COVER STORY

# CYBERSPACE

## The 5th Dimension of Warfare

SEMINAR REPORT

### CYBERTECH INDIA 2018

Cyberspace, a domain created not by nature but by human beings, has emerged to provide tremendous benefits, but also to present new risks. Technologically driven methods are used to gain unauthorised access to computer resources for most cyber operations, regardless of the intended purpose: crime, terrorism, industrial espionage, military espionage, or warfare. Indeed, novel cyber attacks on critical national infrastructure are likely to severely disrupt social activities if successful. Cyber security has thus become a national security issue.

To address the important issue a seminar on the subject was conducted by South Asia Defence and Strategic Review in concert with CENJOWS on 27 and 28 Jun at the DRDO Bhavan, New Delhi. The first such event, conducted by us in 2012, did not draw the kind of attention that was warranted; evident from the fact that only two service officers attended and that too in civies.

However, this year's seminar was a far departure from the first one as the COAS graced the occasion and there were representatives from all the three Services, DRDO, Industry and CAPFs. There was a galaxy of subject matter experts who enlightened the audience, which was enthusiastically participatory and in consequence some very interesting discussions were generated.

The aim of the seminar was to assess our preparedness for cyber war and to chart out a practicable way forward.

## Opening Session

The proceedings were initiated by Lt Gen Vinod Bhatia PVSM, AVSM, VSM (Retd), Director CENJOWS, who spoke about the rapid changes in technology, shifting nuances in the nature of warfare and the need to dominate cyberspace. In his welcome address Air Marshal PN Pradhan, AVSM, DCIDS (Ops) emphasized that the importance of cyber security is poorly understood and gave examples of Wiki Leaks and Cambridge Analytica and went onto state that cyber security is the biggest challenge of the 21st Century. Lt Gen Satish Dua, PVSM, UYSM, SM, VSM, CISC, spoke about emerging threats in the cyber threat landscape, in view of increase in E Commerce and E Governance and therefore the need to tweak our strategies accordingly. General Bipin Rawat, UYSM, AVSM, YSM, SM, VSM, COAS lauded the initiative of the Northern Command of the Indian army to shift to BOSS OS and for developing an indigenous network security overlay which he pointed out were pioneering steps for setting up an indigenous ecosystem for cyber security. The COAS desired that we develop niche capabilities to defeat the enemy and that we should be proactive in our use of cyberspace against the enemy rather than be defensive. Lt Gen DS Hooda, PVSM, UYSM, AVSM, VSM **, Former GOC-in-C, emphasized the need to develop a doctrine and have a cyber command with a coordinator well versed in cyber warfare in the PMO controlling matters related to cyber space. He further brought out that the constitutional provisions on the defence of India mandate that the MoD is responsible. He also cautioned the military leadership about this responsibility and said that they should not be found wanting.

After the Opening Session there were sessions and panel discussions which covered various important facets of the issue. The topics were as under: -

- **Session I:** Cyber Warfare & Cyber Threat Landscape
- **Session II:** Building a Cyber Secure Nation
- **Session II:** Cyber Laws and Policies, International Cooperation and Best Practices
- **Session IV:** Critical Information Infrastructure Protection
- **Session V:** Internet of Things: The Changing Cyber Security Landscape
- **Panel Discussion:** Cyber Analytic Capabilities, Strengthening the Organisation through Skills, Policies and Systems

## Sessions

### Session I

Cyber Warfare & Cyber Threat Landscape

### Session II

Building a Cyber Secure Nation

### Session II

Cyber Laws and Policies, International Cooperation and Best Practices

### Session IV

Critical Information Infrastructure Protection

### Session V

Internet of Things: The Changing Cyber Security Landscape

### Panel Discussion

Cyber Analytic Capabilities; Strengthening the Organisation through Skills, Policies and Systems

## Takeaways

**Evaluation of Preparedness.** We need to evaluate the levels of our preparedness for countering threats posed by Cyber Space. Securing online borders is as important as safeguarding the air, land and sea boundaries. It is only after we identify our strengths and weaknesses that we will be able to move forward in the right direction.

**Policy.** There is a need to chart out a comprehensive cyber security policies. It is imperative to have policies and they must be worked out by taking advise and inputs from technologists and domain experts. Having policies will help only if we ensure that they are implemented in right earnest. Policies must explicitly delineate measures for protection of CII. We must demonstrate leadership and commitment towards CIIP.

**Strategy and Wherewithal.** We must have appropriate offensive as well as defensive strategies to wage a cyber war as well as defend ourselves against cyber attacks. We must have the ability to bring to bear effective cyber deterrence on our adversaries. And last but not the least we need to develop capabilities and infrastructure which provide adequate cyber resilience to the country. We must also come together to formulate strategies to effectively counter online and offline violent extremist narratives to protect national security.

**Structures.** It is absolutely of the essence that we have appropriate structures in place to ensure cyber security of the nation. It is well neigh impossible to take on the challenges posed by cyber threats without having the appropriate structure in place and ensuring that all constituents of the said structure work in concert with each other as also have the required levels of cooperation and synergy.

**Skills.** We need to develop appropriate skills in the work force involved in the cyber space. Awareness and strategic educational initiatives must be strongly encouraged. In addition, multidisciplinary research and development needs to be accelerated involving the academia and industry.

**Develop IT Competence.** Cyber space provides a vast canvas for waging war and advances in technology such as AI, IOT and Cloud Computing etc. have made it a lethal battlefield with immense possibilities. Therefore, we need to develop the requisite IT competence, which helps integrate security aspects with technology and thus enables us to gain a competitive edge.

**Need for Indigenous Technology.** The importance of creating indigenous technical infrastructure in the country cannot but be over emphasised. Having home developed products will certainly help reduce the reliance on foreign hardware and software which is one of the major sources of cyber security breaches as it gives a freeway and backdoor entry to various types of spyware. Policies like 'Make in India' should be highly encouraged and implemented on a wider scale.

**Legislative Measures.** We must have appropriate legislative measures in place to make the cyber security framework effective and strong. Legal framework must be enforced to develop a better cyber security culture that adopts a multi-disciplinary and multi-stakeholder approach.

**Need for International Laws on Cyber Security.** There is a need for cogent International Laws in the sphere of cyber security. These should be universally acceptable and ratified by all concerned. Cyber norms and international laws should be harmonized globally. Threats can be categorized into three categories: National threats, Economic threats and attacks impacting individuals. We need to have adequate cross border cyber laws for all threats and vulnerabilities arising due to cross border flow of data.

*General Bipin Rawat, UYSM, AVSM, YSM, SM, VSM, COAS*

*Lt Gen Vinod Bhatia PVSM, AVSM, VSM (Retd), Director CENJOWS*

*Lt Gen DS Hooda, PVSM, UYSM, AVSM, VSM **, Former GOC-in-C*

*Air Marshal PN Pradhan, AVSM, DCIDS (Ops)*

**Data Privacy.** Everyone using the internet must be aware of their rights and responsibilities while sharing any data on social media platforms. Data privacy is a serious concern that must be dealt with due care. Caution exercised in this regard will pay rich dividends. In addition, Data Privacy and Data Localisation plays crucial role while processing data. Countries like Russia, China, Singapore and Vietnam have their own data localisation laws. There is need for such cohesive laws in India as well.

**Attitudinal Shift to Change.** Wider adoption of the internet and newer technology has also led to an increase in cyber attacks, instilling a fear in our minds and thus creating a defensive mindset because of which we impose unwarranted restrictions and caution on ourselves. We are therefore unable to exploit the systems to their full potential. We should instead adopt a proactive approach and integrate the required cyber defense mechanisms which can facilitate full exploitation of systems by providing the necessary security.

**Encourage Startup Culture.** We must encourage the creation of a startup culture in India that encourages young minds to come up with innovative solutions in the domain of cyber security. Hindustan Aeronautics Limited (HAL) and Bharat Electronics Limited (BEL) are scouting for defense startups to build a culture of innovation and harness the solutions provided by them. As technologies like AI, robotics, drones, and advanced cyber security tools gather prominence, startups in the defense sector, and early-stage technology companies as well as SMEs are well-positioned to contribute to the defense industrial base.

**Making the Digital Footprint Smaller.** It important to hide our identities in cyber warfare as long as possible, for which we need to reduce our digital footprint. This will also reduce the chances of our adversary knowing our progress. R&D with the involvement of both Academia and Industry should exploit the areas of AI, quantum computing, private tactical player computing, etc. with the aim to reduce the digital footprint not only in the physical domain but in digital domain as well.

**Risk Based Security Management.** Risk-based cyber security management, where organizations continuously need to check if they are at risk and that if they are prepared for any eventuality which may compromise security, must be implemented. Once a breach is detected, the organization needs to get prepared for future events and also after the first attack the likelihood of another attack is quite high, which is why continual risk management is required.

**Identity & Access Management.** This is the need of the hour because the lack of multi-factor authentication and reliance on device-based authentication leads to difficulty in identifying the attackers.

**Intelligence.** Adversary Intelligence, Machine Intelligence, Victim Intelligence and Campaign Intelligence should be collectively used to create a cogent picture to fully understand the attacker(s).

**TTP.** People need to understand various tactics, techniques and procedures (TTP) to safeguard their assets from various threat agents in the cyber space. This is vital to the cause as threat agents have continued to use old and proven exploits to carry out attacks. Conventional methods for security in cyber space may consume significant amount of time. Therefore, focus should be upon early detection of such attacks along with quick response in real time. Every organization should do threat modelling from an active-attacker perspective.

**Public and Private Partnership.** Multi-disciplinary research needs to be encouraged in partnership between public and private sector. We need to have collaborations between trusted public and private players to develop incident response capabilities to gain better security controls and thus enhance CIIP.

**Modify IoT Architecture.** The IoT architecture needs to be modified. A three-tier architecture would serve as appropriate IoT solution. Instead of IoT devices to be directly connected to the cloud, we can have another layer in between the devices and the cloud to simplify, scale, and to add security.

**Automation of Policy Compliance Check/Audit:** Policy compliance checks and auditing takes a lot of time and human effort. Automation can help ensure better accuracy and efficiency in a far lesser amount of time. It is more effective in picking out non-compliances to the security policy in large networks (e.g. Defence Networks). It uses log records as evidence to verify policy compliance. There are various challenges for this system like the large volume of logs and varied formats from heterogeneous devices and applications.

**Use of End Point Security and Tools.** We must introduce end point network security solutions. Various apps and software are available for the purpose. In addition, there are several tools available for cyber monitoring and defence. Use of these tools must be done to minimize security breaches.

*Lt Gen Satish Dua, PVSM, UYSM, SM, VSM, CISC*

*Shrikant Shitole Country MD, FireEye*

*Anand Patil India Lead, Networking and Security, VMware*

*Ashwani Sharma, the Editor with the Army Chief*