegal sale and purchase of exploits/data have become evident. A self-sustaining underground ecosystem including digital currency exists, which needs to be surreptitiously exploited, even by legal regimes to achieve ascendancy over the adversary. Technology is bridging the gap between the legitimate and the illegitimate since the tools and methodologies used in a cyber crime or cyber warfare to secure legitimate national interests is primarily the same. Cyber warfare is not bound by the rules of ethical warfare which soldiers of law abiding and

responsible nation states are more used to. Consequently, there is a need to focus on the complex nature of cyber threats in future both at the national level and in the Armed Forces and suggest methods to counter the same.

- *Convergence of Cyber and Space Domains*. Both the cyber and space domains are global commons which are largely unregulated and being exploited extensively. Technology has created a close integration and dependency between these domains. Consequently, an adverse effect on one is likely to affect the other. Since the Armed Forces are extensively dependant on both cyber and space domains for fighting an integrated battle, there is a need to evolve a congruent synergistic approach to counter attacks on systems operating in these domains. The emerging convergence between cyber and space needs further analysis, with focus on the threats and implications.

Cyber Warfare and the Indian Armed Forces

The development of cyber warfare capabilities in different countries has taken place around the core of the Armed Forces. The role of Chinese PLA Unit 61398 and the NSA in the launching of sophisticated cyber espionage activities is well-known and in the open domain. Networks being used by the Armed Forces are vulnerable and are likely to be primary targets in times of conflict. There is a pertinent need to analyse the cyber capabilities/vulnerabilities of the Indian Armed Forces and its neighbours. There is also a need to analyse means employed by adversaries in the employment of social engineering in cyber space with special reference to social media.

The future digitised battlefield will operate in a hostile cyber environment. Disruptions and loss of data and information will be common and the cyber war effects will be felt at the operational and tactical level. The Indian Armed Forces would be required to take the battle into the enemy camp, else purely defensive measures would be breached at some point or the other. There is also a need to address the nebulous aspect of offensive cyber weapons to be used at the strategic, operational and even the tactical levels. The development

of niche expertise within the Armed Forces and participation of other agencies (including the PPP model), also needs deliberation.

Cyber War beyond Military Targets

Media reports of 13 May 2017 indicated an extensive ransom ware cyber attack on computers of more than 100 nations including the National Health Scheme of the United Kingdom. Interestingly, the hacking tool leaked by a group called 'Shadow Brokers', was using a vulnerability in the Microsoft Windows Operating System which was discovered and developed by the US National Security Agency (NSA) but was stolen by hackers. Indeed wars will be fought differently in future with a merger of and military and civilian targets. Hacking and virtual sleuthing would be integrated into all future operations, as indispensable as the weapons and ammunition soldiers carry into battle. To cripple a country during cyber war, critical infrastructure will be targeted. This will include power, banking, water systems, health, agriculture and transportation. To do so, relentless peace time cyber activities looking for vulnerabilities in target networks needs to be carried out so that the systems can be hijacked and injected with cyber tools for use in future operations. To ensure the survivability of own critical assets, a vulnerability assessment would be in order at the national level so that necessary corrective action can be undertaken in time. In consonance with the tenets of conventional warfare, the militaries now need to draw up a list of overseas targets of national importance, where it would make more sense to attack with a cyber weapon than a conventional one.

The Indian Armed Forces are the last bastions of the security, safety and integrity of the nation. War fighting doctrines published at various levels recognise the fact that the Armed Forces will have to fight in the cyber domain as they do over land, sea, air and space. Hence, the Armed Forces should be an integral component in the development of the cyber warfare capability of the nation. Perhaps the time is opportune now for the assignment of a lead agency role to the Armed Forces or any other designated agency to ensure a cohesive development in capability, procedures and expertise at all levels. This will also ensure accountability, which is lacking today.

PROGRAMME

0830-0900h	Tea and Registration
0900-0935h	Inaugural Session
0900-0905h	Welcome Remarks by Lieutenant General BS Nagal, PVSM, AVSM, SM (Retd), Director, CLAWS
0905-0920h	Keynote Address by Lieutenant General DR Soni, VSM, GOC-in-C, HQ ARTRAC
0920-0935h	Special Address by Dr Gulshan Rai, National Cyber Security Coordinator
0940-1100h	**SESSION I: Emerging Challenges in the Cyber Domain**
0940-0950h	Opening Remarks by Chair: Alok Joshi, Chairman NTRO and ex-Chief R&AW
0950-1010h	Challenges of the Current Global Cyber Environment–War in the Sixth Dimension by Captain Raghu Raman (Retd), RIL
1010-1025h	Evolution of Cyber Laws, Policies and Regulatory Mechanisms at International and National Levels by Arun Sukumar, Head Cyber Security and Internet Governance Initiative, ORF
1025-1040h	Need for Synergy between Organisations, Delineation of Tasks and Earmarking of Lead Agency Role–National Perspective by Brigadier Manjeet Singh, DACIDS(DIARA), HQ IDS
1040-1110h	Interactive Session including Closing Remarks by Chair
1110-1130h	Tea Break
1130-1330h	**SESSION II: Cyber Warfare–Tools/Techniques and Future Trends**
1130-1140h	Opening Remarks by Chair: Lieutenant General Davinder Kumar, PVSM,VSM** (Retd) former Signal Officer in Chief
1140-1200h	Cyber Weapons and Advanced Threats to National Security by Amit Sharma, Additional Director, DRDO
1200-1220h	Securing of National Critical Information Infrastructure by Major General Ajeet Bajpai (Retd), DG NCIIPC
1220-1240h	Cyber – Space Convergence: Means to ensure Secure Space Based Assets and Services against Cyber Threats by Colonel Deepak Puri, DG Sigs

1240-1300h	PPP Model for Cyber Warfare in India–Is it a Workable Model and what would be needed to make it Operational? by Colonel KPM Das (Retd), CISCO
1300-1330h	Interactive Session and Closing Remarks by the Chair
1330-1415h	Lunch
1415-1610h	**SESSION III: Cyber Warfare and the Indian Armed Forces**
1415-1425h	Opening Remarks by Chair: Major General SK Pillai, VSM (Retd), Tata Power SED
1425-1445h	Cyber space and Intelligence Acquisition in the Military Domain–Is it Time to Rethink Organisations and Structures in the Indian Armed Forces by Major General SK Pillai, VSM (Retd), Tata Power SED
1445-1505h	Cyber Warfare Training for the Indian Armed Forces–A Fresh Look by Marc Kahlberg, CEO, Vital Intelligence Group, Israel
1505-1525h	Manifestation of Cyber Warfare Effects in the Operational and Tactical Domains–Working Through the Hostile Environment by Major General MU Nair, ADGSI & ACIDS (Int)
1525-1545h	Recommendations for the Indian Army Doctrine–Warfare in Cyber Domain by Colonel Dinesh Kumar, Military College of Telecommunication Engineering, Mhow
1545-1615h	Interactive Session Including Summing Up by the Chair
1615-1630h	Closing Session
1630-1630h	Closing Address and Vote of Thanks by Lieutenant General BS Nagal, PVSM, AVSM, SM (Retd), Director, CLAWS
1630h	Tea and Dispersal