PROCEEDINGS OF ROUND TABLE DISCUSSION
CYBER SECURITY : CITIZEN OF 2030

27 SEP 2017

BY

COL HARPREET SINGH, SENIOR FELLOW CENJOWS

1. The proceedings of the Round Table commenced with the felicitation of distinguished speakers and guests by Mr RK Srivastava, Delhi Public Schools. After the felicitation the Chairman of the Round Table, Lt Gen Vinod Bhatia PVSM, AVSM, SM (Retd), Director CENJOWS, commenced the proceedings.

Session 1 (Inaugural Session)

2. **Chairman's Address**. Lt Gen Vinod Bhatia, PVSM, AVSM, SM (Retd) welcomed the Distinguished Guests, Eminent Panelists, Subject Matter Experts and Students of DPS Bhagalpur and DPS Greater Ranchi. He said that the topic for discussion is contemporary, apt and one which will not only impact our values, beliefs and relationships but also the way we live. He then laid down the construct & concept of the RTD. He finally requested all the distinguished speakers and experts to flag at least a couple of takeaways and policy options to prepare the citizens of tomorrow to meet the challenges and threats in the cyber world, which is an imperative for us to chart out a possible, actionable road map to prepare our citizens in the field of cyber security.

3. **Address by Chief Guest**. Lt Gen DB Sheketkar, PVSM, AVSM, VSM (Retd) complemented the organizers for getting students to attend the round table as they will be the major stakeholders by 2030. The 19th century was the century of muscle power, the 20th century was the century of money power while the 21st century is the century of knowledge power. Combination of knowledge and wisdom is what will take the country forward in the future. Children should be aware regarding what to believe on the net and should not hide facts from parents. Parents should not allow children to get hold of that technology which can destroy them. We need to make our children cyber secure and aware of the dangers of social media by increasing awareness through various means and avoid systematic destruction of our future generations.

4. **Introduction to the Theme of the Conference**. Mr Rahul Aggrawal, Price Waterhouse Coopers, said that day to day services can be controlled, attacked and disrupted by using technology. He gave examples of how vehicle accidents, crashing of hospital systems, tampering of locking systems in

hotels, etc can be done without using any guns or missiles. This is possible because IT penetration is ever increasing and it is imperative that we discuss today how this technology needs to be harnessed in the next 13 years. He mentioned four critical focus areas in the future. Firstly, how to manage and protect critical infrastructure, secondly, how to create a cyber aware society and make our children cyber aware, thirdly, how to create an ecosystem wherein everyone is aware of netiquettes and fourthly, how to build capabilities in HR, skill and technical infrastructure.

5. **Keynote Address 1**. Lt Gen Vinod Khandare, AVSM, SM, DG DIA, said that future wars will be a combination of Kinetic and non kinetic means with non kinetic means having more importance as they will control kinetic means. For intelligence agencies cyber is very useful if they can use technology better than the enemy. To earn respect and power, a nation must have a combination of niche technology, emerging technology and incubating technology. India must endeavour to be a leading figure in the world of technology dominance by 2030.

6. **Keynote Address 2**. Lt Gen VM Patil, PVSM, AVSM (Retd) brought out that computers and smart phones have now become a way of life. Smart phones will become a part of education system in future so we might as well think and prepare for this today. Non state actors are going to play an increasingly important role due to the anonymous character of cyber world. China has thousands of non state militia for hacking, spying, espionage and sabotage. Blackouts in our regional electricity grids and other cyber attacks have been caused by China in the past. They also have more than 100 technical companies established in India. During the recent Doklam standoff Chinese cyber activities were directed towards India with a view to create a fear psychosis. There is a need to change old mindsets in our country and develop in house technology to match the future cyber challenges posed by China and other adversaries.

7. **Special Address 1**. Rear Admiral SY Srikhande, AVSM (Retd) highlighted the need to be conscious of what we do on social media as it is very difficult to be prudent. Children are especially vulnerable as the cyber world makes them drop guard and have a perception of friendship in numbers. There is no fiscal prudence as communication on the net is free which results in higher quantity and lower quality of communication. We need to conduct workshops for both children and parents to teach them virtues of prudence on line. China has own satellites, servers, human resources, etc with a view to prepare for the future and India must follow a similar path. We need a campaign named, say, Savdhan India or Satark Bharat to make our citizens aware of cyber security.

8. **Address by Subject Matter Expert**. Brig Manjeet Singh, DACIDS (DIARA) informed the house that the cyber domain is huge and there are going to be 50 Billion internet connected devices by 2020. Though Indian Army has air gapped networks but these are built up on imported hardware and updating of the same often requires connecting machines to the internet which may render the network vulnerable. The challenges faced by the defence forces are supply chain dependence on imports, targeted attacks (spear phishing) on machines, lack of adequate structures, low technical HR development, lack of trust in hardware due to poor in house chip manufacturing base, etc. The student community must get into cyber mode with passion to ensure that national security will not be outsourced in the future.

9. **Special Address 2**. Mr Jayadev Ranade, Centre for China Analysis and Strategy, said that China and Pakistan pose major challenges in the cyber space. China had set aside 90 Billion dollars set aside for propaganda in cyber domain five years ago. China has done electronic and telecommunication attacks previously and they have multiple targets in mind like Dalai Lama, Taiwan and US. It is a matter of concern that almost 80% of our telecommunication equipment is Chinese. We need to start cyber security and awareness through courses, funded by the IT sector, in schools and colleges. There must be on overhaul of existing rules and regulations and the aim should be to eliminate all Chinese products from critical areas.

10. **Special Address 3**. Mr Vinit Goenka, Centre for Knowledge Sovereignty, highlighted the importance of keeping data within own domain because if data is outside own precincts it will be used by others. Machines going out of secure environments for repair or changing of hard discs are vulnerabilities which need to be guarded against. We must remember that nothing on the net is free and citizens must surf the net with due prudence. We must be strong in the cyber domain as a nation as disruptions in, for example, the rail reservation system have the capability to cause widespread unrest. There needs to be a concerted national effort in this direction with active participation of the private sector.

11. **Address by Subject Matter Expert**. Dr Vipin Tyagi, Centre for Development of Telematics, highlighted the importance of indigenous communication as it is the first building block of a nation. C-DoT builds all its hardware and software indigenously and this concept is the way forward as the real threat will come from breaking down encryption codes by Quantum Computing. C-DoT has started for safe encryption and for guarding against cyber kinetic attacks. In future we need to think in terms of dedicated networks and not machines. We need to commission a task force to handle indigenization at the national level.

12. **Address by Subject Matter Expert**. Dr BVL Narayanan, CRIS, informed the house regarding the safety features in the Indian Railways Systems. All trains are systems controlled and any problem there will disrupt the railway services. In addition to technology, citizens are an important part of the surveillance and feedback system of railways. There is a need to monitor the large number of hits on the railway system to prevent any breach. In future, children can contribute for the same provided they are provided proper training in schools.

Session 2 (Experts)

13. The speakers in this session were Mr Amitabh Mathur, IPS, Dr SD Pradhan, Joint Intelligence Committee, Brig Pradeep Arora, DDP, Commander LR Prakash (Retd), CDAC, Ms Sumitra Goenka, CKS, Ms Ambika Khurana, IBM, Mr Bharat Panchal, NPIC, Dr Savita Kakar, DRDO, Dr Arunima Chakravorty, DPS Bhagalpur, Ms Sanjukta Mookerjee Sahani, Cadence, Mr Pavitran Rajan, CSRC, Ms Uma Sudhindra, IIM Vizag, Prof Dr Sharad Sinha, NCERT, Mr Avadhesh Mathur and Dr Vatsala Joshi Pandey, PS to Speaker Lok Sabha. The speakers/experts in their respective fields gave the following valuable inputs during this session :-

(a) There must be efforts made by national polity to have a cyber footprint all over the world as done by China.

(b) India must move from policy to strategy now and bring out a comprehensive cyber strategy. This strategy must focus on capabilities and not products. We must eliminate lack of will, fear, uncertainty, doubt, and carry out an honest appreciation of the requirements of the cyber domain

(c) India needs to guard against semi-literate citizens being forced to use digital devices for financial transactions. There is a need to bring in Apps or mobile phones with inherent safety features.

(d) India must focus on cyber awareness, fake news detection systems, protection of physical and digital assets, data security, making digital knowledge compulsory and encourage children to take up careers in the cyber security field. Cyber range labs like the one established by DPS Bhagalpur must be established in more schools. Teachers and educationists also need to upgrade their cyber knowledge. We must prepare for changes in future education systems like digitization of books and robots imparting knowledge to students.

(e) There must be more safeguards for food security as new technology renders our supply chains vulnerable. We must prepare for e-homes, e- hospitals, etc in the future.

(f) Make in India should be given full support and the government must strengthen Public Private Partnerships. We need to look at global quality, best practices and solutions and not try to re-invent the wheel.

(g) With increase in data proliferation and Internet of Things looming on the horizon, India needs robust systems to check security lapses and have measures for detection and recovery in place.

(h) Children must be taught cyber ethics and measures against cyber bullying. NGOs must be encouraged to conduct cyber safety capsules in schools from class II onwards.

(j) All digital products should be under national laws to deal with cyber crime. Citizens need to be aware and be wary of the dark net to prevent criminals from stealing personal data.

(k) Institution of Cyber Command at the earliest is imperative to secure military assets.

Session 3 (Open Session)

14. The following questions were asked by the students attending the seminar.

Question. Why is India lacking in cyber security ?

Answer. The major issue is lack of human resource and experts in the cyber domain. Changing education system to a cyber oriented curriculum will obviate this problem.

Question. Is data safe on cloud services from theft and from criminals on the dark net ?

Answer. We need to be careful while posting data on cloud services as servers are located outside the country. It is best for children not to explore the dark net as there are chances of getting into legal trouble and coming into contact with criminals.

Question. What are the basic essential netiquettes?

Answer. Essential netiquettes will be mailed to the school.

Question. How does the government tackle VPNs used for illegal purposes ? Why does the government not employ offensive cyber weapons against adversaries ?

Answer. The government has mechanisms for both aspects, but this information is classified.

Question. Are Chinese on line games safe?

Answer. Basic safety precautions must be taken while downloading any games/apps. Do not give access to data/contacts to any apps/games.

Session 4 (Valedictory)

15. **Valedictory Address.** Mr Shekhar Dutt, Former Governor of Chattisgarh, said that entrepreneurs and the youth must find solutions to problems in the cyber domain. An open mind and proper use of digital tools will give solutions to counter future cyber attacks which will be more difficult to handle as they will be different from current attacks. He said that it was heartening to see the participation of the armed forces and school children on this contemporary topic. He finally thanked the organizers and participants of the round table for making it a success.

16. **Vote of Thanks.** Mr RK Srivastava, Delhi Public Schools, thanked the distinguished speakers, experts and other participants of the round table for their active participation and valuable inputs. He said that there was a need to change the education landscape and redefine education curriculum to meet cyber challenges. Students should have a holistic view about security including cyber security.

17. The Chairman concluded the proceedings of the Round Table.