# CYBER SECURITY, DATA PROTECTION AND BIG DATA ANALYSIS: CITIZEN OF 2030

## 11 APR 2018

## BY

## COL HARPREET SINGH, SENIOR FELLOW CENJOWS

1. The Conference was held at Constitution Club of India, New Delhi, on 11 Apr 18. Cohosted by CENJOWS and CKS Delhi. The proceedings were commenced by Mr Kazim Rizvi, Founder, The Dialogue, who welcomed the chief guest, The Hon'ble Minister of HRD Shri Prakash Javadekar and other distinguished speakers and guests. This was followed by presentation of bouquet to the chief guest, the lamp lighting ceremony and release of a book on "Cyber Security Citizens of 2030".

2. **Address by Hon'ble Minister of HRD Shri Prakash Javadekar.** The Hon'ble Minister complemented the organizers for choosing an important topic for the conference. He hoped that the inputs of various cyber experts will bring out valuable recommendations which the government can implement. He quoted the questioning of Mark Zuckerberg by the US Senators wherein Mark Zuckerberg has admitted that that while they founded a great platform in Facebook, the company failed to realise the pitfalls that came along with technology. This is true for every new technological development. A prime example is the rapid proliferation of mobile phones which has improved life but has brought along corresponding problems of addiction and other socio economic issues. Citizens need to be made aware of technical initiatives, like Aadhar, which have taken by the government to protect citizens. Though there are lot of apprehensions regarding Aadhar, it is largely a secure data bank. Aadhar has eliminated bogus scholarships and subsidies which has resulted in savings of Rs 57,000 Cr each year. Hence we should not oppose new technology and instead but we need to accept technology and anticipate its future misuse. IoT, 3-D Printing, Robotics, etc have revolutionized production, but we need to use these technological innovations with inherent cyber security. There is a need to change our education system and put more emphasis on improving abilities of students in the areas of comprehension, analysis and creative skills. The HRD Ministry is already working to reduce the existing syllabus of students by 50%, while bringing in new aspects like gender sensitization, life skills, compassion, etc. Cyber aspects will also get enhanced weightage in the future curriculum. He requested the audience for suggestions on this issue on the HRD website.

3. **Other Speakers**. The chief guest's address was followed by addresses by cyber security experts/distinguished speakers like Lt Gen (Dr) DB Shekatkar, AVSM, PVSM (Retd), CKS, Lt Gen VM Patil, AVSM, PVSM (Retd), CKS, Lt Gen Vinod Bhatia, PVSM, AVSM, SM (Retd), Director CENJOWS, Lt Gen Vinod Khandare, AVSM, SM (Retd), Cdr LR Prakash, CDAC, Ms Meenu Chandra, Microsoft, Mr Anil Bhasin, Palo Alto Networks, Mr Tarun Vijay, Mr Bharat Panchal, NPCI, Mr Vikrant Khandelwal, Zonal Organisational Secretary, ABVP, Mr Ambrish Bakaya, HPE, Dr Unnat Pandit, Niti Ayog, Mr Vinit Goenka, CKS, Ms Vandana Nanda, CRIS, Ms Sumitra Goenka, Triangle and Fresh Frugies, Mr Karma Bhutia, iShippo, Mr Kazim Rizvi, The Dialogue, Mr Saurabh Rai, Tech Mahindra, Mr Tabrez Ahmed, UPES, Ms Sanjukta Mookerjee Sahani, Jaago Teens NGO, Mr Avik Sarkar, Niti Ayog and Mr Rajat Dhar, Finogent Advisory. The speakers/experts in their respective fields gave the following valuable inputs during this session :-

(a) Emphasis was laid by many speakers on the Prime Minister's recent statement that we need to have servers of big companies in India to ensure that citizen's data remains within the country. We need a specific department/ministry which is accountable and responsible for all cyber aspects pertaining to the nation.

(b) Best hackers are in the age bracket of 15-21 years. Hence for India to become a cyber power, guidance/exposure of students in this field is very important. The nation must give access to digital literacy to everyone from grass root level.

(c) Defence hubs proposed under the Make in India initiative will be using large amount of data which will need to be safeguarded.

(d) In future, India will be holder of the largest data bank in the world. We need to cater for national emergencies which may be caused by disruption or stealing of this data. A case in point is the recent cutting of undersea cable in six African countries which has resulted in a complete disruption of digital services and brought these countries to a standstill.

(e) Future wars will be through the cyber domain without knowing the adversary/attacker. This has the potential to arouse unnecessary suspicions and lead to trust issues between nations.

(f) Recent disruptions of websites of some ministries may be an attempt by China to test effectiveness of its cyber measures and we need to develop effective counter measures and especially strengthen the weakest link. More often than not it is people who are the weakest link and cyber security awareness is now an imperative for all government officials.

(g) With increase in data proliferation and Internet of Things looming on the horizon, India needs a comprehensive cyber security policy, develop own hardware/software, have own servers, have own platforms like SAMVAD (which can replace whatsapp), etc. All these must have in built control, testing and audit facilities.

(h) Rapidly developing technology like image processing with AI implies that almost all data of an individual will be available to AI platforms in the near future. This technology has the potential to spread fake news and cause sociological problems, both at institutional and personal level, and even break up families. We need our AI hardware and software to be designed in India to safeguard our society.

(j) Students are making new innovations and gadgets under the Atal Innovation Mission. An example is a prototype, made by Class IX students, of a wrist worn device which can predict heart attacks. Children must also be taught cyber ethics and measures against cyber attacks.

(k) In-house platforms and tools are required for effective cyber warfare. Since military and non-military domains are difficult to segregate in cyber space, a multi agency organization is required to identify gaps, evolve strategy/road map and allocate resources. We need to develop a strategic culture and take the lead at global level to enhance our cyber capability.

(l) Technical giants like Microsoft and Apple are constantly trying to find solutions for cyber security. The latest trends are that the firms itself are developing technology to home on to perpetrators of cyber attacks in a short span of time. India must hold OEMs accountable for cyber security of their platforms.

4. **Closing Ceremony.** The MC expressed satisfaction that more institutes are joining this initiative with each conference. The ceremony concluded with a Vote of Thanks.