Event Report

CENJOWS & IMR Webinar "CYBER DEFENCE INDIA"

(Organised by Centre of Joint Warfare Studies& Indian Military Review on 10th June 2022)

1. The **Centre for Joint Warfare Studies (CENJOWS)** and **Indian Military Review (IMR)** organised/conducted a Webex webinar-cum-virtual expo on "**Cyber Defence India**" on 10 June 2022. The objective of this webinar was to reflect upon the prospects of attaining the cyber military superiority to provide freedom of action in, though, and from cyberspace to support mission objectives and deny freedom of action to adversaries.

2. The seminar featured distinguished speakers including eminent veterans, serving senior officers, members of strategic think tanks and representatives from the industry. During the course of the proceedings, the participants deliberated on the current and future developments in cyberspace – its threats, challenges and relevance in our society. Further, the Cyber technologies, their capabilities and scope in the dimensions of the Critical National Infrastructure and National Security Infrastructure were also comprehensively discussed.

SESSION-I
(INAUGURAL SESSION)

3. In his welcome remarks **Lt Gen Sunil Srivastava, AVSM, VSM** (Retd.)**, Director CENJOWS thanked the speakers, panellists, participants and other serving and retired senior officers for being in attendance.

4. By equating cyber power to the Sea power of the 19th century and the Air Power of the 20th Century, he highlighted the increasing importance of cyberspace in every segment of our society. Witnessing the unparalleled and unprecedented growth of digital systems in the post-Covid era he stressed a dynamic National Cyber Security Strategy with clarity on goals to be achieved in the need for specific time frames. He further advocated that it should address cyber security governance and standards, capacity building, risk management through technology delivery (in good time), Legal frameworks and cyber deterrence by denial and punishment.

5. Further, he deliberated on enhanced tri-service collaboration, functional and doctrinal convergence, and cross-domain synergy between cyber electromagnetic spectrum and space.

6. He hoped that the webinar would through up pragmatic policy pathways.

7. **Lt Gen (Dr) Rajesh Pant, PVSM, AVSM, VSM, (Retd)**, National Cyber security Coordinator-PMO, Govt. of India, delivered the inaugural address and emphasised that the activities we are witnessing globally today is unparalleled as dark web groups actors are getting more and more active and taking-up sides. Cyber warfare today is an integral part of today's warfare. He also brought out that today, cyber domain is as important as land, sea, air and space and cyber warfare is no longer part of hybrid warfare rather it very well forms a part of conventional warfare especially by acquiring kinetic and quasi-kinetic dimensions. He opined that the defence of national sovereign cyberspace is as important as other four domains. NCIIPC risk assessment and securing National Critical Infrastructures, Indian Cybercrime Coordination Centre, linking cybercrime centres pan India. Cyber Coordination Centre for monitoring and threat prediction by CERT-In.are important steps. Actions at international level like Counter Ransom ware Initiative (CRI) are equally important. India is leading the vertical on Network security and resilience.He added that India is a late entrant in the military use of space but the creation of Defence Space Agency (DSA) with dedicated space satellites has been a positive development. He stressed on the need for formulating a national strategy for space and the requirement of synergy between all stakeholders. He underlined the need to enhance cooperation with friendly nations through space dialogues, and MoUs on Space Situational Awareness (SSA).

8. **Lt Gen Manjit Kumar**, DG Information System delivered Keynote address and emphasised that Rapid transforming world witnessing multi domain warfare where cyberspace being a borderless ecosystem has expanded exponentially in the last few years, especially in post-pandemic period.

9. Attack surfaces have increased and the intrusions are becoming more and more sophisticated due to the emergence of new inflexion points. Therefore, we need to secure all elements in our ecosystem as the chain is as effective as its weakest link. Important part of preparation is threat analysis, based on the known capabilities of our adversaries by looking into their Tactics – Techniques – Procedures. He reflected upon how the

agencies today are working in tandem to secure cyberspace and achieve clarity and situational awareness of prevalent threat matrix thereby minimising the time between identification of a potential threat and initiation of the remedial measures.At the end he suggested how the government and industries need to continue investment in the R&D.

10. **Dr Sundeep Oberoi**, Global Head Cyber Security Services, TCS presented his views on the Importance of data in today's world and the need for sharing and protecting data. Further he reflected on the trends having strategic bearing on cyber security and our ability to deal with them:-

(a) Softwareization of everything: Use of software solutions rather than traditional hardware to solve the problems.

(b) Large and ever expanding attack surface: World emerging as a large cyber ecosystem.

(c) Technology outpacing regulations.

(d) Emergence of monocultures: Large corporations dominating in their own field.

(e) Rising Importance of data.

(f) Global contention for talent.

(g) Strategic dependence: Over Hardware and software clubbed with increasing servitization of products.

11. Mr Sundeep Oberoi laid out following policy considerations:-

(a) Talent retention and long term program sustenance

(b) Addressing long term (30 years) horizons via policy:

(c) Alliances with policy centres

(d) Fostering open source components

(e) Creating high quality skills

(f) Retention of skills

12. **Mr Sumit Chouhan**, Principle Sales Engineer, Blackberry presented his views on **Protecting Critical Information Infrastructure**. He reflected on how today we are witnessing the growth in the threat landscape. While stressing the need for predictive capability he laid out a systematic procedure of Prepare – Prevent – Detect - Respond with the help of Blackberry's Cylance AI. Further he highlighted the features of their Blackberry SecuSUITE catering secure voice and data communication for governments.

Mobile device management for governments capable of managing diverse endpoint services without being connected to the internet.

13. **Col K.V. Kuber (Retd)**, Director Defence and Aerospace, presented on the industry perspective on behalf of Ernst & Young. He stressed on how predictions are the key to absolute solutions. As even if we mitigate the attacks, the damage is done. Also he reflected on how cyber security is linked to the socio-economics of National security.

SESSION-II
(THREATS, CHALLENGES AND GLOBAL AND NATIONAL RESPONSE)

14. The session was chaired by **Brig Ramesh Balan**, VSM, HQ IDS. He reflected on dimensions of the World economic forum's Global Risk Report 2022 highlighting the issues of Social Cohesion Erosion, Cyber security failures and digital inequality. Cyber threats are growing and outpacing society's ability to effectively present and respond to them. These continue to impact public trust in the digital systems and increase the cost for the stakeholders. Further he concluded by reflecting upon the various challenges faced: More complex cyber security challenges, lack of conceptual workforce, fragmented and complex regulatory framework etc.

15. The first speaker of this session was **Col Debashish Bose**, Senior Defence Specialist (Cyber) NSCS; He reflected his views on the **National Cyber Security Policy**. He started by giving the background of the National Cyber Security Policy of 2013 along with the evolving vectors of threat and the need for a new evolved Cyber Security Policy in the post-pandemic era.

16. The vision for the new India Centric Cyber Security policy 2022 would be Safe – Secure – Trusted – Resilient Cyberspace. He further highlighted the features of this new policy as follow:-

(a) Sovereignty (of India) as a root.
(b) Whole of nation approach.
(c) Focus on Economic and Social domains.
(d) Action oriented assessment for next five years.
(e) Common but differentiated responsibilities.

17. In conclusion, he demarcated three pillars of the Cyber Security Policy 2022 i.e., Secure Strengthen – Synergise.

18. **Brig Y Kaura**, Brig Military Ops (Info Warfare); Reflected upon **The Chinese Cyber Threat.**

19. He started by discussing the National Cyber Power Index 2020 with a focus on China in the domains of Cyber Surveillance, Cyber Security, Cyber Offensive, Exploitation for cyber Commercial Gains and enhancing domestic industry. He went on to describe various Chinese Cyber Intrusions and reflected on the Chinese Cyberspace Strategy based on Active defence integrated in Whole of nation approach (military, economic, diplomatic and social domains of society). Further he reflected upon peace time cyber reconnaissance operations and advocated Gaining Information dominance through cyber warfare as the first strike option. Further he reflected upon the Great Chinese Firewall and discussed the Cyber Organisation, PLA SSF, APT's and Technical Reece Bureaus of China. He also covered following National Cyber Security landscape challenges for India:-

(a) Indigenous chip manufacture capability
(b) Capability to manufacture ICT equipment at scale.
(c) Regulations/ monitoring network traffic at National level
(d) Evaluation of embedded malware/supply chain Infection
(e) R&D in cyber security domain
(f) Lack of Military-Industrial complex

20. Further he listed out the Cyber threats from China:-

(a) Threat to Critical Info Infrastructure through Cyber compromise of critical systems
(b) Embedded malwares in hardware & software - Supply Chain poisoning
(c) Espionage and Intelligence gathering through Trojans & Malwares: Gain access to political, military & economic targets
(d) Network intrusion/Hacking into personal devices - Spear Phishing attacks with e-mails on topics of interest of Indian communities
(e) Infect/ steal data when ICT equipment is repaired/overhauled
(f) Insider Threats
(g) Poisoning of Domain Name Server
(h) Influence Operations

21. **Brig Ramesh Balan, VSM**, HQ IDS; shared his views on **Russia-Ukraine Special Military Operations: Cyber Lessons Learnt**. He discussed the backdrop and build-up to the Special Military Operations. He later emphasised how the Russian Threat groups have been pre-positioned to secure persistent access for strategic and battlefield intelligence collection and to facilitate future destructive attacks in Ukraine during the conflict.

22. He also mentioned the key highlights of the conflict such as KA-SAT Satellite Network Disruptions, Uploading government data on cloud, Kinetic and cyber activities, Galvanization of Ukrainian IT Army, etc.

23. Further he shared his views on the contest in the cognitive domain with the help of Propaganda, Disinformation, Social Media Warfare and OSINT. In the end he listed some lessons learnt from the same:-

(a) Civil-Military fusion starkly visible: Nations rather than militaries war

(b) Protective / Enabling / disruptive role played by Big Tech firms

(c) Hacktivist collectives (Anonymous/ Ukrainian IT Army/ Conti) play a plausibly deniable role

(d) Destructive cyber effects are invariably accompanied by espionage and intelligence and sabotage; in fact the latter are a better use of cyber

(e) Impact on critical services and infra can be discerned.

(f) Importance of Protection of data

(g) Pre-positioning and Maintaining Presence crucial to cyber operations

(h) War presented analysts with unprecedented amount of rich, open source data on military movements, troop location, shelling damage, weapon types, and more

(j) Intelligence gained through cyber and other means can be weaponized to prosecute influence operations should it stay locked up?

(k) Repurposing of celebrity handles - Tools of overt geo-politics-e.g. TikTok

(l) Narratives Shaping; Influencer Engagement (TikTok) Entire nation-state de-platformed.

(m) Social Media platforms do take sides and are not strictly Apolitical

24. Key Takeaways:-

(a) Our modern-day habits are trackable, traceable, and predictable

(b) Use of Apps for tracking military activities

(c) Open-source data exposed the Military as troops are digitally connected

(d) Accumulation of open-source data potential to impact the military's ability to fulfil its mandate

25. He concluded his part by summing up following points:

(a) Hastening of move towards Spl internet (autonomous and sovereign internet)

(b) The age of Big Data Analytics and AI has dawned. Deep Fakes and Disinformation are here to stay

(c) Digital Payment Transfer Systems - a critical need for all countries

(d) In the face of our known knowledge gaps & the covert nature of cyber/ info ops - prudent not to draw a final conclusions, just yet

26. **Mr Pramod Khanna**, Country Manager - India & SAARC, BlackBerry.Presented Blackberry's perspective on **Prevention-First Cyber security is Always Better than Cure!.**He emphasised that today the Velocity and sophistication in attacks out paces our traditional reactive approach. Therefore, we need a shift towards predictive and proactive approach leveraged with the help of A.I., ML and Quantum technologies. He further reflected on Blackberry's operations in this respect with a focus on their flagship product CYLANCE A.I. protecting endpoints, business and people. Further he listed out reasons for the endpoint and cyber chaos in contemporary times:

(a) Outpaced speed of innovation
(b) Expanding attack surface
(c) Exponential vulnerabilities
(d) Increase in number of agents involved
(e) Evolution in types of endpoints
(f) Growing geopolitical tensions
(g) Growing number of consoles, offensive investments
(h) Growing numbers of agents and vendors

27. He further reflected upon how Blackberry secures more than 96 per cent of the enterprise landscape in the domain with the concept of One Agent – One Console – One Cloud – One Crowd –Open Architecture and Eco-system.

28. Last speaker of this session was **Mr BalaManoharan**, CTO, SecneurX; he shared his views on **How to stay ahead of the changing threat landscape**.He highlighted the evolving cyber threat landscape with a focus on traditional and new malwares, evolution of ransom ware and Advanced Persistent Threats. Further he reflected on evolving tactics,

techniques and procedures (TTP's) and stressed on the approach of Proactive defence with a model of Inspection – Detection – Protection with a fire drill approach. He then reflected on the key features of SecneurX's product PENATAUR:-

(a) Protection against latest APT Threats
(b) Protection against Evolving Ransom ware Threats
(c) Continuous validations of security systems - evolving threat landscape
(d) Measure Security posture of the critical infrastructure

29. The session was concluded with the closing remarks by **Brig. Ramesh Balan.** He highlighted the Threats at level of technology and challenges faced by the nation states. He brought out a fact that there are no permanent friends or foes and stressed on the need for the "atmanirbharta". We require greater partnerships to develop these capabilities to leverage AI, ML and Quantum.

SESSION-III
(CYBER SECURITY TECHNOLOGIES AND CAPABILITIES)

30. The third session on the theme "**Cyber Security Technologies and Capabilities**" was chaired by Brig A.J.A Pereira. At the outset, he underlined the importance of cyberspace and reflected upon the increase in the attack surface in this domain. He emphasised the perennial importance of the Golden Triangle of People – Process – Technology.

31. The first speaker of this session was **Mr Diwan Khan** from NIC, who shared his, views on "**Protection of Cyber Infrastructure by NIC**". At the outset, he underlined Security measures deployed by NIC at various levels on Pan-India basis.

32. Second Speaker of the day was **Lt. Col. Abhishek Singh**, Army Cyber Group who shared his views on **Countermeasures framework for Military Networks**. He reflected on the peculiarity of the military networks, attack vectors and complex operational requirements and of the military networks. He also reflected on the need to develop decision making and covering the security vulnerabilities in military networks. He made the following recommendations in this respect:-

(a) Securing Cloud based military networks
(b) Incorporating AI and ML in the military networks.
(c) Lightweight military measures for sectional queries (Defence in depth).

(d) Using Block chain for securing Military Infrastructure.

(e) Securing SOA adaptations for Military Systems.

33. Third speaker of the day was**Col KPM Das** (Retd), Cisco Systems shared his insights on **'Atmanirbharta: Cyber Security Opportunities and Challenges'**. He demarcated the foundations of Atmanirbharta in cyber domain as follow:

(a) Leadership

(b) Unified: Strategy, Policy, Governance

(c) National Skill/ Education Capacity

(d) Resilient Supply chains

(e) Global Influence/ Credibility

(e) Domestic standards: Make for Global

(f) Resilient Critical Infrastructure

(g) Public Private Partnerships

34. Further, he covered the threat matrix in the cyber domain followed by the domain of cyber resilience from an Atmanirbhar perspective and highlighted the importance of the role of third party in the cyber ecosystem and resilient and Secure Supply Chains. His recommendations for evolving an Augmenting National Policy - Towards Atmanirbharta were:-

(a) Defining National Resilience Outcomes and Metrics

(b) Defining Interactions, Interfaces and Information flow between citizens, enterprises, institutes and CERTs in order to share information on cyber-attacks and vulnerabilities, with trust.

(c) National Cyber Security Guard: A TA force to be established for defence of cyberspace, being operational arm of NCCC

(d) Securing Critical Infrastructure: Resolve the gaps in ownership of national cyber space and ensure NCSC and NCPC has authority and accountability.

(e) Cyber Security Technology Levers:-

(i) Provide guidelines to procurement agencies on Yardsticks of Trust for Businesses.

(ii) Invest in and set up a "National Shield consisting of a secure and protected DNS

(iii) Supply Chain Security paramount & TPMs (Trusted Platform Modules) form part of network and ICT infrastructure products.

(iv) Develop and provide a Security-By-Design (SBD) set of guidelines to all ministries and departments so that RFIs and RFPs prioritize this aspect in cyber security procurements

(f) Cyber Security Capacity Building:-

(i) Primary School upwards.

(ii) Mobilise High School, College Lab Capacities and invest big.

(iii) R&D costs Money therefore, Public Sector must necessarily invest.

35. He concluded by referring to the key points:-

(a) Policy Ambiguity can be fatal-resolve gaps and ambiguities

(b) A Fragmented instrument of national cyber power is a block towards Atmanirbharta. Diverse points of control: MHA, DOT, MEITY, Consumer Affairs. We need to Consider Cabinet Minister in charge Cyber security (like in Russia, Australia, etc) with single point of accountability.

(c) Acknowledge that critical resources of cyber now with private sector, big tech companies in particular. See private sector as partner and not adversaries.

(d) Bring a balance between localization of standards/practices and international best practices and standards. India could be cyber capital of the world. Y2K moment all over again.

36. Fourth speaker of the day was **Dr. JIJU PV**, CFSL shared his insights on **Lessons from Cyber Attacks on Infrastructure.** He touched upon the foundational aspects of cyber-attacks, cyber and cyber resilience, further he drew lessons from the cyber-attacks on our infrastructure:-

(a) Be on Track with Cyber Security Audits. A thorough analysis of our infrastructure, applications, workflows, and data handling systems will let us rediscover the assets in play but also make us aware of the risks they withstand or fail.

(b) Automating Security at every Stage. Today's organizations emphasize embracing of the distributed workforce and also witnessed an increased dependency on the cloud. Many organizations have learnt the hard way that their underprepared change pushed them more in the face of cyber threats such as phishing, bot attacks, etc.

(c) Updates and Data Backups. Procrastinating important security updates and backups can end up creating vulnerabilities for our organization.

(d) Cyber Security Education. It iscrucial that every organization indulges in proper cyber security & InfoSec awareness programs and training for its employees and customers. Awareness of cyber threats and best practices can help dodge any attack in the form of a phishing email, credential theft, or social engineering.

(e) Move with Time. Hackers and their tactics are evolving with each new attack. Therefore, we need to evolve our guards with changing times by performing regular security audits and to invest in a futuristic and machine learning security solution that keeps up with the rising cyber threats landscape.

37. Further he laid our cyber security measures for the organisation to prevent cyber-attacks:

(a) Educating employees on the emerging cyber-attacks with security awareness training.

(b) Keeping all software and systems updated from time to time with the latest security patches.

(c) Implementing email authentication protocols such as DMARC,DKIM and SPF to secure our email domain from email-based cyber-attacks.

(d) Get regular Vulnerability Assessment and Penetration Testing to patch and remove the existing vulnerabilities in the network and web application.

(e) Limit employee access to sensitive data or confidential information and limit their authority to install the software.

(f) Use highly strong passwords for accounts and make sure to update them at regular intervals.

(g) Avoiding the practice of password sharing at work.

38. He also laid out recommendations to raise cyber security to the Critical Infrastructure Sector as follows:-

(a) Strict segmentation and data logging of SCADA & ICS to guard physical isolation.

(b) Rapid Analysis and recommendation post Audit.

(c) Creating a Cyber Security insight and upgrading the security for New Legislation.

(d) Eliminating risks of data leakage and manipulation.

(e) Using Data Diodes to protect our information.

(f) Mitigating threats of remote access.

(g) Using high assurance technical solutions.

(e) Setting higher security requirements for suppliers by taking up the digital responsibility.

39. The last speaker of this session was **Ms Devsena Mishra**, Founder a2zstartup, shared her views upon **Weaponisng A.I. as related to Cyber Warfare**. She advocated the Weaponisng A.I. by leveraging Big Data and A.I. to enhance the technologies. Mentioning A.I. incorporation in the conventional, Unconventional and sub conventional operations around the world she further stressed on Atmanirbhar approach clubbed with our natural edge in the human resources in order to win eventualities that may arise.

40. The session was concluded with the closing remarks by **Brig. AJA Pereira.** Summing up the deliberations of the day**,** he highlighted the increasing importance of the cyberspace and growth and sophistication of attacks. Hhe stressed on proactive approach for securing the operational Technology and consumer technology for active defence (and not defence in-depth). Further he stressed on Technology being driven by people and not the other way around and for this and for this he reflected the need for being Atmanirbhar in the technology sector.

SESSION-IV
(CRITICAL NATIONAL INFRASTRUCTURE PROTECTION)

41. The fourth session was on the theme" **Critical National Infrastructure Protection)**" and was chaired by **Lt Gen P.K. Mallick, VSM(Retd)**.

42. The first speaker of this session was **Lt Gen P.K. Mallick, VSM(Retd)**, who shared his, views about "**Securing India's Railway, Air Infrastructure and SCADA: Challenges and Solutions**". At the outset, he underlined the difference between the Critical Infrastructure (CI) and Critical Information Infrastructure (CII), wherein he proposed that CII forms the backbone of the CI. Therefore, Physical security of CI and Security of CII may not be same but are intimately linked. He also comprehensively and precisely covered his views on how USA protects its CII and cited the loopholes of the Indian system were the Nuclear Power plants are not part of the National Critical Information Infrastructure Protection Centre (NCIIPC), lack of the executive authority to look over roles and regulation of the private sector in our society, etc. Further he proposed a list of recommendations to secure the ICS/SCADA systems:-

(a) Using a virtual patching to help manage updates and patches.

(b) Applying network segmentation.

(c) Using adequate security measures between the ICS network and corporate network.

(d) Properly managing authorization and user accounts.

(e) Using endpoint protection on engineering workstations connected to SCADA for device.

(f) Maintaining strict policies for devices that are allowed to connect to SCADA networks.

(g) Restrict the roles of transitory SCADA nodes to a single purpose.

(h) Prevent the use of unknown and untrusted USB devices.

43. The second speaker of this session was **Mr Sanjay Goswami**, who shared his, views about "**Securing Energy Supply Chains from Cyber Attacks**". He highlighted the importance of the Energy sector and its heavy reliance on the digitisation. Further he mentioned how today we are witnessing the dawn of the Kinetic Cyber age, discussed motives behind it and listed its grave implications on the economic and human security.

44. The third speaker of this session was **Dr Nishita Kaushiki**, who shared her, views about "**Need for a policy for protection of the Critical National Infrastructure**". She highlighted the importance of the Critical National Infrastructure and shed light on the requirement of policy on securing this Critical National Infrastructure by focusing on three aspects: Physical Security, Digital Security and Information Security (with a focus on Digital and Information). She further reflected upon how the cyber-attacks have expanded their threat landscape as Strategic dependency between civil and military domains (Power, water supply, media houses and data centre of foreign countries) any attack on these will affect both.

45. Further she proposed a list of recommendation to secure Critical National Infrastructure:-

(a) Defining concepts of Digital sovereignty of India to demarcate the acts of war in the cyber domain.

(b) Expanding the horizon of Hybrid warfare for secrecy and security of closed network groups and including sub-contractors, suppliers and data centres as they ensure the system integrity.

(c) Civil-Military fusion to formulate an umbrella of laws reflecting combined aspirations.

(d) Creating an active defence policy and clubbing it with the propaganda warfare and strategic communication for an Active defence and offence balance.

(e) Including cyber laws to tackle cyber-attacks and cybercrime in the upcoming sedition laws.

(f) Differentiating between defensive and offensive cyber capabilities in the operations. Developing offensive cyber capabilities with zero-reversibility to Deny – degrade – Destruct – Destroy - Manipulate cyber-attack.

(g) Formulating a Pro-Cyber doctrine by including perception management and media as vital components.

(h) Defining clarity in roles and responsibilities of Cyber defence team in peace time and field operations.

(j) Demarcating breaking point to determine whether the activity is an act of war or an act of intrusion.

(k) Fostering comprehensive approach in the joint operations and developing cooperative framework with friendly foreign agencies.

46. The fourth speaker of this session was **Mr Sanjay Vaid**, who shared his, views about "**Securing Operational Technology**". He highlighted on the fact that India is the country that faces the largest number of cyber-attacks in its cyber domain. He further demarcated a layered approach to the cyber security for securing the Industrial Control Systems in the Enterprise networks as well as the Industrial Networks. Further he also proposed a roadmap for securing the Operational Technologies:-

(a) **Assessment**: Conducting an IT/OT assessment in the industry/enterprise.

(b) **Framework**: Defining the framework we want.

(c) **Roadmap**: Placing the end state Architecture on the assessment and chosen framework.

(d) **Policy**: Defining an foundational IT/OT policy in place along with the governance model.

(e) **Solution**: Getting visibility on what we can see and what we cannot manage, secure remote access, advanced malware protection, data security, firewall, etc.

(f) **Monitoring and IR**: Getting an IT/OT SOC in place, (Not aiming for perfection rather starting wherever we are) along with well-defined incident response mechanism.

47. The last speaker of this session was **Mr Tanay Bhattacharya**, who shared his, views about "**NCIIPC for Imparting Training and Awareness in Critical Infrastructure Protection**". He highlighted the fact that we need to stress upon empowering and training our manpower as it is the weakest link in the chain of People - Process - Technology (PPT). As per his data only 2-3% staffs falls under the proficient cyber security operatives, this today is quite alarming for us as ensuring security and resilience of the CII is a shared responsibility. Further he stressed upon the role of Public – Private – Partnership (PPP) to deliver relevant, high class and action oriented training to critical sector organisations.

48. The session was concluded with the closing remarks by **Maj Gen PK Mallick (Retd).** Summing up the deliberations of the day**,** he emphasised the dimensions of:-

(a) Holding Custom Auditing Standards as auditing standards of different sectors are different.

(b) Harnessing talented pool of people in the armed forces and setting them up in the hierarchy and strategic leadership to solve the HRD issues faced by the forces.

(c) Giving statutory powers to impose penalties to agency responsible for the cyber security.

(d) Inoculating NCIIPC in the formulation of the strategic policies and CERT-In in the implementations of these strategic policies.

49. Further he highlighted the fact that despite Data Security council of India organised the exercises like NCIIPC still the platform was provided by Estonia. We must develop these capabilities and be self-reliant.

SESSION-V

(NATIONAL SECURITY INFRASTRUCTURE PROTECTION)

50. The fifth session on the theme "**National Security Infrastructure Protection**" was chaired by **Cmde Prem Reuben**. At the outset, he underlined the importance of Cyber security perspectives relating to the national security infrastructure.

51. The first speaker of this session was **Mrs K.B. Jenna**, who shared her, views about "**Role of Cyber Forensics in the National Security Infrastructure Protection**". She highlighted the importance of considering Cyber Forensics as a module within the National Security Infrastructure. She made the following points:-

(a) Effects of non-standard forensics methods being practiced today can be seen in:-

(i) Conflict of Interests.

(ii) Confusion and distrust within the community.

(iii) Failure in growth and maintenance of infrastructure.

(b) In her view, the investigation is as effective as the audit conducted on the device for the traces of activity. Therefore today, Auditability of devices is a grave issue to be looked upon. Device manufacturers should make sure that the components manufactured should be auditable in order to provide improved chances for the audits and investigations to be conducted.

(c) Repository of the Cyber forensic tools (Mobile Verification Toolkit) to be developed and released in the public domain in order to increase public participation in reporting breaches and spread awareness of the crime control.

(d) Indulging general public participation to achieve the national security roadmap.

(e) Formation of a dedicated Forensics Groups/Labs/Task force to counter and regulate threats in the society.

52. The second speaker of this session was **Cmde Prem Reuben**, who shared his views about "**Cyber Security Threats in the Maritime Domain**". He highlighted how Cyber Security in the maritime domain is an essential and vital element of the National Security Infrastructure protection architecture. Breaches in maritime domains have grave ramifications on various domains and ecosystems of the society. He also made the following points:-

(a) The critical need to recognise and acknowledge the Cyber threats posed to Critical Port Infrastructure and Ships at sea.

(b) Incorporating the cyber security dimension at the design stage of the Port infrastructures and vessels.

(c) Rampant vulnerability assessment of challenging tasks by incorporating subject matter experts to enhance the capabilities.

(d) Close collaboration between the Academia and industry for an effective threat assessment and risk mitigation.

53. The last speaker of this session was **Wg Cdr Rama Krishnan**, who shared his views about "**Integrated Cyber Defence**". He highlighted that Cyber security today is similar to an arms race and therefore the state actors need to be one step ahead of the cyber criminals to protect their critical assets. Silo approaches and point technical technologies are no longer efficient to counter emerging sophisticated threat scenarios of today. He also suggested the following points:-

(a) Integrating Networks along with the multiple security tools for proactive threat mitigation.

(b) Integrating Industry leading cyber technologies to provide enterprise wide network security and data protection, resulting in highly efficient incident response and threat detection.

(c) Formulating a unified security strategy and uniform set of security services.

(d) Integrating technologies and security system for faster response time.

(e) Close collaboration between the People, process and technology for an effective threat assessment and risk mitigation.

(f) Automating processes for threat intelligence and analysis. This would allow us to combine the extensive knowledge of threat landscape with ability to respond quickly at multiple level would set a foundation for High level security landscape enhancing security effectiveness

(g) Integrated approach will deliver unified view of organisation security posture for predicting threats and supporting fast and effective solutions.

X--X--X