

CYBERSECURITY CITIZENS OF 2030



“The Union HRD Minister Shri Prakash Javadekar released the “Cyber Security of Citizen 2030 book” at the event, a collection of articles by various stakeholders. Mr Javadekar emphasized that information related to technology should be given to the children. He urged the public to send in more suggestions as part of the govt.’s move to reform school curriculum. He mentioned that Use of technology in welfare schemes under PM Modi’s leadership has helped India save nearly ₹57,000cr, Use of technology in governance has even helped in curbing cases of fraudulent scholarships, added the Minister. It’s important to inculcate the right use of technology in children from an early age, said the MHRD Minister.”

Click Safe. Stay Safe.





Design, Layout and Typesetting done by Manipal Digital Systems, Manipal - Pioneers in Pre-Media and Digital Content Solutions. Printed at Manipal Technologies Ltd, Manipal. - India's Largest Commercial, Secure & Innovative Print Solutions Provider.



FOREWORD

Cyber Security today threatens to disrupt our very way of life. Cyber Space challenges our culture, beliefs and value system. Cyber threats are all pervasive with the ability to intervene and attack our education system, financial institutions, transportation sector (rail, road, air and sea), power and energy, industry, communication and defence, among others.

Internet, social media, smart phones and tablets are an integral part of our lives facilitating all our functions. Future technologies in the cyber world like Internet of everything, Artificial Intelligence, machine learning, autonomous gadgets, BOTs, 3D printing and block chains will grow exponentially and become an adjunct to our lives. Today's world, thanks to Cyber Space is a connected, networked and shared world. The key question is, are we as India and Indian Citizens prepared to face the Cyber security challenges. We need to create structures and systems, organizations and critical infrastructure to ensure a secure nation and well being of our 1.3bn citizens.

The majority of smart gadgets, whether in large corporations, in small businesses, or at home, are connected together in a network that creates a global community. People have become increasingly dependent on the cyberspace for their day to day transactions to conduct business globally. Most people understand that global digital infrastructure is becoming increasingly dependent upon information technology, and no information system is 100% secure. Information security is a topic that everyone knows, but most are not aware of the gravity of the threat. Many users simply think that their firewall and antivirus software provides them with all the protection they need to keep their computers secure. However, as malicious hackers become more resourceful, and users add more information into a growing number of databases, there exists an increased exposure to hacker attacks, information espionage, and other security breaches. Information systems - operated by governments and commercial organizations - are vulnerable to attack and misuse through their internet connections. Workstations connected to the internet are currently the most common targets of malicious hackers. As a result, information assurance is a very serious concern for individuals, businesses, and governments. Not only do we need to be aware of how attacks are perpetrated, but we also need to learn how the systems can be protected against different attacks.

The challenges in cyber security are both difficult and interesting. People are working on them with enthusiasm, tenacity, and dedication to develop new methods and provide solutions to keep up with the ever-changing threats. In this new age of global interconnectivity and interdependence, it is necessary to provide security practitioners, both professionals and students, with guidelines, a focused approach towards a cyber-security policy and knowledge on the frontiers in cyber security challenges in future.

Lt Gen Vinod Bhatia, PVSM, AVSM, SM (Retd)
(Former DGMO)
Director
Centre for Joint Warfare Studies (CENJOWS)

Thank You note by Lt. Gen Dr. D B Shekatkar PVSM,
AVSM, VSM (Retd)
Chairman
Centre for Knowledge Sovereignty



I ask the indulgence of the readers of this book, both young and old, to put aside sometime to ponder and think over the salient points brought out in highlighting Cyber Security 2030 challenges and solutions. This book attempts to put together ideas & thoughts of various people, agencies and departments involved in the domain of cyber security on one platform. In the process of collating this book together,

the editorial team also realised that this is just the beginning. To develop thought leadership in the cyber security domain, it is important for all the stakeholders to consistently work together and facilitate the necessary changes.

We, at CKS, thank each and everyone who was part of the Round Table and the subsequently contributed to the book. We also look forward to more interactions. ■



Message by Lt Gen V. M. Patil AVSM, PVSM (Retd)
Vice Chairman
Centre for Knowledge Sovereignty



In recent years, cybersecurity has emerged as a major focus of national and international concern, as nations, organizations, and individuals realize not just the benefits of the digital revolution but also the scope of cybersecurity vulnerabilities and threats. Consequently, cybersecurity has emerged as an area of intense research activity and great professional demand.

As part of the founding team of Centre for Knowledge Sovereignty (CKS), I invite you to read this book that

has been put together by our editorial team. I also take this opportunity to invite you to our events, where you will come back richer with information and best practices. Our Centre is committed to creating platforms for cyber security professionals and students to come together to create a value proposition for the future.

Looking forward to seeing a cyber strong India. ■



Acknowledgement by By Vinit Goenka
Member-Governing Council-CRIS, Min of Railways;
Member-IT Taskforce, Ministries of Shipping, Road Transport
& Highways
Secretary, Centre for Knowledge Sovereignty



Since the book on Cyber Security was conceptualised, I have received tremendous support from many individuals and organisations from different walks of life. I have been blessed to get the encouragement from my seniors like Lt Gen Dr D B Shekatkar, Lt Gen V M Patil, Lt Gen Vinod Bhatia, Lt Gen Vinod Khandare, Shri Jayadeva Ranade, Ms Uma Sudhindra and my friend Mr Bharat Panchal who have helped me to bring all the people together for series of events to take this initiative ahead. I wish to thank them all for their support and encouragement.

I also wish to thank His Excellency Hon'ble Shri Shekhar Dutt the Former Governor of Chattisgarh for his support and joining us at the round table conference and further events as a Guest of Honor.

I thank the entire team of CENJOWS and especially Col. Harpreet who have helped us in organising the events starting with Manekshaw Auditorium. I wish to thank all the Uniformed officers who have participated in our events and extended their support.

I wish to thank our Knowledge Partners PWC for participating in the Round table conference and sharing the Knowledge Partnership report "Creating a Cybersecure Society".

I wish to thank our Publishing Magazine Partners VAR India and especially Ms. S. Mohini Ratna and Mr Deepak Kumar Sahu for publishing the Roundtable summary in their Online Edition, Monthly magazine and Youtube channels.

I am thankful to Shri Rajesh Srivastava, Pro -Vice Chairman of DPS Bhagalpur and DPS Greater Ranchi and Dr Arunima Chakravorty, Principal of DPS Bhagalpur and DPS Greater Ranchi for the partnering with CKS in the event. I thank all the students and teachers of DPS Bhagalpur and DPS Greater Ranchi for attending the Round table in Manekshaw Auditorium in Delhi as delegates travelling all the way.

I would like to thank the Editorial Team involved in this project and, more specifically, to the authors and reviewers that took part in the review process. Without their support, this book would not have become a reality.

I would like to thank each one of the authors for their valuable contributions. My sincere gratitude goes to the chapter's authors who contributed their time and expertise to this book. I also thank all the panellists who have been a part of our events so far but have not contributed yet to this book. I am aware that your thoughts are always with me and would like to see your thoughts in our upcoming book.

I thank the organising team of CKS, CENJOWS and Zereone for the smooth planning and execution of the event.

Finally, I wish to express my gratitude to my personal team for working relentlessly towards achieving this goal. I thank my family for been a pillar of support. ■

Vinit Goenka
Secretary CKS



CONTENTS

Cybersecurity Citizens of 2030	1
Foreword	3
Cyber Warfare and Cyber Security: Indian Armed Forces	8
Cyber Security & Youth Education	10
Cyber Security – Everyone’s Responsibility	12
Facing The Cyber Threat – 2030	14
Cyber Security 2030	16
Why Should We Store Data In India?	18
Loose Lips Sink Ships – Why Prudence Matters The Most for Cybersecurity.	20
India Needs A National Cyber Strategy	23
Security Including Cyber Security for A Large Service Organization.	26
Design In India for New Digital India	28
Understanding Data Security for The Future of Businesses	30
Building India’s Cyber Capability	31
The Fallacy of The Cyber Commons	33
Cyber Safety for Children – Challenges And Suggestions Jaago Teens, Ngo	38
Cyber Literacy for 2030	40
Challenges-Cyber Security – 2030	42
How Should Governments Protect Citizens?	45
It Security: The New Commanding Height of The Economy	47
Participants At The 1 st Round Table on Cyber Security Citizens of 2030	56
Pwc Report- Knowledge Partners	59

CYBER WARFARE AND CYBER SECURITY: INDIAN ARMED FORCES

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



The second Cold War is widely believed to have started in 2014, however, contours are very different this time. Apart from media and social media, the most exploited arena in this Cold War is the cyber domain. The Russians are widely suspected to be involved in hackings and leaks which had an alleged effect on the US Presidential elections. The cyber war however goes much beyond US and Russia with other nations like Israel, North Korea and China being active participants. Besides the US, Iran and Estonia have faced crippling cyber attacks which are thought to be state sponsored and have proved the power of cyber warfare to shift focus from the conventional to the virtual domain. Easy access to the internet and readily available cyber tools enable 'lone wolfs' and 'non-state actors' to launch cyber attacks. The advantages of non-attributability and deniability are exploited to the hilt in the cyber domain. There are no traditional and physical boundaries in cyber warfare and it is characterized by anonymity, ambiguity, speed, no warning or indicators and lack of posturing. In conventional warfare surprise is a critical element and cyber attacks achieve this almost every time. India and especially its armed forces need to be aware of these cyber realities and incorporate appropriate concepts into their warfare strategy.

Cyber Threats – Indian Context.

As far as India is concerned, 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. It is believed that the PLA's strategic cyber command is situated in the PLA's General Staff Department. It has 1,30,000 personnel and pool of at least 25 million people who have the basic education to participate in cyber warfare, hacking, espionage, spying and sabotage. The role of Chinese PLA Unit 61398 and the National Security Agency in launching sophisticated cyber espionage activities is well known and is in open domain. In May 2008, Chinese hackers allegedly broke into our Ministry of External Affairs. Chinese hackers are known to have used social networking sites to break into computer networks of the Indian defence establishment like the National Security Council Secretariat, 21 Mountain Artillery Brigade, Air Force Station Delhi, etc. During the recent

Doklam standoff Chinese cyber activities were directed towards India as part of its psychological warfare. Blackouts in our regional electricity grids and other cyber attacks have been caused by China in the past. It is a matter of concern that almost 80% of our telecommunication equipment is Chinese. They have more than 100 technical companies established in India. There must be an overhaul of existing rules and regulations with the aim to eliminate Chinese products from critical areas.

The threat from Pakistan is again significant, though their technical prowess is lesser than China, the motivation levels against their 'eternal enemy' may be much more. Pakistan has been defacing Indian websites through hacker groups like Pakistan Hackers Club, G-Force, etc in the past. These groups are of the firm belief that they are working for the cause of Kashmir. Lately some groups have taken to social media to discredit the army and cause unrest in the rank and file. There is a concerted effort by Pakistan for employment of social engineering in cyber space with special reference to social media.

Lone Wolf and non-state actors also pose significant threats. The lack of cyber expertise with such actors is often made up by hiring cyber criminals though the Dark Net for a specified fee. The anonymity factor makes these actors more adventurous as the risk of getting caught is minimal especially if working from another country.

Cyber Structure of the Armed forces

The three critical aspects of cyber security are people, process and technology. There is a continuous effort to plug gaps in these three critical aspects through continuous technological upgradation, advisories, guidelines, training and audits. There is a profusion of armed forces agencies dealing with cyber issues ranging from the Corps of Signals to CERT-Army/Navy/Air Force, the IT departments of various headquarters and the Integrated Defence Staff. The Defence Information Assurance and Research Agency (DIARA) has been designated as the nodal agency mandated to deal with all cyber security related issues of the Tri Services and Ministry of Defence. These agencies work as per guidelines laid down, in coordination with CERT-In which was created in 2004. These agencies are mandated for safeguarding the cyber system

by creating appropriate standards/guidelines, rapid emergency response, audits and advice. The processes and guidelines followed are iterative with accountability and responsibilities earmarked.

Challenges

The cyber domain is huge and there are going to be 50 Billion internet connected devices by 2020. The Internet has become a weapon for political, military and economic espionage. The dependence of cyber space by the military makes it an object of attack. Attacks can be physically on the facilities where the hardware of command, control, communications, computers, intelligence, information, surveillance and reconnaissance (C4I2SR) systems are located, or they can be on the software by distorting the programs which operate the C4I2SR systems.

Each service of the Indian Armed Forces have their own set up for cyber security of critical military assets. This in effect means that the Army, Navy and the Air Force are working in silos and there is hardly any inter communication with respect to this critical aspect. Actually, the inherent secretive nature of the armed forces does preclude jointness. HQ Integrated Defence Staff has tried to bring in some jointness in this regard but the existing structures may not allow much exchange of cyber information. May be with the proposed cyber command coming up the defence cyber space will be streamlined.

The Indian Army has its own air gapped networks which give it a high degree of security. However we do have a history of cases like the Stuxnet virus, which prove that air gapping alone does not guarantee cyber security. The army's network is built up on imported hardware and updating of the same often requires connecting machines to the internet which may render the network vulnerable. The low threshold of education and technical knowledge of soldiers remains a cause of concern. Training such a large military on cyber aspects is a problem area. Also the inherent fast pace of technology in the cyber domain necessitates re-training periodically which is difficult administratively and we need to come up with new training methods which enable on the job training without compromise on standards. The infrastructure for such training needs to be put in place.

The other challenges faced by the defence forces are supply chain dependence on imports especially Chinese, targeted attacks (spear phishing) on machines, lack of adequate structures, low technical HR development in the country, lack of trust in hardware due to poor in house chip manufacturing base in the country, etc.

Way Ahead

The Joint Doctrine of the Indian Armed Forces was released in April 2017. This doctrine is a revised version of the first document which was released in 2006 and addresses the current realities. The Doctrine recognizes the five domains of modern warfare ie land, sea, air, space and cyber space. It lays due emphasis on establishment of the

Defence Cyber Agency with both offensive and defensive cyber warfare capabilities. The nucleus is already in place and is functioning under the HQ Integrated Defence Staff. With the cyber arena now recognized as a new domain of warfare, setting up a force competent to achieve the dual objectives of defending the country from cyber attacks in war and securing the military's network operations in peace requires deep and pragmatic thought.

Cyber Command.

Just as defending the territorial integrity of India is the sole responsibility of the armed forces, they should also be responsible for defending the national interests in cyber space. The US and China had established their cyber commands in 2010 and their cyber work forces are gaining expertise to forge ahead in cyber war fighting. There is an urgent need to establish a tri services cyber command which should function under the upcoming Chief of Defence Staff who would be answerable to the Cabinet Committee on Security. It would also help in real time information sharing and coordination with other government cyber agencies like CERT-In. The dedicated mission teams could be adequately decentralized to, say, Division levels and be given specific tasks of cyber attack, cyber defence, support, etc. Offensive cyber actions are generally not discussed in open domain, but it goes without saying that this aspect will also be looked after by the cyber command as a purely defensive approach in any military operation is a recipe for disaster. However, for the cyber command to be a success we also need a dedicated and trained work force, build a cyber culture in the armed forces and have lateral partnerships with other cyber agencies, including foreign ones.

The student community must get into cyber mode with passion to ensure that national security is not outsourced in the future. We need to start cyber security and awareness through courses, funded by the IT sector, in schools and colleges. 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. The development of niche expertise within the armed forces and participation of other agencies, including the PPP model also needs deliberation.

The future digitized battlefield will operate in a hostile cyber environment. Disruptions and loss of data and information will be felt at the operational and tactical level. Inadequate cyber warfare capability/cyber security will inflict considerable damage to the Indian defence forces and be detrimental to national security. India's strategic challenge in cyberspace emanates not just from external threats but is exacerbated by its rapidly increasing digital ecosystem. A comprehensive National Cyber Force Structure with Cyber Command at the apex will not only allow the Indian Armed Forces to gear up for cyber war fighting and win a net centric war but will also enable synergy with other national agencies/organisations using the cyberspace thereby providing holistic cyber security to the national assets. ■

CYBER SECURITY & YOUTH EDUCATION

Lt. Gen Dr. D B Shekatkar PVSM, AVSM, VSM (Retd)

Chairman

Centre for Knowledge Sovereignty



Cyber security is a problem that we all must be concerned about. It is something that has the potential to impact each one of us. From individuals and small businesses to massive enterprises and government agencies, there's no entity that falls outside of the scope of cyber criminals. What this creates is a computing environment that's filled with malicious threats for all users - if they aren't suitably defended.

With increasing virtual threats out there, the requirement to strengthen their guard and firm up network security infrastructure falls squarely on the potential targets themselves. Unfortunately, this is something that's overlooked far too often. At every level, from the individual to the biggest corporation out there, there's not enough being done to defend against cyber-attacks. And yet the consequences of being attacked couldn't be clearer - as one industry website pointed out, six out of 10 businesses suffering data loss will cease to be operational within half a year.

Many companies, government organisations and other entities find it hard to defend themselves due to a perceived talent shortage in cyber security skills. One will be hard-pressed to find a more in-demand job right now than a cyber security specialist. From the small start-up that just launched its app to the major corporation raking in billions a year, every organization needs cyber expertise. However, such roles call for a relatively new training program, and as a result there aren't the numbers to meet the need in terms of virtual security specialists. But that is beginning to change, globally, as young people are being educated in cyber security.

A Growing Force

Hackers don't exist in a state of inertia. They're always growing, evolving - and as they evolve, so do the threats they propagate. With each malicious network intrusion, cyber criminals gain power and actionable findings. They learn how to refine their criminal craft, and they equip themselves with the tools they need to bring down even more high-value targets. Unfortunately, this kind of rapid growth within the virtual crime sector hasn't been matched by a commensurate push to evolve cyber defence.

At the start of 2015, the US government announced a \$25 million grant rolled out by the U.S. Department of Energy to support educational efforts in cyber security.

The announcement of the grant was a pivotal moment for the virtual crime fighting sector: Not only did it acknowledge the government's commitment to fighting cyber-crime, it also showed that it's ready to significantly invest in the future of computer protection.

There is a crying need in India to do the same.

That future is embodied by the young people who will be taking up the cyber cause. In addition to being important and highly in-demand work, cyber security jobs pay extremely well. As reported by various recruitment surveys, the average cyber security professional can expect to take home \$116,000 a year. That is approximately three times the average salaried income.

Interestingly, the inducement to work in cyber security goes beyond the pay check. "For top talent, cybersecurity isn't about just a job and a pay check," he said. "It is about the hottest technology, deployed by honourable organizations, for a purpose that is inherently important."

Given the nature of this work (lucrative or otherwise), it comes as no surprise that cyber security-based programs are cropping up at educational institutions all over the world. What may be somewhat surprising, though, is how early such educational efforts are beginning. From middle school through graduate programs, the goal with cyber job growth seems to be to get them while they're young and train them into the best experts they can be.

The Indian Scenario

With the digital education space growing in India, it is critical that our school curriculum becomes more practical and includes topics in cyber security. A few years from now, it should be commonplace for 11 and 12-year-olds to learn about cyber security right alongside the periodic table of the elements. Today, a lot of people may scoff at the idea of such young students learning about cyber. It is important to understand the speed at which the internet has taken over our lives. Cyber education is idea that must quickly gain traction in the Indian schooling system.

Schools in US & Israel are teaching students about encryption techniques and how you can hide data. These skills are part of an after-school program where middle school girls can learn the basics of cyber security. The

reason it's a girls-only program is because, women only constitute 10 percent of the cyber security workforce. Countries are focussing on balancing the gender differences in cyber knowledge also. We have a long way to go.

For all workers who enter the cyber security field, having a strong set of virtual security skills will be imperative. The battle against cyber - crime will call for a workforce that's able to anticipate moves hackers make before they make them. This isn't happening in all the fields today, since malicious hackers enjoy the upper hand. On the other hand, if the educational system and ensuing employment opportunities increase multi fold, hackers may not be able to enjoy their advantage for too long. This will depend on how we as a country can unleash the potential of our indigenously trained cyber focussed youth.

Making Cyber Literacy All Encompassing

Educators and strategists who are building cyber education programs hope these efforts instil in young people the values and interests that will stick with them and hopefully lead them into ethical cyber-based careers.

To that end, more specialized college and graduate programs devoted to cyber careers are materializing at the graduate levels. It will serve us good to prepare students for career opportunities in the cyber security field, including positions as cryptanalysts, cyber law enforcement specialists, security administrators, computer crime investigators and computer forensic specialists. Combinations of law, ethics, political systems, trade, commerce and cyber literacy will go a long way in building a workforce that can contribute meaningfully to society and government, alike.

According to The National Cybersecurity Institute, USA, a big part of maintaining strong cyber security, means keeping ethical considerations in mind. After all, the nature of computing makes it easy to find yourself with access to someone else's computer account - or even be in a situation where you can make off with someone's

work or files. Ethical work practices must be ingrained right from basic schooling.

Therefore, in addition to their tech-focused duties, cyber pros will likely play some role in educating the public-at-large on basic computing ethics. A cyber security analyst hired in a company, for instance, may very well find him or herself not only working to solidify the business' security infrastructure, but also hosting semi-regular meetings on cyber best ethical practices, such as not opening a colleague's email account. These types of behaviours make cyber problems much worse than they need to be, and they should be stopped.

Cyber Experts in a Futuristic World

One big reason so many companies are hit by cyber-attacks these days, is, because they're simply not prepared to handle any kind of intrusion. The growth of cyber professionals offers businesses the chance to prepare for the same. This is something they desperately require. In the coming years, as we encourage more students to graduate from cyber security programs and enter the workforce as newly-minted cyber fighters, we will help fill a much-needed gap between hacker efforts and business fortification.

As Lee Vorthman, an industry CTO, pointed out, "These people aren't jumping from job to job looking for salary bumps and signing bonuses. Many of them want to work for federal agencies and most of them tend to stick with employers for the long term. For companies, that means they better get them early or risk not getting them at all."

With the push toward rolling out more qualified cyber defenders, it's nice to imagine a future where there's a lot more expertise as far as virtual threat defence is concerned. This, however, will not deter hackers from their criminal work. As much as young students are learning about computing security, hackers are learning all the time as well. What this means is that when students enter the cyber workforce, they'll have their work cut out for them. ■



CYBER SECURITY – EVERYONE’S RESPONSIBILITY

Lt Gen V. M. Patil AVSM, PVSM (Retd)
Vice Chairman
Centre for Knowledge Sovereignty



A laissez-faire attitude toward cybersecurity is like a bad stomach bug - it only takes one person to infect the masses, then everyone suffers. If a cybersecurity program isn't supported by ongoing technology & cyber research, operations, implementation, & finance, vulnerability to bugs and attacks will eat away at safety, credibility & reputation of the people, organizations & government. Cybersecurity is a problem that every level in an organization faces, one that goes well beyond the purview of a Chief Information Security Officer. Leadership and all members in every team must be committed, and that commitment must radiate throughout every level of every department.

Companies and governments are quickly realizing that having information—especially sensitive people information—makes them a target. As daily headlines show, these attacks are not only growing, but have become more severe, putting people at risk and ruining not only reputations, but also jeopardising security of organizations and countries alike. What many often forget is that attackers are usually not targeting your organization's technology. They're targeting your people through well-designed phishing emails that increasingly look like normal communication. Statistics show that there is a new phishing attack every 30 seconds across the globe.

Cyber security is a vast subject today. It is like a black hole. No one knows what knowledge and how much of it to harness. Given that, it becomes everyone's responsibility and a mandate for personal safety too.

Instilling Responsibility In Everyone

Everyone in organizations, government, or educational institutions need to know their role in protecting intellectual property, information & data. They must be competent at execution in times of crisis and before disaster strikes. Regular communications about cybersecurity policies and procedures are required to align with and support national cybersecurity program and its execution.

When leaders spell out the security priorities, they should discuss the value of information, data and intellectual property to the country and the need to safeguard it.

Sadly, we do not hear many public leaders even talk about data and information security.

A few organizations and people must be held accountable for protection of data and breach, if any. Punitive actions must be immediate and strict. It becomes a lesson for all those who have a lax attitude towards cyber security.

10 Things To Do Right Now

Putting into place a holistic approach to combating cyber-attacks might feel overwhelming when disruptions are happening simultaneously on many different fronts. Nevertheless, cybersecurity has to be a core security priority and it has to be everybody's concern in today's organizations & governments. Here are 10 things you can do right now to make that happen:

1. Cyber security policy must be specific and included in the overall national security policy. Similarly, integrate cybersecurity into the talent strategy and create a Chief Information Security Officer (CISO) role for your organization.
2. Clearly define cybersecurity responsibilities in your government departments and in corporate organizations.
3. Put cybersecurity at the forefront of all strategy - business, financial, political, social & defence. It can't be viewed only as a technology problem.
4. Ensure that cybersecurity is at the heart of digital innovation and helps rather than hinders innovation.
5. Understand how regulation impacts your global business and work with the regulators as they also want strong sectors.
6. Risk-rate all your key assets and determine a protection approach for each one, with a focus on the "crown jewels."
7. Develop a dynamic and nimble cybersecurity risk management model to enable scaling if there is an escalation of external risk, or a decision to change

the risk appetite profile. That way you can calibrate changes in how you enforce security requirements with other countries and multinational organizations.

8. Integrate compliance into cybersecurity strategy. That way, any money invested in compliance will return value by providing proper defence mechanisms for all.
9. Strengthen resilience by having a clear crisis action and communication plan for when things do go wrong. Crisis and continuity management has to be thought through and practiced with a top down approach, before something goes wrong, so that all people involved clearly understand their role in an incident.
10. Collaborate, collaborate and collaborate. Today's cyber risks threaten the global systems. We need to see more intra-sector solutions, as the failure of one key player could damage the safety & reputation of an entire industry, organization or nation.

The future will clearly be defined by the digital agenda with an increased reliance on technology and connectivity. That will deliver many benefits for economies, trade, businesses, but, it will also present many cyber risks and, by doing so, threaten one of the core foundations of relationships – trust.

To win and maintain the trust of everyone who expect their confidential information to be well protected, even as they demand an expanding range of digitally accessible products and services, companies & countries will have to show their determination to preserve privacy, be available any time and any place and maintain the integrity of data. That involves understanding how cyber risks are evolving, keeping ahead of new regulation, embedding the right cybersecurity strategy and culture within the company, working closely with partners and vendors to secure the entire ecosystem and, crucially, identifying the crown jewels that must not be breached.

The ones that achieve these goals and prove to be reliable and trustworthy guardians of data will not only be the ones that people trust. They will have succeeded in making cybersecurity a market differentiator that will offer stability in a disruptive age and help win more business. Those that cut corners and fail to combat cyber risk will lose trust and people.

In today's growing threat landscape, cybersecurity risk won't wait for you. Don't wait to address risk or put off future cyber planning. Take the time now to open lines of communication & share the importance of the threat. As risk continues to grow, the only way to address this challenge is to understand that it's a shared responsibility. ■



FACING THE CYBER THREAT – 2030

Lt. Gen. Vinod Khandare, AVSM, SM,
DG Defence Intelligence



Cyber threat is part of the overall national security threat we face today. Albeit a large one, without a face. To understand cyber threat, we must understand national security threat. National security threat is viewed in two parts.

External threat – we have identified our immediate adversaries here – Pakistan & China. This threat is being dealt with at different levels and in numerous ways.

Internal threat – terrorism & insurgency.

The contemporary era is characterised by what has been described as the 'information revolution'. This is a phenomenon in which automated processes are activated to marshal and manipulate huge volumes of digitised information as relevant to every field of human endeavours before disseminating that information across a virtually unlimited realm. As human societies across the entire globe as well as the systems governing these become entirely captive to usage of information assets, effective harness of information infrastructure in military engagements too becomes an undeniable obligation.

Warfare has changed over the last few decades. It has become all encompassing. Earlier, the armies of the world fought wars to protect geographical territories. Today, the nature of warfare has changed, evolved. Economic & diplomatic warfare is the softer aspect and can have the desired impact, depending on situations. However, the new concept of warfare, in non-contact warfare is now happening in cyber and information warfare. This warfare is as personalised as it can get. Only because it is on your mobile handset and on your computers.

Cyber warfare is currently an integral component of warfare. Information Operations are an essential part of Cyber Operations. As per United States Department of Defence, it constitutes integrated employment of Electronic Warfare (EW), Computer Net Operations, Military Deception, Psychological Operations and Operational Security. It is done in concert with specified supporting and related capabilities to influence, disrupt, correct or usurp adversary's decision making while protecting our own.

Dealing with Cyber Warfare, the Chinese Way:

China, for the last five years has targeted India in all its cyber espionage & threat activities. The Chinese government has a long-term view of how to build and use this capability. A few points we must note regarding China's cyber warfare capability growth. In February 2014, President Xi Jinping took personal control of cyber policies by creating the Central Cyberspace Affairs Leading Group. At a cybersecurity symposium in April 2016, Xi pledged greater state commitment, both financially and policy-wise, to upping China's cybersecurity capabilities – particularly the identification, recruitment and cultivation of talented individuals. China currently suffers from a severe shortage of cybersecurity professionals. In the past few years, Chinese universities only graduated around 30,000 cybersecurity majors, while the current demand for such professionals has risen above 700,000 – a number projected to top 1.4 million by 2020.

The gap is huge. But the Chinese government does have a plan.

On August 15 2017, the Central Cyberspace Affairs Leading Group and the Chinese Education Ministry issued a joint decree formalizing a set of rules on constructing first-rate cybersecurity schools.

In 10 years' time, the plan seeks to establish four to six world-class cybersecurity schools in Chinese universities as training grounds for cyber-warriors. All resources at these institutions – from teaching staff to incentive structures – will be dedicated solely to fostering top-notch cyber-warriors. Universities must meet certain criteria before they can apply for state support.

This is a systematic approach to building up capabilities. The chosen seven universities for the batch of funding by the state are a combination of civil and military institutes and they are spread all over the country. These two points bring out the comprehensive approach that the Chinese government has applied.

India's Cyber Focus:

We have a long way to go in getting our act together. Our approach cannot be piecemeal in putting cyber strategy as part of national security strategy. An acceptance

of cyber as a form of warfare by itself is critical in this approach. Cyber cannot be viewed as an enabler in traditional defence. It must have a different approach altogether as it is part of non-contact warfare.

Few challenges that the technology space faces in cyber security are the following:

- **Digital Data Threat:** Growing online transactions generate bigger incentives for cybercriminals. Besides, establishments looking to mine data—for instance, customer information, results of product surveys, and generic market information—create treasured intellectual property that is in itself an attractive target.
- **Supply Chain Inter-connection:** The supply chains are increasingly interconnected. Companies are urging vendors and customers to join their networks. This makes a company's security wall thin.
- **Hacking:** This action is penetrating into someone's system in unauthorized fashion to steal or destroy data, which has grown hundred folds in the past few years. The availability of information online makes it easier for even non-technical people to perform hacking.
- **Phishing:** The easiest to execute and can produce the results with very little effort. It is the act of sending out Fake emails, text messages and create websites to look like they're from authentic companies.

We, in India, have paid great attention to building of visible infrastructure in the last few years. Today, what is under threat is our invisible infrastructure. This threat is invisible. However, the effects are very much visible and can cripple us as a country.

Our focus must be multi fold if we hope to bring about a change in our cyber security outlook.

- A comprehensive national security policy that includes cyber security policy as part of the overall security landscape.
- Educating and creating a workforce that will allow for our students to specialise in cyber techniques

and use their expertise in anticipating cyber crimes and fortifying our virtual defences.

- Co-opt Indian private enterprises that will work with the government to indigenously build technology & create sustainable processes in the field of cyber security. There is no dearth of talent in India.
- A public - private partnership in every ministry to draw out, monitor and resolve cyber related issues pertaining to that ministry.
- Most of all, an open approach by the government that this is an issue requiring immediate war footing attention and working towards grassroots and high-level solutions.

Besides the above, the government agencies need to audit their systems and educate their employees to ensure they're complying with data security best practices and make sure that government files and communication are encrypted as a rule. Government should

- Monitor systems regularly and ensure they are running the most updated versions of applications
- Patch vulnerable systems and replace unsupported software
- Comprehensively test security on a regular basis
- Strengthen oversight of IT contractors
- Ensure the cyber security tools are implemented and updated properly
- Improve their responses to cyber incidents and data breaches, and
- Better recruit and retain a qualified cyber security workforce.

When the cyber security threats are gaining dangerous dimensions, India needs to build a secure and resilient cyberspace for citizens, businesses and government to prevent and respond to cyber threats. Government agencies need to be able to defend against known threats, respond to new threats immediately, and quickly recover from cyber incidents, whether they are the result of an accident, natural disaster, or malicious attack. ■



CYBER SECURITY 2030

Vinit Goenka

Member-Governing Council-CRIS, Min of Railways;

Member-IT Taskforce, Ministries of Shipping, Road Transport & Highways

Secretary, Centre for Knowledge Sovereignty



Discipline is the soul of an army. It makes small numbers formidable; procures success to the weak, and esteem to all – George Washington.

This is absolutely true of building any army. One such organization that epitomises “Unity & Discipline” is the National Cadet Corps (NCC). The origin of NCC, which started with the ‘University Corps’ was created under the Indian Defence Act 1917 and its objective was to make up the shortfall in the Indian Army. In living up to its motto, the NCC strives to be and is one of the greatest cohesive forces of the nation, bringing together the youth hailing from different parts of the country and moulding them into united, secular and disciplined citizens of the nation. At present, the NCC covers more than 4500 colleges and 7000 schools across India. The main aim of the training given is:

- Develop in the youth the quality of character, courage and comradeship along with discipline, secular outlook, spirit of adventure, sportsmanship and selfless service.
- Organise, motivate and train the youth in leadership qualities in every sphere of life.
- Inculcate in the youth a greater sense of nationalism and patriotism and get them ready to face any kind of challenge, whether natural or man - made.

One can see the same and more of such characteristics in our gentlemen cadets passing out of our military academies.

Youth is the major factor that determines the overall success rate of the country. An educated, empowered and dedicated youth can drive a nation towards success, while negative forces may disrupt growth and development completely. Organisations like NCC, IMA, NDA, OTA, etc., all work towards inculcating social ethos in the youth of the country and directing them towards a career committed to the security, growth & development of India.

It is imperative to bring this into the cyber space too. The foundation for building a dedicated and committed army of cyber warriors will come when there is a National Cyber Cadet Corps.

In the years to come cyber security as we know today will cease to be any effective. Today we can secure data at rest and that in transition using known encryption and access control protocols. However, by 2030, almost every action of every individual will be a data node. We will either be generating, consuming or transmitting data through everyday tasks with no clear idea of how this

data will be used or misused. Starting from individual upwards to the state, the notion of cyber security as we know will need to evolve with this morphing of data. At the level of a country we would need to evolve a cyber-secure way of life so that we are not mere puppets in the hands of those who would possess the capabilities to manipulate our data.

Short term

In the immediate short term, it is essential that the issue is given top priority. It is necessary that Cyber Warfare, i.e. the act of war committed using networked devices is declared as the same threat as a Nuclear-Biological-Chemical [NBC] for the countries armed forces. There should be specific courses conducted for training our engineers and signals units for tackling such attacks. Similar courses should be conducted in training institutes at MHOW, MILIT, CME & other military training institutes for Young Officers [YOs]. Over a fixed period of time this training should be extended to training institutions like the NDA, INS Shivaji & the IMA to name a few. Once a time bound training is inculcated in the armed forces the same should be extended to the training academies of our police and para military forces.

The Government of India can sign specific MoUs with countries like Israel that are at the forefront of cyber warfare for imparting such trainings. It can conduct joint training exercises with like-minded friendly countries to assess our strengths and weaknesses. While the Ministry of Defence would be tasked for the training of the armed forces, the para military and police forces need to be trained under mandate from the Ministry of Home Affairs.

Medium term

In the medium term it is necessary to institutionalize these efforts. The first and most important aspect of this would be the setting up of a Cyber Defence Academy on the line of the National Defence Academy under the combined command of the armed forces. This would give us a premiere institution that would be the centre point of all training and research around not just cyber warfare but also emerging technologies in this domain. While it would have the academic rigor of the IITs it would also need the practical capabilities that military training institutions have known to possess in our country.

This institutionalization will allow for continuous creation of highly trained and efficient cyber cadets who would go on to become leader of a force that will most probably be fighting more cyber wars than terrestrial wars in the future. The standards set by this institute will need to be replicated across para military and police training institutes. Alumni of this institute should be periodically deputed to other organizations like Railways and other critical infrastructure agencies of the government to help design their cyber defence systems and ensure that they are robust and near impenetrable.

Long term

The foundations of long term reforms need to be laid today so that they are given the due time that will be needed for successful implementation. The first intervention needed is to overhaul the National Cyber Security Policy [2013] and ensure that it is more in sync with our long - term goals. It needs to move away from the 'also done' approach as of now to a more 'mandating' approach. Policy interventions need to be clearly defined and sun-set clauses for implementation should be defined with a clear demarcation of penalty for agencies not in compliance with such measure.

The policy should clearly state the need to inculcate a cyber-secure way of life for the future generations. It should mandate the MHRD to make necessary changes in all school and college curriculum so that cyber safety and security practices are made a part of everyday learning. Much like a value - based education approach for social service and environment, this curriculum should stress on the fact that being cyber aware is a pre-requisite for a better future for the individual as well as the society at large.

Stakeholders

Politicians

For their direct connect and accountability to the people of India, politicians stand at a very crucial juncture of driving a particular narrative in the country. It is necessary that consensus in built across the aisles of power to make sure that laws and policies that favor a cyber secure India are prioritized in the Parliaments and subsequent legislative bodies.

They should also utilize their decision - making powers as ministers to ensure that good initiatives of one ministry are replicated or supported by another. [As an example: The MoD can expedite land grants for training institutions by utilizing land under its control if the MHRD approaches it with such a request.] Politicians are well known public figures and they need to opine on public platforms about the benefits of the long - term impacts of such policies.

Think Tanks/Academic Research Institutions

These will play an important part in fulfilling the goal of a cyber secure India. Institutions like the IDSA, CLAWS in Delhi and the Defence and Strategic Studies department of the University of Pune as well as IITs, C-DAC and other high end technical research institutions will contribute the initial human resources towards these initiatives. They would also need to work closely with the training institutions set up under this program to make sure that academic rigor continues to be at its best here.

Media

Media, both traditional as well as alternate media will play a crucial role in the dissemination of information and awareness around these goals. It will be the channel through which people are made cyber aware on a sustained basis. The role of media will also include rigorous fact checking to ensure that misinformation and false news do not create an atmosphere of fear and panic among the citizens. In the long term, media channels can also be used as an educative means for running infotainment programs aimed at educating citizens.

Conclusion

The aim of a cyber secure India is noble and achievable, however the start for the same needs to be done immediately. It is of paramount importance that a policy is drafted to codify this process and a well-defined plan of action is put into practice at the earliest. All around the globe, millions of dollars' worth of economic losses is being reported over cyber-attacks, if we do not prepare our present, we might not have a future worth talking about. ■

Rahul Aggarwal
Director - PWC



In 2030, technology will be 13 years old from now. By using technology you can control anything. We hear of Driverless cars, which will gain momentum in coming years, lights in a house being controlled, so this is how technology is changing. Our dependency on technology and IT is very high. You can access information services, transaction services online sitting at home. So if all this is happening, how are we going to manage it? What are the areas as a govt., as a private corporate and as a society we need to address? That's what we need to discuss. But from our perspective, whatever research we have done, most of the countries will always have a critical infrastructure for the financial sector, defence sector, transport sector etc. Every country has defined it. If the critical infrastructure is not available for the society at large we have a major disruption. From the govt. perspective, critical infrastructure always needs to be protected.

WHY SHOULD WE STORE DATA IN INDIA?

Vinit Goenka

Member-Governing Council-CRIS, Min of Railways;

Member-IT Taskforce, Ministries of Shipping, Road Transport & Highways

Secretary, Centre for Knowledge Sovereignty



The exponential growth of data-enabled services in India over the past decade has brought in its wake concerns that occupy a wide spectrum extending from user data theft to data sovereignty concerns arising out of sensitive data residing on data servers based out of geographical boundaries of India. Recent policy papers released on regulating Over the Top (OTT) applications by TRAI and the draft National Encryption Policy by DeITY have opened vibrant public debates around issues of net neutrality and government control over encrypted communications. There is now a general consensus that policies relating to the data ecosystem need to be product agnostic and focus on streamlining processes instead.

In 2010, guidelines were issued to State governments for setting up Data Centers that would act as a mediator and convergence point between open unsecured public domain and sensitive government environment. These SDCs aimed at enabling various State departments to host their services/applications on a common infrastructure leading to ease of integration and efficient management while ensuring that computing resources and the supporting connectivity infrastructure is adequately and optimally used.

The guidelines allowed for outsourcing of the SDCs to private/public sector service providers for technical and administrative assistance. The intended outcome was to strengthen the state IT apparatus to administer and manage data centers while creating an enabling environment for private players to setup their own data centers. This objective has not been achieved as all the 31 data centers established under this plan are operated and audited by private service providers, while the investment for them came from the Rs. 1623.20 crores allocated for this project over a period of 5 years. It would now be appropriate to evaluate this project and subsume it under the ambit of a National policy.

Market based unregulated model

In the absence of a comprehensive policy guiding establishment of the core data infrastructure, private sector service providers have tried to fill in the vacuum with

colocation facilities to serve short term requirements than long term objectives. Almost all of these data centers are crowded in cities of Mumbai, Delhi & Chennai that have provided a fairly consistent supply of electricity and high-speed fiber optic connectivity, the backbone of the data infrastructure.

Data centers established under this model have not had any guidelines in terms of adherence to environmental & energy standards. Standards of reliability, availability, scalability, and serviceability, and provisions for backup, redundancy, survivability and disaster management are not audited by competent authority. It is imperative that such a competent authority is established to facilitate setting up, formulate policies and audit for compliance of private data center operators in the country.

Digital Infrastructure under Digital India

The recently announced program incorporates the aim to provide Digital Infrastructure as a utility to every citizen. Ambitious as it may sound, the program recognizes the need to provide high speed internet as core service to citizens. It draws out a road map to attain this through special missions focused on expansion of fiber optic connectivity in rural and urban areas. It also identifies the need to extend mobile coverage to the yet uncovered regions that are primarily rural in nature. The program is an exercise in consolidation aimed at bringing all existing schemes under a common umbrella.

Digital India, however, puts the entire burden of this expansion on Government funded efforts and does not look to tap into contribution of the private sector towards attaining its objectives specific to Broadband Highways and Public Internet Access Program. Further, multiple implementation agencies have overlapping mandates, while the Broadband for All (Rural) is under the Department of Telecommunications (DoT), the National Rural Internet Mission is under the Department of Electronics and Information Technology (DEITY). With close to 50 thousand crore rupees allocated for the programs focusing on data infrastructure, the need for a single agency to take over the implementation of these programs has become apparent.

Rationale for a National Data Infrastructure Policy (N-DIP)

The National Data Infrastructure Policy (N-DIP) should aim to address the overlapping issues in an data ecosystem. Existing models are stop-gap solutions and cater only to specific components of the ecosystem instead of being an overarching framework that guides the growth of the ecosystem.

User Data Security

End user data is the foundation on which a data ecosystem is built upon. Putting in place policy and legal safeguards to sustain user trust will be essential for long term stability of this ecosystem. The N-DIP should have stringent data security and privacy guidelines that are drawn from global standards. Further, the compliance to such standards would be routinely audited and posted in public domain for further scrutiny.

Data Intermediary Concerns

Data Intermediaries are *body corporates* that aid in the transmission, storage, and third party access of end user data. These intermediaries comprise of the entire spectrum of service providers including telecom operators, ISPs, cloud based services and Over the Top (OTT) applications. They form the back bone of the physical infrastructure of the data ecosystem. The N-DIP should address the concerns raised by them and assign them the role of "Collaborators" in the data ecosystem. The N-DIP should also provide a single window facilitation forum to

enable collaborators to scale up the data infrastructure with least procedural bottlenecks.

Lawful Interception

There is an urgent need to put in place an accountable system where legitimate requests for interception would be vetted, documented and realized in public domain at regular intervals. This will prevent incidences of blank surveillance that have long being used for political arm twisting than it's intended purpose. This will also make it easier for the intermediaries to comply with genuine requests of interception and end user information. The N-DIP should make provisions for a comprehensive overhaul of the legal interception provisions in the Telegraph Act (1885) and Information Technology (Amendment) Act (2008).

Data Sovereignty

The demand for data centers within geographical boundaries of India is based on two reasons. The first is that Indian IT laws are not applicable to data stored outside India, so investigating agencies often face procedural delays if access to data is sought for prosecution purposes. The other reason is the possibility of misuse of such data by the country hosting it. The N-DIP should have clear guidelines on the expectations of "Sovereign Rights" over Indian data hosted abroad. The policy should also make legal safeguards for data hosted within India to be protected from acts of surveillance, with due exceptions for financial frauds, acts of terrorism and crimes against humanity. ■



LOOSE LIPS SINK SHIPS – WHY PRUDENCE MATTERS THE MOST FOR CYBERSECURITY.

Rear Admiral Sudardhan Y Shrikhande, AVSM (Retd)



Most discussions on cyber security encompassing the protection of governments, businesses, institutions as well as individuals from cyber attack focus on the technical means to do so. This is natural as well as right because the cyber-world is essentially enabled by technological advances in IT as well as in communications in ways that can confound us almost as much as they enable us. Many of the protective/defensive aspects of cyber security also will continue to rely on technology as an instrument. Likewise, cyber-attacks would also require harnessing technology in a way that harms us.

People are the Foundation of Cyber-Security

Nonetheless, my submission in this article is that human beings are the essential foundation as well as instrument of cyber security. Technology is only one major instrument. To that purpose, it is absolutely right that the Centre for Knowledge Sovereignty has chosen a theme “**Cyber Security: Citizen of 2030.**”

It is for that reason that I have used the title “**Loose Lips Sink Ships: Why Prudence Matters Most for Cyber Security.**” From my youngest days in the Navy, we were familiar with this slogan which was pasted in a few places in ships and in barracks. But, the catchy message is really applicable in almost all matters and spans not only official lives but, equally, our own personal well-being and safety.

Whither Prudence?

The unsaid thought of “Loose lips sink ships” is the need for **prudence. This is my first and overarching proposition.** What should we understand beyond the obvious meaning of the word? The advice given to us as young cadets, midshipmen or officers, and in turn one that we passed on to our own juniors, was that prudence in an individual meant that you were cautious about what you spoke in the context of where you spoke. The circum-

spection went beyond discussing your own ship’s sailing or fleet exercise programmes. It went beyond discussing your ship’s capabilities in a place where the wrong ears might be able to eavesdrop. It went beyond the need to be very careful about what you said on the phone because it was drilled in that phone conversations could be intercepted and that even very secure lines could be broken into and that cracking a cipher system was a matter of **when**, not **if**. Rather, it encompassed the need to build an attitude of caution in ensuring security of information that had to become second nature.

One must, of course, consider the environment prevailing before a world of computers; of smart phones; of e-mail and the internet; about the easy media for exchange of information; or of the abundance of information out there. We must consider the ease with which we can make our instant opinion on the most profound or of the most mundane of circumstances known to hundreds or lakhs of viewers through tweets, instagrams, facebook posts, whatsapp etc, etc.

Difficulties in Being Prudent?

All this would seem obvious, but what is not obvious is the very ease and ubiquity of instruments in our hands that makes us throw caution to the winds. **Why is it so difficult to be prudent?** Why is it that children in school, using e-mail and smart phones are willing to share things about themselves, their feelings, their pictures etc with large groups but cannot always confide in their own near and dear ones within physical distance? Why is it that larger groups of college friends, alumni associates, military academy batch mates, etc drop their guard in the cyber world despite all the prudence observed in earlier decades?

I am neither a psychologist nor a sociologist to provide deep explanations. However, it seems to me that prudence becomes a casualty for several reasons. One could be that there is a perception of friendships that can be

measured in the number of friends rather than the depth of friendships. It is quite easy to be trapped in the number of “followers” or “friends” and to figure out ways in which these could increase. How could young people, older people in positions of authority, even national leaders not be occasionally swayed by their seeming worth measured in numbers of followers? But, in the cyber-world, is leadership or followership a very useful measure anyway? How many virtual “friends” are friends; how many virtual, often faceless “followers” will actually follow anything we have to say and even lesser, what we may ask them to do? How many “likes” to a post does it take to make a young school-going child’s day? When does a decline from a 100 “likes” to merely 40 “likes” after a few days lead to onset of depression? What makes slightly sad or depressed young people sign on to sinister games like “Blue Whale.” What is meant, in our emotionally isolated “worlds” for young people to have a “whale” of a time?

Emphasising Prudence

These issues are raised here, perhaps in an audience who are specialists in cyber-issues and are not among the “*aam aadmi/ aurat/ baccha*” (common man/ woman/ child) who are less likely to think of the potholes, breakers, obstacles, traps and horrible accident spots on the cyber highway. But, these people are citizens today and will be **Citizens 2030. How is the prudence of “Loose lips sink ships” to be drilled into them so that it becomes second nature?**

Begin Early, Begin in School, Co-opt Parents

A few years ago, we thought of having meaningful workshops and presentations to the boys and girls of naval schools in Kochi and elsewhere in the Southern Naval Command. In asking relevant people to convey to them the problems on the cyber- highway, I felt myself at some disadvantage. I had easily internalized the meaning of “loose lips sink ships” in the use I made of e-mail and the internet. I knew someone could watch me, and therefore, I needed to watch what I wrote, read, surfed and studied. Before that job as Chief of Staff, I had been ACNS Intelligence in Delhi for the Navy and was aware of cyber- security, vulnerability and counter-measures to an extent greater than many others. Yet, I did not have a smart phone (2010-2012), nor a facebook account, nor any personal experience of how these things work, what were their safe uses and what was their utility. In my mind, the problems seemed to overshadow their utility and the inevitability of their increased usage. But, the workshops were popular and received what we hoped was serious consideration by school children. **The underlying theme was prudence.** These interactions were then repeated with parents because they needed to understand more. Just like what our seniors and those posters in ships and barracks did for us, **the parents needed to educate their children in the virtue of prudence.** It is difficult to say how well these messages were absorbed, how long they lasted or how well they might serve in keeping children safe in their own future? The effort, in my view needed to be made and repeated periodically. **In the very centre of this initiative by the CKS, very rightly, are experienced principals of schools.**

Internalising Prudence, Count to Ten, Before “Send”

It is my belief that **once prudence is internalized, once it becomes an attitude** it matters little if the medium is

an old phone where you rotated a dial with a finger in the notch or a “send” symbol on a smart device or keyboard with virtually instant connectivity. **Here I would like to suggest a second proposition.** The old phone, literally enabled us to count to ten if we were dialing a five or six digit number. It gave us time to remind ourselves, even if subconsciously, that prudence was necessary in what we were going to say on the phone. Similarly, the chance that an incoming phone call was from someone entirely new, or an imposter was lesser than today. Besides, the caller was also more likely to be prudent himself or herself. And, we must remember, of course, that calls cost money if on a personal phone line. **Fiscal “prudence” was an important constituent of conversational prudence.** Don’t older readers remember how prudently they must have composed pictures in their minds before clicking on older, non-digital cameras. Digital photography is cheaper, virtually free. There is imprudence in taking photos as well as in posting them. **Financially there may be no price to be paid, but isn’t there often a high emotional price to be paid for imprudence?**

Unsafe at any Speed? Not Quite!

The few telephones that existed in a military work place often had a warning that fundamentally meant “loose lips sink ships”. Today, the send button works instantly and once pressed, one often realizes how “edit- unfriendly” that button is. The speed at which things happen simply increase the chances of trouble, of accidents. This is in no way different when we drive at an unsafe speed. We have less time to react; others have less time in which to avoid us; and the kinetic damage is greater for all than at a lower speed.

Increasing Quantity, Declining Quality

Working backwards, there are other factors leading to the **third proposition that as a society, and as individuals the quantity of communications have led to a decline in quality.** Many people form instant opinions, offer instant judgement or seek instant answers or invite instant opinions and judgements. There is often a lack of quality in forming them, but rarely a lack of quantity of such views being aired. Let us look dispassionately at what are real gains from say, chat groups based on past associations like school, college, or university groups? The sheer quantity of traffic can lead to hurt feelings, sub-groupism, name-calling, offence caused via conversations or sometimes even via silences! In a few months of such associations what do we really gain? Does the bond grow stronger merely because it is now easier to touch base or organize get-togethers? Are we intellectually or emotionally better off? This is not to deny some of the advantages, some of the happiness of connecting with one’s past, but to reiterate that there inevitably would be problems of quality because of quantity. There are chat groups based on narrower professional and scholarly interests. These can work well if the numbers are not large and everyone displays the maturity to stick to the purpose of coming together. In such cases too, there could be a problem of quantity trumping quality.

Prudent Individuals Beget a Prudent Society

The above three broad propositions could be merged into the **fourth and final proposition. Societies and citizens that educate and train themselves to be prudent in decades ahead could be better poised to protect themselves collectively as a society. Citizens have, first, to learn to better protect themselves as individuals.** Of course, this is going to be exceedingly difficult. I must add

that I do not have too much of an idea of how this is to be done. Cyber-insecurity could be a problem of governance itself, just as physical insecurity or a perception that terrorist attacks could occur anywhere and everywhere.

Prudence at the National- Strategic Level

How do large nations and institutions train and educate themselves to be prudent users of IT as it exists today and as it would exist tomorrow and the day after? At a grand-strategic level, see how China is preparing for a more secure cyber-future with its own satellites, its own versions of GPS, its own softwares, its own safeguards, its own cyber-companies, national as well as multi-national. Match this with their own restrictive practices of who and what they allow for their own citizenry. While not advocating unfettered restrictive practices, cyber-security measures may require us to examine this dispassionately. **Link all this with China's growing capabilities to go on the cyber-offensive if required.** One nation's cyber-defence would be closely and dynamically dependent on other nations' capabilities for cyber-attacks.

Prudence at the Institutional Level

At the institutional level, various organizations approach this with different degrees of seriousness. IT and communication are spreading information in institutions far more rapidly than before. Nonetheless, implementation follows its own pace. One has heard that ministries have officials sometimes exchanging agenda points and notices for meetings on media like whatsapp. While travelling, it is often the one medium that is used. But, regardless of encryption, how do we know that usage would not hurt us in some way later? How can we accept assurances? In any case, speed of information and actions thereafter are not necessarily linked. The armed forces have strict policies and fairly stringent protocols for the way in which IT and communications are done and monitored. Yet, vulnerabilities remain but are always under assessment. **The guard cannot be let down.**

AS India becomes a greater industrial, scientific and economic power, corporations and banks, research bodies and even customers would need to observe protocols carefully. The US is worried about what it may have lost already and is losing to others' cyber-espionage. On our part, it seems that there is only some recognition of this. Cynics feel that we have nothing much that can be stolen (they are wrong to think this way); some feel that

safeguards are generally adequate. Others feel that the risks can be coped with and that expenses on cyber-security are sometimes not justifiable. **Whatever be the thinking, we simply cannot afford to be imprudent.** Experts engaged in corporate and institutional cyber-security perhaps need to be more vocal and more candid about risk assessments and solutions. Within their own organizations, prudence at individual levels needs emphasis as do ethics. Computers do not leak or steal data, people do.

Savdhaan Aur Satark Bharat? (Watchful and Alert India)

As far as Citizen 2030 goes, I suggest that a "*Savdhaan aur Satark Bharat*" type of campaign, if I may call it so, is required. If campaigns for social change, against smoking, against *gutka*, against gender-selection, or against dowry have succeeded in some measure, why can't campaigns against cyber-threats be justifiable? How, when and in what measure should it be conducted? How are returns on investment to be measured? Can an argument be made that this education violates fundamental freedoms? By that measure, isn't a smoking ban in public places violative of the right to destroy one's health if one feels like it? **How does "*Savdhaan aur Satark Bharat*" inculcate prudence as a national virtue?**

Begin Making a Savdhaan & Satark Citizen in Schools

Finally, how are schools to educate their students about the perils as well as the correct usage of the power in their palms that connects them to the wider cyber world? How are parents and elders to be co-opted so that basic security is ensured; so that perilous games like "Blue Whale" or those that may appear in future can be kept at bay? (The cyber world alone is not to be balmed. Such devious, suicidal events have occurred in other ways. For example, in the 1978 Jonestown, Guyana, mass suicide that took over 900 lives.) Those young citizens who have entered primary school this year would be about 21-22 years in 2030. How to prepare them for cyber-opportunities and cyber-threats? How do we inculcate prudence as a childhood virtue?

The "ship-of-state" is as vulnerable to cyber-security threats as are individual citizens of all ages. Increased prudence could be the key so that "no ship sinks because of loose lips. " It is useful to think of each citizen as a shipmate in this ship-of-state. More can be done, but not less. ■

Dr. Savita Kakar
Chief Scientist - DRDO



Indigenization is one solution we have in hand and I think DRDO and other organizations are taking steps towards it. But for doing that the private industry, DRDO and academia have to come together because what I found that there is a lot of knowledge but they are in the form of compartments. So we have to come together to do work of such magnitude. It is very easy to say that we want to indigenize things but it is very difficult to accept. Generally we are more overwhelmed by imported stuff. Whatever products we are indigenizing generally when it goes to user, instead of accepting and giving the suggestions, users start comparing with the imported stuff. People have to change this mentality and they need to start accepting things. We have suddenly started doing indigenization and we might not be able to deliver the products of imported level. So, definitely some motivation is needed to accept these things.

INDIA NEEDS A NATIONAL CYBER STRATEGY

Dr S D Pradhan
(Former Dy. National Security Advisor and Chairman Joint Intelligence Committee)



Cyber space has witnessed rapid and dramatic developments in the last two and a half decades. Today the internet has become an easy to use and inexpensive medium for the government, private sector and individuals with advances in microprocessor communication especially in the mobile, storage and software technologies for communication. The World Wide Web and social media touch every aspect of human lives. While the World Wide Web began only in 1991, today more than 3.58 billion people are on line with about 5.5 billion internet connected devices. More are set to join in the coming period.

Internet is revolutionising our society by providing a fast and easy way to connect people, provide access to data and knowledge banks and is an important source to drive economic growth. Internet has become increasingly central to our economy and social relations as also in international relations. The revolution in the information technology, processes and internet connected computers are altering our way of living- how we communicate, perform banking transactions, make purchases and make use of this in diplomacy and wars. While the cyber world provides a number of facilities, it also brings with it a host of problems for security of communications, data and infrastructure.

Today cyber space occupies a key position in national security. It is an interactive domain made up of digital networks that is used to store, analyse, modify and communicate information. Our dependence on cyber space has immensely increased in all fields –economic, military, diplomatic, social interactions, transportation, banking transactions, education and science & technology. The cyber-attacks can disable official websites and networks, disrupt or disable essential services, steal or alter classified data, can influence elections advantageous to the users through disinformation and cripple financial and military systems i.e. they can affect all components of national power. Cyber threats are assuming dangerous dimensions that include cyber-crime, spreading disinformation, cyber espionage, cyber terrorism and the cyber warfare. In an effort to address vulnerabilities and related issues, stakeholders across the national security system are actively seeking to develop legal and policy solutions to protect the national assets while limiting regulation and intrusion into what is largely a privately owned and operated domain.

In cyber world, threats come from five different sources. First, the network hackers who exploit the known

vulnerabilities for fun or making political statements. Second, the hackers who are motivated by economic gains either individually or as part of organised crimes. Third, foreign intelligence agencies/armed forces or non-state actors targeting business as part of industrial espionage to achieve competitive advantage or government organisations including defence for intelligence gathering. Fourth, disgruntled employees like Snowden could also harm the nation by leaking confidential information. And the fifth, the nation states now openly combine the use of cyber operations in warfare, placing them at the same level as land, air and sea operations.

While there is no accepted definition of cyber warfare, generally speaking it is a form of information warfare. It is Internet-based conflict involving attacks on information and information network. In view of the centrality of cyber security in national security sphere, a number of countries are setting up cyber commands. The US has declared cyber space to be the fifth dimension of warfare after land, air, sea and airspace. The US reserves the right to take all actions, including military strikes in response to cyber-attacks against it. China places the cyber operations as an essential element to maintain deterrence and equates it with nuclear weapons. Some other nations too have developed similar concepts. While deterrence in this field is a highly debated issue due to the problem of attribution, those countries which are building cyber command perceive that this may work at least against the known adversaries.

India's concerns of cyber space are manifold- use of social media by anti-national elements to foment communal tension or disharmony, economic crimes, attacks on critical information infrastructures, use by terrorists as a tool to radicalise youth and to conduct operations, use by some countries to gain competitive advantage in global trade and as an effective instrument for cyber warfare programmes of hostile states and non-state actors. While in our neighbourhood China and Pakistan are enhancing their capacities to face new challenges and capabilities for cyber warfare (given close Sino-Pak military relations, there is a distinct possibility of China sharing its cyber capabilities with Pakistan), US, Russia, UK and North Korea already have such capabilities.

They have integrated cyber warfare with general warfare in which the cyber operations play a decisive role. The cyber commands and national cyber strategies are meant to deny the use of cyber space by their adversaries,

confuse their decision making loops and destroy their critical infrastructure including military command and control networks in wars. A subtext of the national cyber strategies is to use the cyber power to deter their adversaries from pursuing a particular course of action. This blurs the distinction between war and peace for cyber operations which includes psychological campaigns, Distributed Denial of Services (DDOS), attacks on critical infrastructures, espionage both for military and economic purposes and destruction of the military command and control systems of adversaries during wars. While a US report pointed out that more than 30 nations were building cyber warfare capabilities, another report suggests that about 140 nations are working on to produce cyber weapons. These are indeed scary reports which suggest that we should be prepared to face the challenges emanating from different levels of cyber threats.

In view of the above, India needs to be prepared to face the strategic use of cyber operations by others. The reality today is that India faces four kinds of threats in cyber space-cyber-crime, cyber espionage, cyber terrorism and cyber warfare. What is alarming that broadly speaking they are all parts of a larger warfare programme of Pakistan and Pak linkages with China makes our security challenges much more serious than can be imagined.

However before formulating a national cyber-strategy, the special characteristics of cyber warfare must be kept in our calculus. First, since much of the cyber space is owned and operated by private sector, controlling the cyber space becomes complex. Second, attribution remains a problem and often it becomes extremely difficult to know the source of attacks. Adversaries can use proxies. The deterrence can work only against the known enemies. Third, early warnings like in physical world, are not possible in cyber space. One can at the best know when the system is under attack. Usually this is learnt after the attacks. All these factors add up to one conclusion: in cyberspace, offence is significantly easier than defence. And this aspect must be given importance.

The cyber-attacks can take various routes, which can be used simultaneously by adversaries. First, various malwares (commonly refers to software codes like malicious viruses, worms and Trojan horses) can be placed in our system by adversaries. Malware is simply defined as a code with malicious intent that typically steals data or destroys something on the computer. Malware is most often introduced into a system through email attachments, software downloads or operating system vulnerabilities to destroy critical data or infrastructure. It can also be implanted through moles. The insertion of Stuxnet virus in the Iranian Nuclear Facility by Israel and US using a mole to destroy the Iranian nuclear programme is an example of such an act. Phishing attacks, which are quite common, are sent via email and ask users to click on a link and enter their personal data. Phishing emails have become much more sophisticated in recent years, making it difficult for some people to discern a legitimate request for information from a false one.

Second, the imported equipment used by our information infrastructures, agencies and companies could have implants that can provide information to other countries, from where the equipment are imported, without the knowledge of the users. Instead of hacking, the adversaries can use or 'own' the companies supplying devices and export them after implanting backdoor surveillance tools to steal sensitive information. The US, China and Russia are reported to be doing this. In 2012 the US Congressional Report warned that Chinese telecommunications

companies Huawei and ZTE posed a "threat to US national security interests" and could sell companies equipment with backdoor surveillance tools to give the Chinese government control over American communications networks. China also purchases companies dealing with computer network with this intention. The Chinese company Lenovo, which bought IBM' PC business in 2004, was reported to be shipping laptops with 'superfish' malware which undermines basic security protocols. Similarly, the US is using equipment to attack its targets. Glenn Greenwald, who broke the story of Snowden, in his book captioned "No Place to Hide" brought out that routers built by the Cisco (and perhaps by other companies too) are routinely intercepted without Cisco's knowledge by the National Security Agency (NSA) of US. The NSA implants backdoor surveillance tools, repackages the devices with a factory seal and sends them on. Snowden's revelations confirmed this. The Russian hackers are reported to have used Kaspersky software to create vulnerability in the US National Security Agency's system to collect classified information.

Third, the attack can take the shape of the Distributed Denial of Service (DDOS) attacks. In the DDOS attacks a number of computers are used to attack target computers or network for a pre-determined period causing complete paralysis of the system. The attack on Estonian network in 2007 is considered the biggest DDOS attack so far. In December 2015, Ukraine faced a similar attack.

Fourth, attacks can be launched through various social media platforms to manipulate public opinion for political purposes. Information is so heavily bombarded with aggregated impressions through social media platforms that it becomes almost impossible not to be influenced by the constant flow of impressions being made with images, headlines and fake videos. The implications of that are rather staggering. A vested interest could sway an election at the local, state or federal level without anyone really noticing and paradoxically by using the same technologies that people believe would provide them with better insight. These social media platforms are also used as a powerful tool for psychological campaign by hostile states and social groups. In India, all the incidents of communal violence had witnessed increased circulation of doctored social media messages and videos aimed at inciting people. These platforms are also being effectively used for radicalisation of youth by terrorist groups and are responsible for increased number of lone-wolf incidents of terrorist attacks.

Fifth, cyber-attacks can take the shape of full-fledged cyber war separately or supplement an armed conflict in which they can play a decisive role. The cyber-attacks are one of the main elements of the "Hybrid War" which includes conventional, irregular and cyber operations. As mentioned earlier, several nations have now evolved cyber warfare strategies as parts of their national security to secure their information networks. In times of conflict, an adversary can exploit our vulnerabilities in cyber space and paralyse the critical civil and military networks.

A study of the national cyber strategies of US, UK, China, Russia and Israel points out certain common aspects. There are three aspects that are common in the strategies of the above mentioned countries. First, the cyber security is perceived as a part of national security and all are accepting the possibilities of a cyber-war. The countries are taking a number of steps like enhancing capabilities to defend the critical infrastructure, information data and network; enhancing capabilities to respond to the cyber-attacks in real time; developing abilities to identify the

sources of attacks; integrating it with armed forces operations; preparing for both defensive and offensive operations; and having an empowered body (involving top policy makers) to prioritise operations and ensuring that various stakeholders act as one force. Second is the use of cyber capabilities to deter the adversaries. Cyber operations are not merely seen as supplementing military operations but are also used as a deterrent like the nuclear and missile power. And third, there is a greater thrust on developing domestic capabilities to produce necessary IT products.

The cyber warfare is a new development and is drastically changing the nature of warfare. Hence its key dimensions merit attention. In cyber warfare there are no rules and no regulations and it has a reach to practically all fields. Cyber warfare is an ongoing war that is never declared and is not bound by any law. The issue of attribution remains a problem. The use of cyber space by hostile elements is not only increasing rapidly but their attacks are assuming new dimensions. They are becoming more diverse, becoming better at what they do and becoming more adept at using virtual attacks to inflict real damage. The Artificial Intelligence procedures can manipulate networks and devices in unthinkable ways. They engage very large elements at the very same time and correct the nature of the attack by self-learning depending on the method of the defence it faces.

In essence India needs an overarching national cyber strategy to prioritise the objectives in an evolving environment, achieve synergy between different stakeholders so they work in coordination to deal with different threats both during war and peace. The national cyber strategy should provide guidance to all to achieve the long term and overall objective of securing cyber space

(protection against multiple intrusions) and it should be a part of national security strategy. The focus should be on enhancing cyber power, which is an essential component of national power.

India in future will face increasingly sophisticated and strategically “destructive” cyber threats as compared to the “disruptive” attacks in the Indian cyberspace that are currently being faced by the nation. India urgently needs to develop policies and capabilities in this ‘Fifth’ domain of war. These cannot wait and must be taken up on top most priority in a “Mission Mode” by the Services. The situation and threats to India are unique and hence there is an urgency to develop an indigenous solution in consonance with the national cyber strategy.

The element of deterrence should be an essential component of the national cyber strategy as this can keep under check the known adversaries up to some extent. All countries despite accepting that attribution remains a problem, feel that this can deter the known adversaries. The deterrence should be credible and should reflect India’s resolve to use all instruments to cause “massive and unacceptable damage” to the attackers. For this, there is a need for a special cyber command like that of China. c) A high powered organisation to take decisions to launch operations for the protection of national critical infrastructure in changing security environment, task different entities and ensure compliance of directions is needed. It is suggested that India should create a National Cyber Authority under the PM. The need for having a national cyber strategy can hardly be underestimated in the present circumstances when every war, battle or skirmish has a substantial element of cyber operations. ■



SECURITY INCLUDING CYBER SECURITY FOR A LARGE SERVICE ORGANIZATION.

Dr. B V L Narayana
Executive Director
CRIS, Indian Railways



The Indian Railways represents a pan India spread, large organization which deals with the core element of public transportation including goods. This transportation extends to every corner of the Indian sub-continent. The growth in the network of Indian Railways is enabling it to not only connect every district but also increase its level of connections by improving the number of links into the district thus making it highly intense network of transportation assets. Further the utilization of these assets is so intense because of the number of services which are run to cater to rising transport demand of Indian economy. This makes it the central portion of the logistic framework which drives the Indian economy. Of late, the highly integrated production system has been digitized so that today Indian Railways is an IT concentric transportation giant.

The implications of these factors is that Indian Railways:

1. Is a critical driver of the economy and any disruption in its network leading to dislocation of rail services can lead to wide spread economic loss and huge impact on citizens life.
2. Given the large scale digitization of its system, large volumes of legally permitted users are at any time accessing the system. This requires a distinction between legal and devious users of the system.
3. Therefore security on Indian Railways covers security of assets and intrinsically interlinked to cyber security. Any breach in the IT Systems of Indian Railways can cause serious dislocation of the services leading to over all security risks.

Given this very integrated and inter-linked requirement of security and cyber security on the Indian Railways, the security can be defined as a function of vigilance and trust. Vigilance is the ability of the members of the organization

and the organs of the state to perceive, identify and address risks leading to dislocation of services. This is an outcome of the capabilities within the Railways and the Govt. security agencies to collect intelligence from the country wide contents and use it to neutralize any threats before it can cause significant dis-location and damage.

Security as a function of trust which is an outcome of the strength of the psychological contract between citizens, the state and Indian Railways.

The general satisfaction derived from the services delivered by Indian Railways on a consistent basis strengthen this psychological contract. It is this unwritten commitment of the citizen towards Indian Railways which ensures desirable behavior leading to:-

- (a) Proper usage of the assets of Railways.
- (b) Extra-ordinary citizenship behavior in times of crises and accidents.
- (c) Vigilance against disruptive actions of deviant citizens who may indulge in attempts to dislocate Railway services.

The combination of vigilance and trust feed and re-enforce each other. Increased citizenship trust facilitate lower cost of vigilance while effective vigilance re-enforces citizens desire to be part of intelligence gathering and network.

The conceptual basis for the above system is based on the core concept of organization, organizations and its members have an unwritten contract (psychological contact) implicitly agreed to grow, sustain and protect it. A state is also like an organization where the citizens are its members. They actually empower the state to deliver services for their economic activities while they in turn commit the support to state in maintaining such services. Therefore, over time the society re-presented by the citizens develops ethics which facilitates security of the state and which are passed on from generation to generation.

In light of this model governance, then becomes an integrated function of the vigilance of the Govt. and the ethics of the citizens. This model is also at the core of the security of any running system, be it manual or IT based. Any break in these two integrated concepts leads to disproportionate increase in the cost of delivering vigilance or ensuring adequate citizen support.

The Railways by virtue of the properties given in the above Para face a difficult task in maintaining constant vigilance. It essentially needs a combination of citizen based incident reporting and citizen based vigilante groups to control damage from dislocations of the system. Since the Railways are heavily digitized and are using mobile based systems, Two suggestions are given for enhancing security including cyber security for Railway services. They are:-

1. A mobile app. based incident reporting mechanism which is GPS linked to enable identification of location of potential disruption.

2. Creation of a GPS based signaling mechanism which is interlinked with the mobile ticketing and other services apps which can indicate the geographical location of a potential cyber security threat.

These two suggestions are aimed at addressing the need for identifying which citizens are entering and using the system and who are causing damage. It also distinguishes between people who are legal users and those who are deviant users. The other suggestion needs research and development. Development of a software based IOT would enable development of mobile apps which can act as data sending signposts in applications of service users which would enable much better security monitoring of mobile service users further, it is moot question whether agencies involved in cyber security on Indian railways be wholly within the government or not.

Given these suggestions, development on these lines would considerably enhance security monitoring including prevention on Indian Railways. ■

Brig (Retd) Manjeet Singh
DACIDS (DIARA)



The cyber world is a hugely complex word. Today we have 3.7 billion of users, 500 million in our own country. Added to it are the mobile devices which are all across. We have one billion mobile devices, out of which 30% are smartphones. And to add to that we now have one billion IOT on the network. So see the complexity which has been added. IOT is going to become 50 billion across the world by 2020. So it's a hugely complex world of cyber space in which we have to operate as common cyber citizens and the cyber warriors of tomorrow. There are two types of network on which we operate and function - first is the Air gapped networks which have also been built on imported hardware. So how much we are secured is a question mark. Second is the dependence on internet, like any other citizen we at the army too have to function by having dependence on internet.

Dr. Vatsala Joshi Pande
OSD (Research) to Hon'ble Speaker – Lok Sabha Secretariat



We cannot handle cyber world in the way the nation handles agriculture and industry. When we got independent, we were into agriculture and only looked into only 1 aspect of production - which is to increase production to feed our citizens. It was a similar case in industries too, where we looked at increasing GDP without understanding the pollution effects. But in case of cyber world we have to look into totality. Cyber world is both a very individual and collective point. So as an individual and as a nation, we have to be very well versed in using the internet. This point should go into policy decisions as well. Personally I feel that the public representatives should be aware about these cyber threat aspects in totality, so that policies can be framed accordingly and a general awareness is created among the masses. Knowing the cyber world properly will bypass half the danger of cyber threats.

DESIGN IN INDIA FOR NEW DIGITAL INDIA

Dr. Vipin Tyagi
Executive Director
Centre for Development of Telematics (C-DOT)



Cyber Security, Internet Security, Communications security and financial systems Securities are very closely integrated and when seen in light of strategic security, it becomes clear that present day security threats are motivated by gaining information based intelligence for Strategic purpose of States.

We need R&D in core communications technologies to design, develop, manufacture, market, support and upgrade both hardware and software of these complex but important systems which formulate heart of present days communications system.

There are few myths which are getting ingrained in minds of the decision makers who decide about such network related Procurements. These are

1. India cannot build highest end of technology and it is very difficult to build that capability at this stage
2. We are good in software but we cannot design hardware systems.
3. As we do not manufacture semiconductor, the value addition as well as security issues cannot be contributed by Indian designers.
4. We cannot trust Indian designed and manufactured systems as these are less reliable and less trust worthy compared to the Imported Systems even if these are coming from countries with whom we may have mistrust at different levels.
5. The cost of Indian Designed and Manufactured systems is very high so Indian Companies cannot be cost effective due to lack of economy of scale.

The list can go on but now is the time to break these myths. This is what I have done at C-DOT in the last 5 to 6 years. My analysis is based on my experiences as opposed to logical deductions and inferences alone.

I chose to come back to C-DOT and we have built complete range of Communication Systems for Broadband and Internet Service Providers.

C-DOT has capability to create Broadband Network of any size and complexity.

We have designed Pan India Bharatnet Architecture, Planning Tool and complete Electronics and Network Management Systems in C-DOT. C-DOT has given these

Technology to more than 24 Manufacturers through 80+ Technology Transfer Agreements.

Now, let me move to explain why these myths are completely baseless :

1. Indian Engineers are very good in designing complex Hardware and Firmware, Device Drivers, Broad Support Packages, Diagnostics and Porting Specialized OS. These Engineers need Sponsors who can very clearly specify requirement systems in one go and provide them with freedom and resources. The problem is that, we try to copy specification of a Western IPR based Propriety System and ask our Engineers to copy it and want them to be more Competitive without breaching IPR? Even after all limitation, Indian designers do excellent job.
2. Semiconductor no doubt are the building block of Systems and these hold key to protection of IPR at the same time Semiconductor Manufacturers require Market Leadership to sustain in Competitive World and need credible ODMs to give them scale and diversity. Most of these semiconductor are controlled by software except in case of 'Backdoors' which can be detected at higher layers in software in many cases. This makes the entire equipment extremely Safe & Secure by design. This also provides knowledge about future Improvement & Analysis. If Indian original Design & Manufacturing (ODM) becomes successful, Semiconductor Providers will be only happy to gain Market Access through them.
3. Indian Test labs are sometimes equal or more stringent than foreign Test labs and take long time to clear the products so quality of the output of these labs is better consequently, even imported equipment should be subjected to similar tests in India as acceptance of foreign Test lab results provide edge to Foreign equipments Manufacturers over Indian Suppliers. These are required to ensure the quality of supplied equipments.
4. What C-DOT has experienced that in GPON Tender, cost of Indian supplier was 2.6 times lower subsequently in all tenders wherever the C-DOT Manufacturers could clear the hurdle of Qualifying Criterion,

the cost of the Products have been lower to foreign suppliers by 40% or so. The basic competitiveness of Indian products originate from competitiveness of Hardwar and Software Design Developments competitiveness of engineers and ability to integrate in shorter time. The impressions about the cost gets formed based on commodity products like Memory Sticks, CDROMS, USB accessories where there is very little or no element of design or software based differentiation is possible. India can be very competitive in high value addition products.

5. Consequently, for safe, secure and Competitive Network/Telecom Offering, there is a need for Indian Designed, Developed & Tested Network Elements and application. Specially high end,

high value added products like Routers, Switches, Softswitches, Controllers aggregators, Optical Transport Systems including DWDM, Firewalls and other high valued added systems which are also very Security Sensitive.

The Key Challenge is to get these products passed through Business Models, Financing, Qualifying criterion, Non Tariff and Tariff Barriers, Non-Compliance to PMA and Step Motherly treatment to Indian Manufactures.

Let us commit that we will make to more rationale decisions making by buying Make In India, Design in India for New Digital India. ■

Amitabh Mathur, IPS

Former Head Aviation Research Centre - RAW



Amitabh Mathur- I speak more as novice on the subject of security but as a concerned human being or as a concerned citizen of the country, I say that change is inevitable. Technology is upon us and in many manifestations of cyber world, we are getting constantly overwhelmed by technology. Hyper connectivity in our daily lives has the potential to erode our humanity in unprecedented ways. Now phones, screens have changed the way we interact with each other. A study was conducted in which it revealed that 89% of people were interrupted by their telephone, WhatsApp and SMS messages while in conversation. 82% has said that use of devices had a negative impact on social interaction. These are very important statistics. Science gathers knowledge faster than the society gathers wisdom, so we must learn from this and I think this is the lesson for the younger students who have these gadgets in hand which allows them access to anything in the world.



UNDERSTANDING DATA SECURITY FOR THE FUTURE OF BUSINESSES

Mr. Bharat Panchal, SVP and Head – Risk Management, NPCI



Cyber security is one of the most important areas of discussion and investments for organisations today. More so for the players in the banking, finance and insurance sectors because of the increasing risks with digitisation of banking industry. While consumers are fast adopting to the new ways of banking and payments, in the wake of the Digital India movement by the government, security experts are discussing the next level of cyber security for a truly digital age.

Technology innovations are developed with a futuristic vision, to enable what was not possible before. As more and more businesses are finding tremendous Return on Investment (RoI) in big data analytics, Artificial Intelligence (AI) machine learning and virtual reality - the challenge to keep viable and confidential data safe is surmounting. Evolving security threats, both internal and external, require the use of new controls, latest methods and sophisticated advanced security tools to protect all transaction activities and data. This is applicable for not just financial institutions but all businesses having customer data to secure.

While organisations are investing heavily on security infrastructures and preventive mechanisms to get real time alert on potential breach attacks, the future is going to be exciting and complicated at the same time. Today cyber security is focused on data protection, but the future will be different.

The possibilities on the table are fully automated production lines, robotics in manufacturing and healthcare, use of AI in customer services across industries, machine learning, augmented reality in creating retail experiences, completely automated automotive and what not. Imagine the difference in a security breach now from that of in 2030. Imagine a rogue assembly line, hacked robots, failed home security, transportation, aviation, healthcare automation systems and so on. It could get much worse.

Security readiness is not an option any longer. The importance of ensuring safety with each and every innovation is an absolute must in order to make the world a more efficient and secure place. Let us start with the information available with us now, and imagine what the future of security will need to ensure protected and safe customer delivery.

- It is safe to consider that with the current wave of IoT (Internet of Things) by 2030 the world of innovation will revolve around 'things', which will change the life for every human being on the planet.
- Things like connected devices, connected devices and machinery, smart home components will define lifestyle globally.
- Automated systems will take over traditional production processes.
- From rigid structures and networks, business will become more fluid and interoperable.
- Organic resources will hit dangerous depletion levels, to be replaced by smart materials.
- A new workforce who thinks and functions in a manner much ahead of their time, essentially characterised by technologically sound, smart and demanding generation.
- Lastly, artificial intelligence will take over the human brain.

A view into the above insights leads to one particular question, above all. How do you ensure and implement effective security systems to protect large product ranges and insurmountable amount of data? This may be sourced from products, connected devices and systems including homes and workplaces, and connected humans. No amount of forecasting will be enough to step into the future with ideas. Solutions need to be built basis the insights gathered from current enterprise risk strategy, in turn leading cybercrime risk management. As long as organisations work towards the future, unlimited data from multiple sources will only pose further security threats. Being future-ready by integrating advanced tools today, will help organisations move towards 2030 with advanced connections, architectures and security frameworks. Digital ethics will also play a major role as with unlimited connected devices and lives, the potential of doing the wrong thing will constantly loom over businesses. Doing the right thing comes at a cost, and strong digital ethics ingrained in the technology development will help organisations and people make that choice. ■

BUILDING INDIA'S CYBER CAPABILITY

Uma Sudhindra
Member, Board of Governors, IIM Vizag



According to Data Security Council of India, the cyber security market is expected to grow to US\$ 35 billion by 2025. A report by NASSCOM states that the country needs at least one million skilled people by 2020. These figures are clear indication that the country has a huge scarcity of qualified cyber security professionals and the need is going to become severe with cyber criminals increasingly targeting enterprises and government establishments.

India has ranked 4th in cyber security breaches and 5th in ransomware attacks. Statistically speaking, the costs of cyber threats are spurring up very quickly. For instance, the insane cyber-attack on Bangladesh Bank costs \$ 81 million and in 2014, the cyber-attack on Sony studio was \$100 million. More recently, the outbreak of WannaCry ransomware attack cost the world \$4 billion. Cyber frauds carried out in India was worth \$4 billion in 2013 alone, and there is nothing to root it out yet. Due to thin interests in building cyber offensive and defensive mechanisms, India has become a target of cyber - attacks mostly generated from China and Pakistan.

How should India address this issue?

India needs to move out from the present reluctant position to become a truly digital power. India needs to expand cyber diplomacy and digital economy with like-minded countries to address cyber issues at the global level.

At the domestic level, we have a lot of ground to cover. Bulk of our resources are used in tackling localised cybercrime while responding to major attacks on a case-by-case basis. Recognising the criticality of the strategic dimension of cyber space, the Prime Minister's Office created the position of National Cyber Security Co-ordinator - a laudable effort. However, in the absence of a national security architecture and policy, the above-mentioned position cannot operate in a silo. Today, we do not have a system that can assess the nature of cyber threats and respond to them effectively. India's civilian institutions have their own firefighting agencies, and the armed forces have their own insulated platforms to counter cyber - attacks.

The asymmetric character of digital warfare requires a multi-agency organisation that is technically equipped, but also bases its decision on sound strategy and regular policy inputs.

A Multi - Agency Organization: Need of the hour

India has already created and established numerous organisations focussing on national cyber security. These organisations come under various ministries.

The Ministry of Home Affairs (MHA) has the following:

- National Intelligence Grid (NATGRID)
- National Cyber Co-ordination Center (NCCC)
- National Crime Records Bureau (NCRB)
- Besides the above, the MHA controls all data in Intelligence Bureau (IB), National Investigation Agency (NIA), Central Bureau of Investigation (CBI), and, Narcotics Control Bureau (NCB)

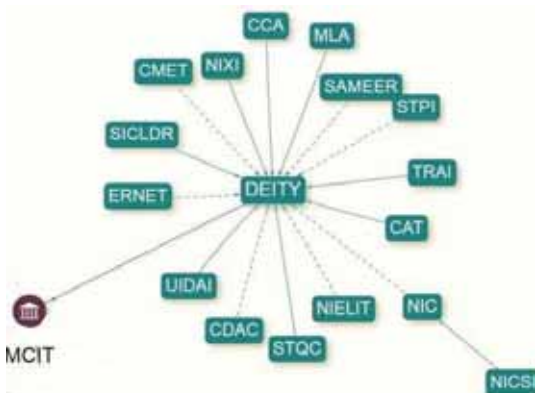
Ministry of Information and Broadcasting (MIB) has:

- The New Media Wing (NMW)
- Electronic Media Monitoring Centre (EMMC)

Ministry of Communication and Information Technology controls:

- Indian Computer Emergency Response Team (CERT - In)
- National Media Analytics Centre (NMAC) [proposed]
- Digital Swachhata Kendra (DSK) [proposed]
- Department of Electronics and Information Technology (DEITY):

Picture courtesy Medianama



Prime Minister's Office manages and controls:

- National Security Council (NSC) which controls National Security Council Secretariat (NSCS), Strategic Policy Group (SPG) and National Security Advisory Board (NSAB)
- Cabinet Committee on Security (CCS)
- Research and Analysis Wing (RAW)
- National Technical Research Organisation (NTRO) which controls National Institute of Cryptology Research and Development as well as the National Critical Information Infrastructure Protection Centre.

Ministry of Defence:

- Defence Intelligence Agency (DIA)

The **Ministry of Finance** and **Ministry of External Affairs** have their own divisions dealing with cyber security issues pertaining to their areas.

With all these organizations and agencies involved in cyber security in their own way, there is a compelling need to create one National Cyber Command or National Cyber Security Agency, with a functional nucleus or secretariat. Simultaneously, this agency's policy functions and operations must be defined clearly. This must be guided by a document that outlines India's cyber strategy as part of the overall national security strategy.

Given the power entrusted in such an agency — as with India's nuclear command, it would report directly to the PMO — it should have political or parliamentary oversight. In particular, the use of its capabilities against Indian citizens or domestic networks must be guided and supervised by a legal framework.

We should not hesitate anymore, to build our offensive cyber capabilities. This would involve the development of software designed to intrude, intercept and exploit digital networks. The deployment of cyber weapons is not a low-cost affair, as the digital trail allows adversaries to track and possibly predict the development of future technologies. Nevertheless, a cyber arsenal serves the key function of strategic deterrence. India's cyber command should be the primary agency responsible for the creation and deployment of such weapons.

Irrespective of the final form India's cyber command takes, the government would do well to pursue a two-pronged strategy in the interim.

- Advocate restraint in cyberspace as a global norm. India is an active participant in discussions around the Tallinn Manual, which is a set of non-governmental guidelines for engagement during war.
- The government should draft recruitment guidelines to hire and train a cadre of cyber specialists. Attracting such officers may require high pay scales and other benefits. USA, Israel, Russia and China have already built their cyber armies under the government umbrella. It is high time we did so too.

A highly skilled IT workforce, which, all these years has been inadvertently involved in becoming net information exporters are ready for technologies that can be "Built in India".

The question is "Will the government harness this talent effectively?" ■



THE FALLACY OF THE CYBER COMMONS

Pavithran Rajan
CyberSecurity Expert



Introduction

The global commons have been defined as those areas that are not under the control of a particular state, but are open for use by states, organizations, and individuals worldwide. They have also been described as the “fabric or connective tissue of the international system,” and include the sea, air, space, and cyberspace domains.¹ The term “commons” was originally coined by Admiral Alfred Thayer Mahan in his seminal study entitled, *The Influence of Sea Power Upon History*.²

Mahan revolutionized the concept of commerce and warfare through his analysis of military control of the seas. Mahan reviewed the role of sea power in the emergence and growth of the British Empire. He identified several narrow passages or strategic “chokepoints,” the control of which contributed to Great Britain’s command of the seas.³ Mahan drew attention to the economic benefits gained from control of such passageways through the creation of trade routes and the consequent power a state could reap by dominating seaborne commerce.

Mahan also foresaw as early as 1901 the fundamental geopolitical realities of the Cold War that emerged from the ashes of the first two world wars. In *The Problem of Asia*, Mahan urged world leaders to “glance at the map” of Asia and note “the vast, uninterrupted mass of the Russian Empire, stretching without a break from the meridian of western Asia Minor, until to the eastward it overpasses that of Japan.” He envisioned a Russia that would have to be contained by an alliance of the United States, Great Britain, France, Germany, and Japan, which is precisely what happened between 1945 and 1991 and continues to this day.⁴

Mahan also recognized the potential of China and foresaw a time when the United States would need to be concerned with China’s rise. Mahan wrote a letter in 1893 to the editor of the *New York Times* in which he urged the annexation of Hawaii by USA as a necessary first step to exercise control of the North Pacific. Mahan also foresaw a struggle for power in the area of Central Asia he called the “debatable and debated ground,” and identified the “immense latent force” of China as a potential geopolitical rival. Mahan knew that Western science and technology would, at some point, be globalized and wrote that under such circumstances “it is difficult to contemplate with equanimity such a vast mass

as the four hundred millions of China concentrated into one effective political organization, equipped with modern appliances, and cooped within a territory already narrow for it.”⁵

In 2016 if Mahan had been alive, he would have also added India, home to 1.3 billion, dominating the sea-lanes of communication of the Indian Ocean with a rapidly growing economy, having a huge population dividend and a talented human resource, as a future threat. The Indian elite does not see these realities and are preoccupied with the internal politics of a cacophonous democracy. They profess their peaceful intentions to the world and believe that their civilization is inherently a peaceful one as they have rarely ventured out of the Subcontinent, not realizing that it has more to do with the geography of its neighborhood than that of any cultural or civilisational reasons. They have a vague idea of the great potential of their ancient nation but do not realize the dangers that, apprehensions of others to their latent potential are inherently the source of strategic threats to the Indian nation. Alfred Thayer Mahan was a visionary who actually saw naval strategy as a construct for both a political and economic system. The 21st century now has a different ocean with much larger potential – *Cyberspace*.

Global Commons

In 2003, Barry Posen a Ford International Professor of Political Science at MIT and the director of MIT’s Security Studies Program wrote a landmark piece on the defense and security benefits of having unchallenged freedom of operation in the commons entitled, *Command of the Commons: The Military Foundation of U.S. Hegemony*. Posen argued that the ability to dominate these shared domains serves as the foundation of the leadership role that the United States holds in the international system. He stated, “Command of the commons is the key enabler of the U.S. global power position. It allows the United States to exploit more fully other sources of power, including its own economic and military might as well as the economic and military might of its allies. Command of the commons also helps the United States to weaken its adversaries, by restricting their access to economic, military, and political assistance”. Posen’s work on this topic brought to the forefront the role that the global commons play as a key enabler of U.S. defense, national security and economic strategies.⁶

As the 2010 U.S. Department of Defense's Quadrennial Defense Review Report states, "Global security and prosperity are contingent on the free flow of goods shipped by air or sea, as well as information transmitted under the ocean or through space."⁷ Access to the global commons enables these flows, in turn promoting both international prosperity and stability. The ability to control this access is the key to coercive diplomacy in the world order crafted by the US and its Western allies and the ability of other nations and their armed forces to ensure the unrestricted access to the global commons in varying degrees is what determines the pecking order of global power.

Thus a commons can be defined as: -

A space a) in the international system over which states do not exercise the normal prerogatives of sovereignty, and b) to which norms provide for universal access for economic, political, scientific, cultural, and sometimes military purposes, for those states with the requisite technological capabilities. **Aaron L. Connelly, B.A.**⁸

This is readily observed in each of the domains in which the commons has been said to exist and is one of the most accurate descriptions of the Commons. Without the law of the sea, which restricts the writ of sovereignty to increasing degrees as one travels further from shore, there would be no maritime commons. Without the Outer Space Treaty, which declares that outer space is "not subject to national jurisdiction," most low earth orbits would involve violations of state sovereignty, and there would be no space commons. Without the web of bilateral treaties and international cooperation providing for access to each other's national airspace, there would be no air commons.⁹

In both the maritime and space commons, states have explicitly given up the prerogatives of sovereignty through international agreement. In the air commons, they have reserved these prerogatives, but have concluded a web of bilateral treaties and international agreements that facilitate the precedence of norms of a commons over the prerogatives of sovereignty. In each case, these regimes also provide for universal access, given possession of the requisite technological capabilities even for landlocked countries.¹⁰

To bring up the strategic significance of the commons, it is important to explore how they play a role in the global economic framework. The value of world trade as per 2014 figures is about USD 18 trillion. About 70 per cent of world trade by value and 80 per cent by volume are carried by sea. Only a minuscule percent is by air and there is substantial trade, by land, particularly Europe, North America and Eurasian regions. About one per cent of the volume and 20 per cent of the value is by air. Air Carriage of freight is mostly of high value, electronic goods, including the latest smart phones, computer chips, perishable goods, medical supplies, vaccines, organs etc. The remaining is accounted for by land transport and rail.¹¹

To bring these figures into perspective vis a vis cyber space, it is estimated that **daily** transactions on SWIFT (Society for Worldwide Interbank Financial Telecommunications) is about **USD 10 trillion**.¹² The global critical infrastructures are composed of both public and private institutions in the sectors of agriculture, food, water, public health, emergency services, government, defense

industrial base, information technologies and telecommunications, energy, transportation, banking and finance, chemicals including hazardous materials, and postal services and shipping. Cyberspace can now be described as their nervous system—the control system of the Modern world.¹³ It is now evident as to why Cyberspace has been described as the strategic high ground of the 21st century the domination of which is the prize pursued by global powers. This explains the reasons for the 2016 US budget for cyber security²³ being larger than their nuclear weapons budget and the Chinese declaring their intentions to concentrate on cyberspace and information warfare.

Cyber Commons

The first to describe the existence of a commons in cyberspace was Vice Admiral Arthur Cebrowski (Retd) in 2004, while he headed the Pentagon's Office of Force Transformation. Though Cebrowski did not seek to define the global commons, he did seek to describe it. Cebrowski compares the cyberspace commons to the maritime commons of the 19th and 20th century, suggesting that cyberspace will be the most important strategic commons of the 21st century, just as the maritime commons had been the most important strategic venue in the preceding centuries. He notes the importance of the cyberspace commons to trade and communication. But he suggests that the cyberspace commons will differ in four important ways from the maritime, air, and space commons: the entry fee is much lower, and thus access is influenced by non-state actors more than states; it is non-dimensional; it is expanding at a non-linear rate; and "its characteristic interactions more closely approximate the human condition, making it an enormously complex operating domain." Despite Cebrowski's untimely death in early 2005, the "cyberspace commons" language was included by the Defense Department in its 2005 National Defense Strategy.¹⁴

Cyberspace can be broadly divided into a physical layer and an information layer. Each layer operates under a different set of dynamics. It is easily understood that the information layer's existence is dependent upon the continued existence of the physical layer. Less easily understood is that this is not a one-for-one dependency. Parts of the physical layer can be destroyed, damaged, turned off or replaced without effecting the destruction of proportional value in the informational layer. This is, in part, because of the increasingly common information assurance practices, which create redundancies within the information layer.¹⁵

Second, cyberspace's information layer is a social construct. Much of the value in cyberspace is stored not only in the code on servers, but also in the various patterns of interaction that take place via the exchange of code between servers. For example, the value of an enterprise like Facebook is not only primarily in the data stored on its servers, but in the way that Facebook facilitates interaction that result from the connection of people around the world. The international community is slowly realising the intelligence potential and economic value of this record of interactions. It is thus the most efficient domain for the transmission of ideas, goods, and capital. If the physical layer of cyberspace is destroyed, damaged, or turned off, these networks on the information layer persist in the minds of those who build and use them. If they are of value, participants are likely to seek to reestablish them either using other elements of the physical layer, or by building new physical infrastructure to support them.¹⁶

Third, cyberspace is a human-made domain, subject to quick and constant reorganization and reconstruction. This is true of both the physical layer, which is comprised of terminal appliances, fiber-optic cables and radio frequency spectrum, as well of the information layer.¹⁷

Fourth, cyberspace is a venue for military activity. This includes a spectrum of activities across the political, strategic, and tactical levels—from the formation of alliances, to competition for superiority, to low-intensity conflict, espionage and surveillance to complete warfare. Scholars of cyber war describe a range of military activities in cyberspace, from surveillance to coordinated Denial of Service (DDoS) attacks. Scholars of security studies have also reached a consensus that cyberspace constitutes a separate “domain” of warfare, alongside the maritime, land, air, and space domains. This elevation of cyberspace to domain status has gradually occurred over the last ten years.¹⁸

Fifth, barriers to entry are low. One no longer even needs a personal computer and landline connection to take advantage of the benefits that cyberspace provides, given the ubiquitous smart phones and wireless connectivity in both the developed and developing world. But barriers are not only low for individuals; they are also low for those interested in using the Internet for military activities. Building a navy, air force, or fleet of satellites and space weapons are all extremely capital intensive and costly endeavors. In this sense, the cyberspace domain is similar to the land domain, where barriers to entry are also very low.¹⁹

The Fallacy of the Cyber Commons

Though governments have asserted sovereign control over the Internet in response to perceived threats, the authority to govern the Internet has always resided with the state, specifically with the U.S. government. The Internet is a DARPA invention and at the most basic level; the United States Government controls the current system of organization of the Internet. The United States Commerce Department holds ultimate authority over the disposition of the official root zone file—simply defined as the file, which directs the Internet Protocol (IP) address of every end user. This is the technological hierarchy that directs all traffic on the Internet. The U.S. government has strategically taken a hands-off approach to this responsibility, contracting it out to either academic or non-profit institutions; all attempts for multinational control have been stonewalled. But this arrangement may not be sustainable especially after the Snowden revelations.²⁰

In recent years other governments have challenged American control of the official root zone file. Governments around the world are increasingly unhappy with the custodianship of the Internet Corporation for Assigned Names and Numbers (ICANN), the Los Angeles-based non-profit contracted to administer the file since 1998. As this article is written there was an announcement that the US control of the Internet has ended. The announcement; to end direct US government oversight control of administering the Internet and commit permanently to a *slightly mysterious model of global “multi-stakeholderism”*; whatever that means. This falls far short of attempts by other nations to have the United Nations, International Telecommunication Union to take over its job.²¹

Much of the assumption of the existence of a cyberspace commons appears to follow from a basic recognition of cyberspace’s network-like qualities under different national jurisdictions but once we understand that the key networking hardware, protocols and big data companies in numerous spheres are all American, in combination with the recognition that cyberspace constitutes its own domain of warfare, alongside the land, maritime, air, and space domains.²² Given this assertion of state sovereignty over cyberspace, and the lack of any norms of universal access, it is evident there is no commons in cyberspace. The construct of a commons in cyber space appears to be a careful orchestration of US strategy to promote their interests and to consolidate their grip on this vital domain through a strategy of promotion of big US centric MNC’s.

As we peer into the future, it is evident that the USA, the dominant global power, would like to preserve the chimerica of a Cyber Commons that it can continue to dominate, the contours and dimensions of which are yet to emerge. A future Cyber Commons if it ever evolves should be a physical layer of access based on open source technologies controlled by the UN. Such a physical layer could be based on non-terrestrial platforms (preferably space based) to prevent nation states from exerting sovereign control. The information layer eventually will evolve wherein data generated in a sovereign jurisdiction would be stored within its territorial jurisdiction. Not doing so would result in big data companies like Google and Facebook having tremendous ability to influence economic, diplomatic, military and political activities in other nations. The realities of today are that control of the physical layer rests with the Original Equipment Manufacturers (OEM’s) and not with the system/network administrators who have an illusion of control by their perceived ability to configure the Graphical User Interface of their appliances. The vast majority of the information layer is also firmly in the grip of the Big Data companies, which are primarily of US origin and have their server farms located in USA.

China and Russia

When you look at the cyberspace domain outside the west, it is but natural to examine the state of affairs of the two open strategic challengers of the west, China and Russia.

China with a 700 million plus population online is the largest market in cyberspace. Although it has embraced the Internet along with the rest of the world, China has always enforced a strict control on the content of the net, which was called the ‘Great Firewall of China’. Western literature was widely critical of these controls and effectively tied them to the idea of an authoritarian political system suppressing free speech to cling onto power. The West was also widely critical of state supported hacking by Chinese groups and the world was widely outraged by the specter of massive espionage; stealing of intellectual property of top Western companies, dissident groups, neighbouring countries, international bodies etc. These reports were mostly true and still continue, but dramatically lost steam after the Snowden revelations and the perfidy of the US and the NSA with most of the silicon valley technological firms exposed as being part of a global surveillance infrastructure. The US has since tried to differentiate between the economic espionage by the Chinese, and US surveillance chiefly being supportive of the global war on terrorism with little success.

The Chinese by its policies have successfully midwived such companys as e-commerce giant Alibaba Group Holding Ltd., online conglomerate Tencent Holdings Ltd. and information aggregator Sina Corp, which enable Chinese citizens to enjoy most services Westerners use, without needing Google or Facebook. The Chinese government is directing financial and policy support toward domestic firms that are developing semiconductors and servers that can replace ones provided by Western firms. China has also unveiled Internet Plus, a strategy to incubate Chinese companies that integrate mobile, cloud and other types of computing with manufacturing and business. Many Western companies have started conforming to Beijing's rules to take advantage of the Chinese markets. LinkedIn structured its Chinese operation as a domestic company and agreed to comply with Chinese rules. Hewlett-Packard, sold a majority stake in its China server, storage and technology services operations to a Chinese company after it came under pressure in China following revelations that U.S. officials collected information abroad using infrastructure produced by American companies.²³

China is seeking international validation for its efforts. Earlier this year, China led Russia and some Central Asian countries in proposing the United Nations adopt an Internet "code of conduct" that would effectively give every government a veto over technical protocols interlinking the global Internet. As social media helped topple regimes in the Middle East and northern Africa, the People's Liberation Army publicly warned that an Internet dominated by the U.S. threatened to overthrow China's Communist Party. The Chinese declared that the Internet represented a new form of global control, and the U.S. was a "shadow" present during some of those popular uprisings. On July 1 2015, China's legislature passed a new security law asserting the nation's sovereignty extends into cyberspace and calling for network technology to be "controllable." A week later, China released a draft law to tighten controls over the domestic Internet, including codifying the power to cut access during publicsecurity emergencies. Other draft laws under consideration would encourage Chinese companies to find local replacements for technology equipment purchased abroad and force foreign vendors to give local authorities encryption keys that would let them control the equipment.²⁴

Cyberspace in Russia was largely considered a zone of relatively free expression and little state involvement. Following the rallies of the Russian opposition in 2011-2012 and the onset of the Arab Spring in both of which the Internet played a significant role, cyberspace and its potential for political disruption was taken note off. The Snowden revelations added to Russian threat perception and military actions in both Ukraine and Syria and the resultant tensions with the west prompted a series of legislative, technological and diplomatic measures aimed at preventing domination of cyber space by the west. 01 Sep 2015 saw the enactment of Russia's new law on personal data, which requires foreign companies that handle personal data of Russian citizens to process and store such information inside Russia. To comply with the law, many have already moved servers inside the country's borders. EBay, Google, and others are in the process or have already moved user data in country. EBay is transferring data from Switzerland to Russia. Google has moved some servers' in country to comply with data localization laws and announced plans

to discontinue development work in Russia and move its engineering operations there to other countries. Adobe said it would close its offices in Russia, and Microsoft closed a developer office in the country, moving a significant portion of the operation to Prague.²⁵

Russia has banned use of foreign software for many categories of government services and the new changes will include the introduction of ten percent levy on software sales in Russia, the abolishment of VAT preferences for software developers and the design of Russian analogues of imported software. It is planned that the revised doctrine will also encourage the establishment of software production within Russia and increase the powers of law enforcement agencies to block banned information spreading through anonymous networks. This currently occurs in accordance with court decisions and as part of extrajudicial procedure.²⁶

Russia has reportedly run tests to see if it can remove itself from the World Wide Web to stem the flow of information to and from foreign countries. The tests were run to prepare for an information blackout in case of a potential domestic political crisis. The goal was to see if Russia's Internet could continue to function even though it was cut off from the global Internet. The Putin regime has publicly stated that the freedom of the Internet will be protected but the state will take measures to defend itself.²⁷

Indian Calculus

USA, the world leader in innovations in Cyberspace, and the original proponent of concepts of Information Warfare, today controls most of the Information repositories of the world through their giant MNC's and has been successful in influencing the thought processes of the majority of the global population where free flow of data has been linked to freedom of expression and ideas. Such a construct has been propagated with the connivance of their Western allies.

The hollowness of these ideas were exposed by the Snowden revelations and recognized recently by the European Union in a landmark judgment where the principle of 'safe harbor'²⁸ used to transfer data across national boundaries was stuck down. This has profound implications for the world wherein clear delineation has been made between freedom of speech, ideas and personal data.

In the Information Age, although traditional methods of power projection is still relevant, the advantage will always belong to nations that can effectively garner and process the huge information flows of Cyberspace to give a competitive advantage to their nation in all spheres; be it military, diplomacy, trade etc. The global ICT market is poised to undergo a revolution post Snowden. The initial ripples can already be seen in the recently concluded BRICS conference where Brazil, Russia and South Africa urged India to take the lead in building a new global ICT architecture based on Open Source Technologies.

India has still not exploited this situation fully, although the political leadership has made the right beginning with the *Make in India* initiative. A very effective and entrenched software industry catering to the West and their representative industry bodies in collusion with sections of the bureaucracy

in both the military as well as the civilian sector has opposed transition to indigenous and open source technologies with out fully understanding the strategic dimensions of the issue. Such a change can, not only kick start domestic manufacturing and entrepreneurship but will find huge markets overseas. This strategy will also find increasing backers from nations who want a multipolar world and are in consonance with India's stated strategic aims.

Conclusion

National defense is no longer ensured only through maintaining the sanctity of one's borders, but is also highly dependent upon the ability to navigate safely, not only through the global commons but also through cyberspace, to ensure that the economic interests of the nation is looked after. These commons—sea, air and space plus Cyber Space are at present dominated by the USA who does that by leveraging two pillars of power - the USD as reserve currency and American military power funded by fiat dollars. The American dominated world order has permitted other nations including China to economically progress as long as they do not upset the current world order.

American strategic thought process identifies Russia, China and India as long term strategic rivals, India less so than Russia and China. Although American strategy currently involves shoring up India as a counter to China it is uneasy on the long term implications of Indian power potential and views India as potentially a long term rival that can challenge American domination. To that extent the Indian nation, if it has to reach its full potential will have to make an independent cyber strategy based on indigenous technologies as otherwise it can be open to strategic disruption from the cyber medium as the diverse population mix is more susceptible to internal schisms in comparison to a much more uniform Han Chinese and Russian population to a Hybrid threat matrix. The short term threat to India might be from Pakistan and China, but these threats are not existential in nature unless there is a nuclear war. As the Indian economy grows the West might increasingly tend to keep India disbalanced to have leverage, as Western strategy tends to look at capabilities than intentions. The Indian nation by its very size is a long term strategic competitor for China as well as the USA for global leadership and the threats to it from realising its just place in the comity of nations in a globalised and nuclear environment are more likely through internal disturbances exploiting the numerous social, regional, religious, economic and political faultlines intelligently orchestrated using cyberspace. The ocean of Cyberspace, *the strategic high ground of the 21st century*, is without doubt firmly in the grip of the USA with only China even attempting to challenge it. A nation the size of India, with its latent power potential and huge diversity of population cannot afford to ignore these realities. The need of the hour is understanding of strategic realities and a well-nuanced plan of action. ■

Bibliography

1. http://yalejournal.org/article_post/security-challenges-in-the-21stcentury-global-commons/ Tara Murphy 1,2
2. <http://thediplomat.com/2014/12/the-geopolitical-vision-of-alfredthayer-mahan>, <https://history.state.gov/milestones/1866-1898/mahan>, <http://dailyreckoning.com/alfred-thayer-mahan-the-influence-of-alfred-thayer-mahan>, <http://www.worldaffairsjournal.org/article/mahan%E2%80%99s-naval-strategy-china-learned-it-will-america-forget-it> 3,4,5
3. The Case Of The "Commons" And Cyberspace: Concept Formation And Social Construction By Aaron L. Connelly, B.A., <http://cyberbelli.com> , Defining our National Cyberspace Boundaries By Colonel Jeffery R. Schilling 8, 14, 16, 17, 18, 19, 20, 22
4. https://www.wto.org/english/res_e/reser_e/ersd201506_e.pdf Staff Working Paper ERSD-2015-06, 18 June 2015, World Trade Organization Economic Research and Statistics Division, <http://www.icao.int/sustainability/Pages/FactsFigures.aspx> 11
5. <http://www.forbes.com/sites/brucedorminey/2015/11/02/russiannavy-probing-u-s-undersea-communications-cables-in-new-globalthreat/#72f6e6b266b1> , <http://www.bis.org/statistics/rppb1601.pdf> , BIS International banking statistics at end-September 2015 - rppb1601.pdf , <https://www.swift.com/about-us/swift-fin-traffic-figures> 12
6. https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf, Homeland Security: An Introduction to Principles and Practice By Charles P. Nemeth 13
7. <http://www.theguardian.com/technology/2016/mar/14/icann-internetcontrol-domain-names-iana>, <https://www.icann.org/resources/pages/governance/aoc-en> 21
8. <http://energy.gov/cfo/downloads/fy-2016-budget-justification> , <https://www.whitehouse.gov/blog/2015/02/02/fact-sheet-middle-class-economics-president-s-fiscal-year-2016-budget> 23
9. <http://searchcio.techtarget.com/definition/Safe-Harbor> , <http://www.theguardian.com/technology/2015/oct/06/safe-harboureuropean-court-declare-invalid-data-protection> 28
10. <http://www.wsj.com/articles/china-pushes-to-rewrite-rules-of-globalinternet-1438112980>, <http://www.wired.com/beyond-thebeyond/2015/12/respecting-chinese-and-russian-cyber-sovereignty-in-the-formerly-global-internet>, <http://www.businessspectator.com.au/news/2015/12/16/china/xi-callsinternet-sovereignty> 24
11. <http://www.russia-direct.org/archive/russia-direct-report-digitalsovereignty-kremlins-tangled-web-internet-security>, 25
12. <http://www.scmagazineuk.com/russia-updates-its-it-security-strategy-inreaction-to-current-tensions/article/399679> , <http://news.discovery.com/tech/gear-and-gadgets/russia-wants-out-ofinternet-151019.htm> 26
13. <http://www.russia-direct.org/archive/russia-direct-report-digitalsovereignty-kremlins-tangled-web-internet-security>, http://www.huffingtonpost.com/entry/china-cyber-sovereignty_b_6324060.html?section=india, https://rbth.com/defence/2016/02/02/russias-defense-industry-to-get-itsown-internet_56422927

CYBER SAFETY FOR CHILDREN – CHALLENGES AND SUGGESTIONS JAAGO TEENS, NGO

Sanjukta Mookerjee Sahni
Cyber Safety for Children: Challenges & Suggestions



Is there a chance that a person who has not learnt how to drive can kill himself if he tries to drive? If yes, then make sure a child (first-time user) does not go online until he/she learns how to use the net safely.

Would you let your child sleep in a public place? Keeping the internet in their bedrooms is like allowing people into your public space; we think children are safe and secure in their bedrooms. (This issue is extremely important: blue whale cases - **having access to the net when everyone else is sleeping**).

Challenges:

Weakest and strongest link in the cyber world is the human being
Just one wrong click on a link can create a monumental problem – e.g Wannacry Ransomware

- 1. Impact on Real World Safety** - huge perceived gap among the masses in India, of the impact that one's online actions can have on one's Real World Safety! The free-for-all mentality needs to be urgently set right from the time a child is in 2nd or 3rd standard... There are rules online and how we use Internet can impact our own safety
- 2. Social Engineering & Vulnerability** - a stranger impersonates and discovers a child's whereabouts and personal information; Vulnerable age of children has moved downwards where earlier we targeted children from class 8 upwards, we are now looking at educating children class 3 onward; Hackers exploiting people/children posing as friend is a grave threat. Apps and permissions that we give away so easily and children sign-up for these Elderly/grandparents are also vulnerable to social engineering;

- 3. Lack of knowledge & awareness** - parents and teachers not aware of scope of safety, of global reach of internet and of internet misuse; Netiquette: The Internet is a public space that needs to be maintained and used with decorum. The way the Delhi Metro is a huge behemoth that needs to be maintained in orderly fashion for optimum benefit; One must remember that the fine print that says terms and conditions always puts the onus on the user.

- 4. Digital Safety must go hand in hand with Digital Literacy**
Technical Safety -> anti-virus, cyber security firms: these are steps to ensure data is safe
Online financial safety -> banks & companies have IT depts. who work on financial fraud prevention
What about Social safety, emotional safety, physical safety - who works towards this? Emotional and social safety impacts financial as well as physical safety
Abroad we have NGOs/organization like Netsmartz, and in India?

- 5. The Human Element: Emotional and social conundrum** - the huge impact that incidents can have on kids when there is improper use of net or lack of knowledge on how to handle situations; it has a 24/7 impact and the anonymity of the internet makes it easier to misuse.

Suggestions:

- **Defining boundaries & Communication Channels** - open communication between children and educators; tracking time spent online; Asking children not to clam up but to talk freely about any unsettling situation they face online. Their trusted adults might not have much knowledge of the internet, but still they must talk.

- **Broadcasting/Public awareness** - messages to teachers regarding any new challenge/cyber security treat to children; keeping them up-to-date with technical knowledge; probably awareness campaigns too
- **Parents/Teachers survey** - to discover depth of knowledge
- **Experiential journey into cyber education:** Road-shows, exhibitions, children's pavilion activities, fun/interactive booths

NGO JaagoTeens

Formed: 19th apr 2010

Coverage - 80000 students/teachers/parents/rwa

Future Strategy - Extensive coverage: pan India as fast as possible; Target the educator to spread message

JaagoTeens, a Society registered in April 2010 under Societies Registration Act of 1860, **is committed to promoting a responsible and safer internet ecosystem.**

With the recent massive thrust in Digital Literacy being witnessed in our country, we sincerely believe it is imperative that **Digital Safety goes hand in hand with Digital Literacy.**

To achieve this mission we constantly work to expand and evolve our content, encouraging and educating, especially our student communities, to promote a safe and responsible internet, enabling youth to benefit from the massive potential the internet holds.

G- 138, Sarita Vihar, New Delhi - 110076

info@JaagoTeens.com

leena@JaagoTeens.com

Website: jaagoteens.com ■



CYBER LITERACY FOR 2030

Dr Arunima Chakravorty
Principal, Delhi Public School Bhagalpur
Secretary, V.B.College Of education
Member, Angika Development Society



Cyber literacy needs to be seriously addressed if we wish to secure the future of 2030. The topic needs to be addressed seriously by every user and stakeholders. I don't know how far we can make this virtual space safe as the realistic space around us is still to be made safe so that our future generations can move safely without fear. Every now and then we hear news of crime, which needs a pathological insight. *We all are moving towards becoming digital citizens of world consequently safety should be our first concern with cyber literacy.*

Of all students are very vulnerable to cyber crime as because of they are curious but limited in maturity and awareness. The criminals get information about children through name, address, class, and school name and birthdays. The collected information from the children are used by the cyber criminals to guess passwords of children and their parents as in general password of family members are mostly related with family names and days. According to Uninor, a telecom operator, in a study conducted in some states in India, states that one third of school going children have experienced cybercrime in the form of cyber stalking, defamation, cyber bullying and hacking. Children rarely speak to their parents about their online activities, experiences and in cases if they do so, parents are ignorant about it or take it just as a small happening. It is imperative for the parents to be open with their kids about online safety as much as it is by their Teachers. Children find these online services a good way to make friends and start relationships. We should educate the children on the consequences of meeting people they meet online.

Parents remain under the impression that children are on the net doing projects, work assigned to them by the schools but many a times on contrary they indulge in social networking due to psychological inherent characteristics of curiosity to explore, downloading music and movies. Children see internet as an option with tons of information and answer to any of their queries. We need to teach them how to handle cyber space constructively for prosperity of human experiences and build resilience in them and at the same time monitor their activities and ensure them to rules that keep their use in limit but more important is to create awareness on principles of on-line activities like safe passwords and not to share information and indulge in fake profile, morphing pictures and posting them on social networking sites to defame their friends.

Education is the only way to prevent any type of crime in the society. We shop online. We work online. We play online. We live online. More and more, our lives depend on online, digital services. Almost everything can be done online - from shopping and banking, emotional mapping to socialising and card making - and all of this makes the Internet, rather known as cyberspace, an attractive target for criminals. Crimes can only thrive in the world where we have humans known as essential part of civilisation. But yes, we all have the responsibility to protect the digital services from being misused in the best interest of humanity. Students should be guided and educated. Feeling for the urgent need we need to have in place a proper structured syllabus on cyber security. Students should be taught with the basics of cyber, from confidentiality, integrity and availability to the meaning and types of Malwares to the concept of phishing. It may be surprising that many cyber security breaches do not result from technical failures. GPS and location services also aids the cyber predators. Students need to be aware that face book is tracking us much today and if we are worried about privacy then Google, face book and twitter should be minimized. In fact it is commonplace for attackers to exploit the goodwill and trust of people to gain access to systems, using a form of attack that is known as 'social engineering'. Pretending to be technical support personnel or crafting emails that ask for usernames and passwords are common forms of social engineering attacks. Phishing is a form of social engineering. Students should also be taught the ethics governing cyber space as how to handle threatening messages and making them understand that they need not suffer in silence if they are cyber bullied and sharing information with the right person they are comfortable with. Students should also be educated on the punishable offence as per cyber laws. Our focus is on cyber literacy, moral basics, and emotional quotient in cyber, ethics in cyber domain, technological innovation and Artificial intelligence so that we can create an army of Cyber professionals ready for future world. Students are "glued" 24/7 to their mobile devices, but still it is necessary for schools to make them digital literate. But what does it mean to be "digitally literate"? Is it being digitally fashionable or digitally learned? The answer is not clear but with time we should be able to reach at the difference. Educators struggle to understand their evolving role in teaching and using technology in their classrooms, We

too need to be properly educated as educators to become digital gurus. Most importantly, many of us wrestle with how technology is shifting the way kids learn.

New York Department of Education defines digital literacy as “having the knowledge and ability to use a range of technology tools for varied purposes.” Digitally literate people are those who “can use technology strategically to find and evaluate information, connect and collaborate with others, produce and share original content, and use the Internet and technology tools to achieve many academic, professional, and personal goals.

Most teachers recognize those skills as critical for 21st-century learning. But before teachers and students dive into using technology in class, we need to understand that digital literacy curriculum is **necessary rather essential**. There needs to be a detailed syllabus on this and the organisers and stakeholders in India’s education system should deliberate at length.

Students are the “digital natives” while teachers and parents are the “immigrants.” Students do not “naturally” know how to use technology for learning and needs to be taught like literacy and Algebra. In one of his most popular posts titled “The Fallacy of Digital Natives,” Dan Ponte-fract claims that “learning and technology has nothing to do with generational divides;”. We as Indians are paranoid about safety, specially our parents that we all have gone through in our age as students.

Certainly students view their devices as an essential extension of their body. Certainly their first instinct is to Google the answer to an unknown query, the flip side of it is that technology is making us dependent to an extent that we ourselves not sure of the answers that we have to our questions. Are we suspecting our own knowledge just because of technology? Caution at times is good and we Indians as we are culturally sensitive take step with immense checks and balances. But often times they only scratch the surface of potential for using their technology for authentic learning. Many times, their parents are either afraid of engaging with their teen’s digital social lives or clueless about the degree to which their teen’s virtual

social lives even exist! Parents and teachers often operate from a default of fear and suspicion, choosing to hide their own social networking or forgo it altogether because of “what might happen.” There are legitimate concerns about oversharing and inappropriate behaviour. When social media makes the formal informal and blurs the boundaries of appropriate behaviour, damage is done. But these concerns will NOT prevent our students from using social networks. It will only keep these social spaces separate from the positive influence of adults. Because the adults are *condemning* them instead of *engaging* with them. All the stakeholders should ensure that a proper structured syllabus be put in place in all schools, sensitization of students and parents be undertaken in the wake of rising cyber crimes. The problem lies in our system as we are there for knee jerk reaction than being ready with a syllabus that can take our children of present age to a different tangent of ethical cyber awareness coupled with training for cyber warfare simultaneously. North Korea and China are training their five-year children in cyber. China is preparing a horde of army by ensuring thousands of children reaching five year of age to learn Hindi and study Indian books on culture and heritage so that they are able to think, act and work like we Indians and this exercise is being done by China at war footing as they see India as a potential threat. Our education system has not specifically taught or prepared our children with cyber hygiene, cyber ethics and cyber offensive when country needs, the students have just been left open to high end technology and devices to play with. We have given free laptops to empower the youth with technology but have hardly worked on cyber education. We must bring in digital awareness, cyber hygiene in education curriculum and cyber nationalism in case of an emergent war with any country in times ahead as the students have become vulnerable and the most tragic part is many a times most of them are not aware that they are committing an offence. We need to channelize these young fertile minds to productive use in the best interest of India as a country and a global leader in making. ■

Professor Chandan Chowdhury
Associate Dean – Indian School of Business



On 22th September, when I used to be a managing director in an MNC, I received an email that I have to do a remittance to HSBC bank for acquiring a company. My president then got into a call with me telling me to do it immediately. It was actually not my president but a Robot; the email was a fake email. The size of the cyber world is increasing. We cannot run away from it and we have to protect it. The government might have removed 500, 1000 rupee notes but now cryptocurrency like Bitcoin is becoming very popular. We know about in US this month the identity and confidential data of 143 million people have been hacked. Bitcoins’ value in 19 months increased by 10 times which resulted in many people investing in it. Now if you look at bitcoin itself we had a huge catastrophe with a company called Bitfinex and 65 million dollar worth of bitcoin was actually hacked.

CHALLENGES-CYBER SECURITY – 2030

Prof Dr Sharad Sinha
NCERT, New Delhi



The education system in India, and across the nations, has evolved from community sessions in open spaces and Gurukuls, to teacher centered classrooms and ultimately giving way to learner-centered, technology driven education, off-line, on-line and on demand. The implementation of the Right to Education Act to provide access to quality education to all children in the country irrespective of gender, caste, creed, religion and geographies has enhanced the demand integration of technology for governance and better delivery mechanism.

As an academician, I see a tremendous paradigm shift and emerging challenges in the future education scenario. While we are slowly moving towards digitization, various emerging stakeholders across the globe are progressing on a fast forward mode and developing technology leaps and bounds. Two decades back it was a matter of pride for a school to own a computer, today computer have become an inseparable part of student life and a necessity.

The evident shift from teaching computers as a separate subject in schools to a revised ICT curriculum for school across India focusing on integrating ICT tools as part of pedagogy has made the classroom a different place altogether.

As technology is changing at a rapid pace, so much so that it's challenging to grasp and integrate it in education system. The proliferation of gadgets and access to internet is further democratizing education. As per a recent Google- KPMG report, the Indian on-line education sector is expected to grow to a USD 1.96 billion industry by 2021, owing to increased Smartphone's penetration and increased data speed. The development of MOOCs and other e-learning platforms will further provide plurality of resources for teaching-learning process and skills development.

As futurist Thomas Frey predicts, in 15 years from now learning will be through robots teachers over the internet.

Moreover, with the growth of the Internet based technology, we can see the creation of tremendous opportunities for enterprises to develop new services and products for education system that will offer increased convenience and satisfaction to their end users. The rise of objects that connect themselves to the Internet is releasing an outpouring of new opportunities for data gathering, predictive analytics and IT automation for producing better learning outcome among students.

What happens to technology in the next 13 years may not simply impact learning in a typical cause-effect

relationship. Rather, it might be the case that one absorbs the other, where information access, socializing ideas, and creative collaboration may be organic and completely invisible, this will require to shifts the focus from developing and operations as it is done now to developing, security and operations together.

I predict assessing learning out-comes of education system will be based on the feedback of biological responses of students including sweat gland stimulation, heart rate, eye position, and other data rather than the traditional ways and serve not only the educators, but-profit organizations for the purpose of analytics, market research, and ultimately consumerism. Learning simulations are on way to replace teachers very soon.

Schools as we know them will be outnumbered, no longer just supplemented by eLearning, blended learning, and self-directed learning platforms, but incredible learning simulations and full-on virtual worlds. E- Books will replace the existing books with other plurality of resources available online.

As futurist predict, the largest companies will be education based that have not been thought of. As cybersecurity evolves, so does the thought that everything cannot be protected equally rather we need to find ways and collect only what that matters.

Artificial intelligence is gaining momentum, IBM on way to develop Watson powered Robots, Google developing Deep Mind and Amazon developing Drone delivery

Remaining schools that refuse to adapt to new technology and cultural trends will cause splintering in some communities as the significant cost of technology integration increases socio-economic gaps. Seamless Heads-Up Displays will equip learners with information, feedback of performance, and social data in real-time.

New certificates of achievement and performance that are social, portfolio-based, and self-selected will begin to replace institutional certificates, including college degrees.

The rapid uptake of Bring Your Own Device (BYOD), and the introduction of wearable devices in the workplace, will increase an already high demand for mobile applications for both school and home. To meet this increased demand, developers working under intense pressure, and on paper-thin profit margins, will sacrifice security and thorough testing in favor of speed of delivery and the lowest cost. This may result in poor

quality products that could be easily hacked by criminals or hackers.

The threat of theft of sensitive information by unauthorized users and siphoning information from smartphones via insecure mobile applications. The level of hyper-connectivity means that access to one application on the Smartphone can mean access to all of a user's connected devices.

In this scenario, the important stakeholders of our education system, learner, irrespective of his age and people associated with him will be prone to cyber threats, cyber bullying or cyber attacks. Cyber security-attacks / bot attacks will continue to become more innovative and sophisticated with each passing day. Unfortunately, while businesses are developing new security mechanisms, cybercriminals are developing new techniques to evade them at a faster pace. The increase in the sophistication of cyber-attacks is much higher than increase in our dependence on the Internet and technology. It is not heard to believe that cyber security is an area with zero percent unemployment rate.

After many years of trying and billions of dollars in investment, why are organizations are still struggling with cyber-security? Answering this question requires moving beyond a purely technical examination of cyber-security. But if looked at the challenge more broadly, even if the technical issues resolved, cyber-security would remain a tough challenge for three reasons:

- It's not just a technical problem
- The rules of cyberspace are different from the physical world's
- Cyber-security law, policy, and practice are not yet fully developed

- It's not just a technical problem

Cyber-security is more than just a technical problem, incorporating aspects of economics, human psychology and further advancement in technology some time make it prone to hack and misuse.

- Differing Rules in Cyberspace

Cyberspace operates according to different rules than the physical world. As a result, our physical-world mental models simply won't work in cyberspace. For example, in the physical world, we assign the federal government the task of border security. But given the physics of cyberspace, everyone's network is at the border. If everyone lives and works right on the border, how can we assign border security solely to the federal government? In the physical world, crime is local — you have to be at a location to steal an object, so police have jurisdictions based on physical boundaries. But in cyberspace you can be anywhere and carry out the action, so local police jurisdictions don't work very well.

The same principles of cyberspace that allow businesses to reach their customers directly also allow bad guys to reach businesses directly. Yet you can't have governments get in the way of the latter without also getting in the way of the former. Sharing information among people at human speed may work in many physical contexts, but it clearly falls short in cyberspace. As long we continue to try to map physical-world models onto cyberspace, they will fall short in some fashion.

Legal and Policy Frameworks

Next, cyberspace is still very new from a legal and policy point of view. In the modern form, the internet and cyberspace have existed for only about 30 years and have

constantly changed over that time period. Therefore, we have not developed the comprehensive frameworks we need. In fact, we don't yet have clear answers to key questions:

- What is the right division of responsibility between governments and the private sector in terms of defense?
- What standard of care should we expect companies to exercise in handling our data?
- How should regulators approach cyber-security in their industries?
- What actions are acceptable for governments, companies, and individuals to take and which actions are not?
- Who is responsible for software flaws?
- How do we hold individuals and organizations accountable across international boundaries?

In India, we have Information Technology Act 2000, amended in 2008 with key provisions under section 66-A to 66F, 69A and information technology rules under section 79.

In the near future, as artificial intelligence (AI) systems become more capable, we will begin to see more automated and increasingly sophisticated social engineering attacks. The rise of AI-enabled cyber-attacks and bot attacks are expected to cause an explosion of network penetrations, personal data thefts, and an epidemic-level spread of intelligent computer viruses.

Even today, AI can be used to defend and to attack cyber infrastructure, as well as to increase the attack surface that hackers can target, that is, the number of ways for hackers to get into a system. In the future, as AIs increase in capability, I anticipate that they will first reach and then overtake human beings in all domains of performance, as we have already seen with games like chess and Go and are now seeing with important human tasks such as investing and driving. It's important for business leaders to understand how that future situation will differ from our current concerns and what to do about it.

If we are unable to address the issues related to cyber security in education sector in particular then we should be ready to face the following consequences of these challenges which our new generation will encounter:-

- **Biological Challenges:** Penetration of technology in personal and professional life of a learner is a boon till it serves the purpose for which it is used. Misuse of shared information of learners will increase the anxiety levels of learners leading to mental stress, neurological problems, erratic behavior, aggressiveness etc. In unsecured sea of cyber environment one cannot expect the balanced biological development of learners.
- **Psychological Challenges:** Cyber crimes are result of psyche of hackers to misuse the information, damage the reputation and create chaos in the system. It is less of technical and more of psychological in nature. If cyber-crimes remain unaddressed then it will act as multiplier effect in catalyzing more of such activities.
- **Social Challenges:** We are not dreaming of a society of biologically and psychologically challenged learners busy in acquiring knowledge and skills through internet which is harmful to society. We do have numerous examples of social unrest in our different part of country and even international conflicts originated through information leaks by hackers.

- **Economical Challenges:** Most of the cyber-crimes used to be done for economic consideration. So, this is a route of economic prosperity for an individual, society or even for a state. The number of unemployable youth who are techno-alert will increase around the world with the explosion of new technologies and artificial intelligence. The probability of such youth who are living in disintegrated family and fragmented society to indulge in cyber crimes are high.
- **Emotional Challenges:** Young learners are emotionally weak and therefore, whenever their shared information get leaked or misused then it not only adversely affect their performance but it act as multiplier effect in challenging the different sub system of family and society.
- **Value based conflict:** Cyber crimes, hacking etc. are the by-products of loss of values in society. Youth swimming in the ocean of information's resulted from different cultures, religions, value system, thoughts and opinions found it difficult to judge what is right or wrong for them. The changing values in society from better to worse produce catalytic effect in diverting intelligence of youth towards cyber crime. With the advent of technology and artificial intelligence there will be further erosion in value system of society. If we are unable to check the erosion in value system, we will not be able fight the cyber criminals simply on the basis of improved technical inputs.
- **Authenticity and reliability of e- content:** By 2030, books will be replaced by e- books and other cyber

contents, teachers by robots catering personalized learning based on artificial intelligence and schools by cozy environment of learner's home place or work station. In such situations, it has to be ensured that knowledge and skills acquired by learners should be authentic, reliable and better serve the purpose based on the objectives of course. Chances of manipulation of contents of course by hackers will be more. If few cartoons picture in NCERT books after many years of publication could create social unrest then just imagine the effect of cyber crimes across the world through e-content of course books. We need to adapting security setup to focus on detection, response, and remediation. That's where the cybersecurity fight is today. In the future we need a proactive approach and move to prediction of what's coming before anything happens.

Although technology has supercharged the learning process from a very young age, there is no guidelines in place for its judicious and ethical use. The rate of its growth and expanse is not proportional to the security measures being taken to keep the information reliable and secure for people of all ages. Everyone on Internet has an opinion, might not be a reliable one, but can be an influential one. When being propagated unchecked, can lead to more harm than empowerment for the young ones and adults alike. As Alexander Pope says so poignantly, "Little knowledge is a dangerous thing". Cyber security and awareness about Cyber security should become as fundamental and easy as being able to use a smartphone. ■



HOW SHOULD GOVERNMENTS PROTECT CITIZENS?

Ambika Khurana, Public Policy - Government and Regulatory Affairs, IBM



Governments face an increasingly complex security landscape. New technologies are ushering in enormous benefits for citizens. They are also exposing citizens to threats- threats that are increasing exponentially.

At the same time, Government bodies are under pressure (greater than ever before) to protect personal data of citizens, resulting in unprecedented investments in information security- both at the Central and State-Government levels.

Most of the first and second world economies have clearly earmarked 30-40% increase in the year-on-year budgets for cybersecurity- to modernize and protect IT across various Departments that deal with citizen data and governance functions.

According to estimates, cyberattacks cost the global economy more than \$400 billion each year. But how serious is the risk posed to the public sector by data breaches and other cyber threats? How can public-sector organizations—large and small—manage digital risks?

Here are five key steps for gauging the cybersecurity “health” of an organization:

Undertake Risk Assessment

Modern threats can manifest in myriad ways. To prepare for a cyberattack, government agencies should conduct a risk assessment to determine where they are most vulnerable and what the consequences of such an attack might be. A thorough understanding of the most likely, the most common and worst possible scenarios will give valuable insights to the government. This will enable the relevant agency to engineer defences that address their unique vulnerabilities.

Open dialogue between security experts and business stakeholders is also crucial, to ensure that everyone—across all levels of an agency or organization—understand how data is utilized and what safeguards exist to keep information secure. It is prudent that Government agencies seek support from global organisations and equip themselves with world class technology solutions that empower the country’s cyber infrastructure.

Devise a Cybersecurity Strategy

Many organizations have crisis plans in place to help them respond to and mitigate the impact of cyberattacks. But as digital threats become more common and sophisticated, leaders must develop a more proactive approach to data security.

Prioritization is an important element of any security strategy. Once an agency has conducted a risk assessment, they can build systems that protect what’s most vulnerable and essential. Because breaches can happen at all levels of government, it’s also important for agencies to develop protocols that can be leveraged by federal, state and local officials.

Further adoption of the globally accepted and respected NIST (National Institute of Standards and Technology Cybersecurity) Framework would help provide robust protection for public-sector organizations and citizens alike, while also reducing the administrative burden and uncertainty for smaller agencies.

Take an Intelligence-led, Analytics-based Approach

Effective cybersecurity can no longer rely on a passive ‘gates and guards’ approach that uses endpoint detection systems that can only identify known malicious activities. By employing advanced analytics systems that incorporate cyber threat identification and intelligence (garnered from suspect behaviour within networks), government agencies will be able to respond swiftly and proactively to digital threats.

Likewise, advanced analytics will empower public-sector organizations to effectively use and manage large volumes of data, rather than suffer from data overload. Such an approach will also make it easier to integrate intelligence-led cybersecurity with new and emerging technologies such as cloud, mobile and social media while protecting confidential data.

Leading global IT majors offer AI (Artificial Intelligence) powered, Cognitive solutions- that should be leveraged for advanced predictive analysis. This will equip the country’s

intelligence-led, analytics capabilities to become empowered to address issues from all possible threat sources.

Increase Stakeholder Collaboration

In the digital age, the role of the individual in cybersecurity has become more important. This is especially true considering the volume of data citizens generate daily on tablets, smartphones and wearable fitness or health-monitoring devices. Citizens need to understand the risks and security protocols when using mobile devices, wearables or operating in the cloud.

Cross-sector collaboration is also crucial. Governments should build upon existing relationships with peer organizations, academia and the private sector when developing security procedures and systems—particularly in the context of cybersecurity R&D and intelligence gathering.

Invest in Cybersecurity Talent

No cybersecurity initiative can succeed without the proper talent to back it up. Unfortunately, many

public-sector organizations are finding themselves short on the skills and competencies required to stave off digital threats.

According to an industry-led research, 42 percent of enterprise security professionals believe they have insufficient budget to recruit and train security talent, and 76 percent say they aren't adequately equipped to conduct threat and vulnerability assessments.

To prepare for the next wave of digital threats, all public-sector leaders must allocate resources to build a strong cybersecurity team. The National Cybersecurity Action Plan should take adequate steps to address the skills gap through strategic investments in cybersecurity education and training. Those deterred by the idea of additional spending should consider the potential cost of a data breach.

In today's data-driven world, a reactive approach to cybersecurity won't cut it. By developing a robust, proactive cybersecurity strategy, government agencies will be better equipped to prepare for, prevent and resolve digital threats into the future. ■

Commander L R Prakash (Retd)
Director – CDAC



Beige suit man- Why do we need indigenous and open source initiative? First is money, this money is going into the software industry. One thing is common to all of them is none of them has an Indian flag. Where is this money going - is it going in the license fee, or research fee abroad then you are directly spending your money in enriching other nations. There is a set of 3 Microsoft products which every PC has - the windows operating system, the patch management system that gets your windows updates and Microsoft Office - they put out disclaimers stating as to what they don't collect. If they see how careful they are in saying of what they don't collect, but basically they are collecting everything else. A combination of these three essentially means they map your entire network; they map your entire organisation, your network and your users.

Brigadier Pradeep Arora
Chairman of cyber security group



If you look at the users today - the users of internet and all the mobile devices are exploding day by day and as the rates of data access have fallen, the users have also moved on from the cities, from the literate population to the people who are semi literate or illiterate. We are forcing them today to use these mobile devices for accessing their own financial assets, accessing their own data as we already refer to it. And as we all are trying to find the solution, there are challenge that citizens are going to face in accessing what is due to them, what is their own and what we as on the side of government want to deliver to them. So possibly one of the solutions lies in providing them a safe environment - maybe we need apps, safe frameworks which can also be made available to children.

IT SECURITY: THE NEW COMMANDING HEIGHT OF THE ECONOMY

Sumitra Goenka

Founder Director- Ratein Infotech India Pvt Ltd & Freshfrugies Storage and Logistics Pvt Ltd



Information technology (IT) has been a progressive field in the development trajectory of the world, and India has been no exception. We are moving towards a digital economy at a faster pace and should continue to do so, to extract the best from the world of IT. When Information technology has become such a crucial part of people's lives through an open network, its security should not be neglected at any cost. Thus, IT security or what we also call as Cyber security, has become the new segment gaining major focus and a forward outlook across the globe.

The urgency in India

According to the recent Norton Cyber Security Insights report, Indians are increasingly becoming aware of cyber threats, but still, they frequently fall victim to cyber-attacks due to complacency. The operation modes used by hackers today to intrude into an IT infrastructure include hard-to-detect phishing and cloaking attacks which create identical looking, fake mirror servers to cheat the users. Clicking on untrustworthy links and responding to emails from unknown sources are the most prominent reasons through which users fall prey to such attacks. A recent cyber breach between May and July 2017 came along with the malware attack on Hitachi Payment Service Systems, which provides banking automation products, ATM and point-of-sale services. The attack affected more than three million Indian debit cards. Authorities were unable to map the origin of attack, the identity of the hackers and the malware technology which caused the cyber invasion.

Last few years have brought a wave of cyber threats coming from varied sources located in different countries. According to the Indian Computer Emergency Response Team (CERT-In), China has been targeting India's cyber space and networks for years; 50,362 incidents numbered in 2016. Amidst the Doklam standoff against China, a cyber war has eventually begun between the two countries. Multiple occurrences of recent high-profile cyber-attacks globally, have propelled India to catch up to its global peers and secure the digital information system. Fortinet, a cyber security solutions provider, conducted a survey for recent years and found that approximately 84%

of India's organizations have fallen prey to security breaches from local and foreign sources in the last two years. It also pointed out that Business executives, especially need to make cybersecurity one of the topmost priorities. However, a ray of hope has been the increased expenditure done by small and medium businesses and service providers on network security.

Recent WannaCry and Petya ransomware attacks on Jawaharlal Nehru Container Port in Mumbai have further alarmed the cyber security providers to create the best firewalls with advanced threat protection capabilities and securing online applications from potential malware. Fortinet further recorded that over 10% of the IT budget of Indian Organizations is being spend on cyber security and the Compound Annual Growth Rate has been 13.5%.

Cyber Security Solutions

Cyber or IT security has now been identified as a crucial field which cannot overlooked to maintain a data sovereignty. New cyber solutions are coming up to reach out to public, government agencies and business enterprises.

With increasing reliance on Cloud storage, services like Cloud security are gaining interest in Indian market along with the efficient costs and flexibility guarantees of cloud storage. A well-crafted cloud security strategy is what we need. This is where cloud security gateways and Cloud security broker system come into action. A cloud security broker can monitor and defend the entire cloud and all the systems within. In a typical government cloud, citizen data is moving constantly, as part of the daily operations. It is important that this data is only seen and accessed by authorized and authenticated systems or users. For example, a citizen's Aadhar card is used as verification by many different Government programmes and systems and third-parties like banks, hospitals, telecommunication, pension, income tax etc. Here, the cloud security broker has the intelligence to detect when data is sent or intercepted in an unusual or unsanctioned manner. If there is an unauthorized user accessing Aadhar information, multiple times over the span of a few minutes and from different locations, it does not fit the normal pattern of access. For this, the cloud security broker could trigger an alarm

and possibly even block access for the particular user for it to be investigated.

Cyber Security need not always be perceived to be complicated and out of layman's ability to comprehend. Simplest of solutions can act useful. From impersonation to credit card information theft, crimes are being committed online every day. Users lose sensitive data and money, suffer invasion of privacy and much more. This is where VPNs come in. A *Virtual Private Network (VPN)* is an extension of a private network across a public network for providing users a secure connection. They are especially very useful in the business world as they allow branches located in different cities to connect to the main office's network safely while creating a cohesive network. Private individuals can easily by-pass censorship, geo-restrictions, and secure their personal identity and location through its usage. VPNs in India can be either paid or free dependent on the services offered in a particular package. Of course, with free VPNs, one cannot be sure of the performance and the number of devices that can connect to it. Paid VPNs are usually very cheap and billed at the end of the month. We can have plans to choose from according to our budget and needs. An increasing percentage of India's citizens are turning to VPN services to enhance their privacy and security in the face of government internet censorship. Based on certain online sources, NordVPN; ExpressVPN; Cyber Ghost VPN; Private VPN etc. have been rated some of the best VPN providers.

Disaster Recovery as a Service (DRaaS) is also gaining momentum in the Small and Medium Enterprises. It is more advisable for these enterprises as they are not financially equipped to support the entire infrastructure. In case any cyber attack strikes, they get an option to create a backup restore and not lose all their crucial data in a go. DRaaS allows a customized subscription and a need-based service. In the past few years of India, the original DR Investment model has evolved into the Cloud Based Disaster Recovery model with emergence of major cloud service providers. Recently, HCL Infosystems collaborated with Sanovi, a technology provider, to bring the best solutions of DRaaS for the customers.

Rising trend of Ethical Hackers

The rising trend of hacking and other cybercrimes has created the need for the Social media giants in the world to employ ethical hackers for information protection and counter attacks. Ethical hacking has grown tremendously over the years in companies like Apple, Facebook, Twitter who are introducing "bounty hunter programmes" for hackers and encouraging them to penetrate their vulnerable systems and rectify the loopholes. Facebook bounty hunter programme was started in 2011 and it rewards hackers who report the worst glitches. Many fin-tech companies in Chennai are also employing ethical hackers to

test the security systems of banks. Telecommunication industry especially has become very vulnerable at present and even amateurs penetrate and steal the database to use for their selfish purposes. In such a case, India needs to focus on the accurate provision of advanced training and employment scope for ethical hacking which can act as the saviour route for our personal and confidential data protection at a mass-scale.

India's policy initiatives to combat Cyber-crimes

In the past few years, India has taken some significant initiatives to strengthen its cyberspace-

- One of the most important is the *National Cyber Security Policy of 2013* which provides the vision and strategic direction to protect the national cyberspace
- The year 2017 followed the formation of Cyber Security Kendras and the *National Cyber Security Coordination Centre (NCCC)* in 2017 which will perform real-time threat assessment and create situational awareness of potential cyberthreats to the country
- *National Critical Information Infrastructure Protection Centre (NCIIPC)* was created under section 70A of the Information Technology Act, 2000. It is designated as a National nodal agency aiming to protect and safeguard critical information infrastructure (CII) against cyberterrorism, cyberwarfare and other threats
- India has entered into *bilateral agreements* with developed nations such as the U.S.A., Singapore and Japan in order to promote research and information sharing on cyber security
- There are plans to set up 10 additional *Standardisation, Testing and Quality Certification (STQC)* testing facilities across the country for the evaluation and certification of IT products

India's strategies and initiatives at the Policy front are commendable. However, in the long run, India needs to transform its greatest asset- the large pool of Skilled IT professionals, to create cutting edge softwares for powering India's technology and not depend on imported technology. Well-known Cyber Security providers like Quick Heal Technologies or Net Protector, who have successfully managed to create a niche for themselves in the foreign dominated market of Norton, Kaspersky, AVG etc. should be customized for developing affordable and accessible protection mechanisms in all sorts of worst cyberattack incidents. Cyber Security can maintain a commanding height in India when its public is fully aware of the impact of science and technology on national security. Event such as US-based Maker Faire, for creative digital workshops and idea propagation, currently limited to IT hubs like Bengaluru, should become a nationwide practice. ■

Jayadeva Ranade

President ,Centre for China Analysis and Strategy & Cabinet Secretariat R&AW.



We have a new kind of warfare in cyber space - sci-war, cyber threats and media. Our biggest challenge other than China is Pakistan. China has set aside \$90 billion for expanding their footprint across the globe for propaganda and moulding the people's mind and extending their reach including the cyber domain. 80% of the main service providers in our telecommunication industry are Chinese companies. Huawei and ZTE complete them and they today cover Bangladesh, Nepal, Sri Lanka, Pakistan, Afghanistan and the Maldives. It is their system that is operating there, whether it is a landline or a wifi. So, we need to really look at it and start thinking how we can set up either a parallel system or a system that in course of time will take over.

We say that we have a problem of manpower, but I will rightly point it out where is this manpower. All our best designers and developers are sitting abroad. We are IT coolies who are living here. We are doing backend operations which are very low end and we need to upgrade that. And the way to upgrade is by starting cyber security, cyber training and cyber awareness.

Hon'ble Shri Shekhar Dutt (SM)
Former Governor of Chattisgarh
Chairman Angika Development Society



Life cannot exist without challenges. There are security difficulties, challenges in technical solutions, but the entrepreneurs and enterprising people will identify those challenges, meet them squarely and come out as a winner. In fact I remember during a discussion at Harvard School, the man addressing young entrepreneurs said that if you don't find challenges on the horizon, go beyond it and seek out challenges and then deal with it. When I used to serve in a desert area, someone asked me what is so unique about the desert. I said that when you go up to a sand dune, you will find another sand dune before you, and you cover that and find another sand dune. So that is the principle of life, you keep meeting new challenges in life and deal with them as you go about. It was a team of young people who had invented the Internet in the mid 30's, and thereafter it was young entrepreneurs who launched various applications for the internet. After the collapse of the Soviet Union, 2 enterprising youths of Estonia found Skype.

Rajesh Kumar Srivastava
Pro Vice Chairman - DPS (Bhagalpur & Greater Ranchi)



There is a contradiction in whether you adopt technology to a limit or not. Technology has taken us in its grip whether we like it or not but there is a need to make our youth aware of the use of technology – both defence and offensive mechanism. I am proud to announce the creation of the first Cyber Forensic Lab machine intelligence analysis across the country with the help of NTRO.

The creation of intelligence agency coordinating the intelligence arms of 3 military services that has long been called for by senior intelligence Indian military officers was formally recommended by the cabinet group of ministers headed by the then Shri Lal Krishna Advaniji. The committee also recommended a national security doctrine that is yet to be adopted. The cabinet group of ministers investigated the various intelligence lapses during the Kargil war and recommended a comprehensive reform of the Indian intelligence agency.

Mr Kaushik Acharya
DPS Bhagalpur



Each morning seems to bring new reports of hacks, privacy breaches, threats to national defence and even shutdowns of hospitals.

As a part of DPS Bhagalpur and Greater Ranchi family I saw Cyber Range in our school and feared the terrible side of Cyber crime.

Fortunately, I got a chance to attend the seminar in General Manekshaw centre, New Delhi along with my students. We saw and thrilled by the presence of some personalities who are back bone of national cyber security.

They addressed many important and burning problems our society facing now a days.

The complexity and trap present in web world well explained. I saw my kids were also no less. They initiated few untouched topics and forced everyone to think. The use of BITCOIN and ONLINE GAMING is a big problem now. Easy availability of Smart Phones and Digital Currency making things worse.

End of the day it was a fantastic experience for all of us. We were lucky enough to share lunch time with those personalities.

We are in safe hands and the next generation developing with command.

Jai Hind. Jai Bharat ■

Dr. Subhasis Kundu
PGT and H.O.D (Biology)- DPS
CBSE School Co-ordinator



During the time of globalization and digitalization of new modern era, the Internet is a huge part of everyone's lives today, including childrens. And if mature, intelligent, sometimes even tech savvy adults can fall for scams online, we can be most certain that a child full of curiosity, but limited in maturity and awareness, can fall victim to the dangers of the internet. The reality is that cybercrime has become more of a threat than traditional types of crime. Some schools may not start teaching about cyber security until middle or high standards. They need to implement soon. You can't always be sure that the problem will start within your own hardware or software systems. If a member of staff or a student has an infected personal device and connects to the schools Wi-Fi this could leave your systems vulnerable to being infected also. Awareness among the school students is a basic need to cope up with this alarming situation. The best method is to give students some supplement materials to read and giving them exposure to a vast range of knowledge regarding cyber security. I hope this book will definitely help the children and make them aware about cyber crime and security.

Priya Kumari
Teacher DPS School, Bhagalpur
and NCC incharge



Cyber Security

Cyber security is the security of the hardware, software and other information from being stolen. It prevents them from any foreign access and saves the documents from hackers due to the increase on the dependence of Bluetooth and wireless networks people make several mistakes which can prove a threat to our life. Therefore cyber security provides us with different aids to work with website. It secretly secures doing mistakes while surfing the internet.

CYBER SECURITY- CITIZENS OF 2030 - Neha Minnat (Teacher-DPS)

On the 27th of September, 2017 the Round Table Conference on "Cyber Security- Citizens of 2030" jointly organized by 'Center for Joint Warfare Studies' and 'Center for Knowledge Sovereignty' and the two schools Delhi Public School, Bhagalpur and Delhi Public School, Greater Ranchi at the Manekshaw Auditorium, New Delhi was a congregation of some extremely distinguished speakers. A few of them who was a part of this meet were-

- Dr. Vipin Tyagi
- Dr. S. D. Pradhan
- Mr. Rahul Agarwal
- Lt. General Vinod Bhatia (PVSM, AVSM, SM)
- Lt. General D. V. Sriketkar
- Lt. General Vinod Khandare
- Mr. Vinit Goenka
- Admiral S. Y. Srikhande
- Mr. Jaydev Ranade
- Brigadier Manjeet Singh

The Chairman of the conference Lt. General Vinod Bhatia is the Director of Joint Warfare Studies. He served 40 years in the Indian Army as the Director General of Military Operations. His focus as a DGMO was on capability development and capacity enhancement. He also has vast experience in Disaster Management. Mr. Vinit Goenka who deserves a special mention as he is the man behind bringing all these very notable speakers together from a wide array of fields. Mr. Rajesh Srivastava and the Principal Dr. Arunima Chakravorty who made it all possible by making this happen for which I am forever indebted.

The speakers were all the chosen best in their respective fields of expertise. It included Defence, Academics, Corporate, Civil actors, Bureaucracy and Cyber Security experts. The topic for the conference "Cyber Security- Citizens of 2030" is a very contemporary and extremely urgent issue that needs to be addressed. The conference and the speakers gave a much needed holistic perspective to the topic. The cyber world being this blind arena of warfare where actual use of guns and machinery are not needed to cause damage and destruction to the one sought. An enemy who sits behind a screen and has access to almost all and every personal information of the possible victim is a reason of much concern and worry. In these times when we expose any and every possible information about our existence to this unknown invisible world through the means of internet is a reason for much worry.

The conference had the delegates reflect and think on the power and capacity of this simple yet extremely powerful weapon called the cyber world. Our naive and simplistic approach to this world is what calls for threat. An informed generation of young minds and a mind that works with caution is what the respected speakers and the conference aimed to bring. We need to sensitize ourselves to the need of the hour by equipping ourselves with a knowledge bank that permits us to an informed and responsible usage of the web. The future of our nation needs to be safe, this is how we make INDIA safe. A simple sim card has the potential of getting you surveilled and noticed by anyone in the world. This is the power of the web.

As a part of the conference I personally had a priceless opportunity to expose myself to all the best minds of our country. An event from which I have a lot to take in. I was inspired and motivated listening to a man who is now doing his third Phd, a man who after taking care of our country's security still finds time to come and motivate young souls like me and my students. That is called a life worth living. A LIFE THAT MAKES A DIFFERENCE!

UTTAM DEY

Coordinator: External Examination
Delhi Public School, Bhagalpur



On 12 May 2017, 200000 computers across 150 countries were attacked by WannaCry ransomware causing prodigious financial loss. Inadequate knowledge of cyber security may cause reoccurrence of similar kind of attacks time and again. Within next three years there will be 635.8 million internet users in India, a major portion of which will be our students who are the future of India. Therefore our students should be endowed with adequate knowledge of cyber security to protect them from the threats they face on the internet. Right knowledge and skills of cyber security will help students to be responsible digital citizens who know how to protect their passwords, personal data and prevent their gadgets to be used as phishing tools. Empowering students with cyber security is a major step to fulfil the dream of "Digital India".

The Student - Parantika Deeksha,
DPS Vasant Kunj

With the growing use of technology and Internet, our lives have become easier and filled with fun but we're unaware of the fact that everything online is decrypted. It's the web we are all stuck in. Many people around the Globe know how to operate device but not all of them are aware of how to keep the data safe and secure. The growing rate of cybercrime in the cyber world is an indication that cyber security is not just an option but a necessity. The cyber world is for us (people) and it must be protected by us. It has become crucial for us to educate ourselves in this field as we are oblivious when our actions online can cause a great threat to us.

The 'Cyber security, Citizens of 2030' conference that was held on 27 September 2017 gave me the opportunity to meet world-class professionals in the field of cyber world. The esteemed panellists not only outlined the perils to individualistic data but also expanded our horizons on the devastating repercussion cybercrime could have on mass database. Lastly I would like to thank the organisers for giving all of us the exposure in this field and making us realise how important it is for us to be aware of our activities online and how a single mistake of ours can give a path to the cyber criminals for committing a major cyber-attack.

Rishi Kalia
An eternal Optimist, entrepreneur



I am highly indebted to Vinit bhai for giving me a lifetime chance to attend such an august gathering that include personalities like Lt. Gen. Vinod Bhatia, Lt. Gen. D.B. Shekatkar and many others who are an authority in themselves when it comes to the topic being discussed i.e. Cyber Security. Are we doing enough to secure our future generations from a threat that looms large as we expose ourselves to the world of Apps, Software, Internet etc. The presence of Students from Delhi Public Schools, Bhagalpur and Ranchi made it all the more interesting as they got their queries answered by the people that matter. I wish and request Vinit Ji to organize many such events in future.

Manish Pant, New Delhi
Media & Communication Strategist



At the outset, I would like to express my gratitude to Vinit Bhai on prevailing upon me to attend the Center for Knowledge Sovereignty (CKS) session on cybersecurity in September 2017. During my years in the media, I have attended several international conferences related to the subject. However, this was the first time that I was attending an event that addressed this very important issue from the perspective of a developing economy like India and the grave present and future challenges in its path. Among other things, the session made me realise how proprietary national data can be compromised to not only endanger a nation's sovereignty and integrity but also manipulate public opinion to create civil strife; a full six months before the Cambridge Analytica scandal broke in the public domain. It was also humbling to learn how highly committed personnel from fields such as the nation's armed forces, government agencies, software companies and academia quietly work in harmony to keep us safe from threats from battleground cyberspace in this era of the Fourth Industrial Revolution.

Shiva Jangid

Cultural, Political, Social Activist



In Yuga of IT, World's information, access has reduced on just finger tips, on dash boards. But at same time it carries a challenge of misuse of Data in terms of Strategy, Defense, economically or target via various ways by within or outside enemy of country.

To Secure interest of our country, India must need its own Server, Internet policy & data network system to ensure safety of data, system and as well secure our Defense lines. Round table conference on "Cyber Security, Citizen of 2030" initiate by DPS, CKS, CENJOWS, PWC & 01 is eye catcher by providing a platform to expert of IT, Academic, Defense & policy makers.

Prof Dr Ashish Gupta

BDS, MDS, DNB , M OrthRCS

FICD, FPFA, FICDE



The Conference held on Data and Cyber security held at Manekshaw Auditorium was the need of the hour given the fact that data control has replaced petrol , so as to be coined the new "DataDollar" and the warfare is "Cybercrime" which has drawn new frontiers in warfare and crime .

This was a brilliant initiative to draw attention to Government of India , Law makers , Defence Analysts , Institutes , Corporates , Health Providers and the Society by and large to the growing importance of Data Security and Cyber Security . Glad to be part of the 1st such conference and contribute to the transformation of New Bharat.

PARTICIPANTS AT THE 1ST ROUND TABLE ON CYBER SECURITY CITIZENS OF 2030

Name	Organisation	JobTitle
Hon'ble Shekhar Dutt SM	Former Governor of Chattisgarh	
Lt Gen Vinod Bhatia, PVSM, AVSM, SM (Retd)	Centre For Joint Warfare Studies (CENJOWS)	Director & Former DGMO
Lt Gen Dr. D. B. Shekatkar PVSM, AVSM, VSM (Retd)	Center For Knowledge Sovereignty	Chairman
Lt Gen V. M. Patil AVSM, PVSM (Retd)	Center For Knowledge Sovereignty	Vice Chairman
LT Gen Vinod Khandare AVSM, SM	Defence Intelligence Agency	Director General
Rear Admiral S Y Shrikhande AVSM (Retd)	Indian Navy	Rear Admiral
Dr S D Pradhan	National Security Council Secretariat	former Deputy National Security Advisor and Chairman, Joint Intelligence Committee, , Government of India.
Mr.Avadhesh Mathur	R &AW	Former Secretary, Cabinet Secretariat of the Government of India
Mr.Jayadeva Ranade	R &AW	Former Additional Secretary in the Cabinet Secretariat, Government of India
Mr.Amitabh Mathur, IPS	R &AW	Former Head Aviation Research Centre
Mr.Rajesh Kumar Srivastava	DPS Bhagalpur and DPS Greater Ranchi	Pro Vice Chairman
Mr.Vinit Goenka	Center For Knowledge Sovereignty	Secretary
Brig Pradeep Arora	Joint Intelligence Committee	Chairman
Brig. Manjeet Singh	DACIDS (DIARA)	HQ IDS
Brig Jai Singh Yadav , VSM	Centre For Joint Warfare Studies (CENJOWS)	
Brig Deepak Malhotra	Centre For Joint Warfare Studies (CENJOWS)	
Brig H S Cheema	Centre For Joint Warfare Studies (CENJOWS)	
Brig R K Bhutani (Retd)	Centre For Joint Warfare Studies (CENJOWS)	
Dr Vipin Tyagi	Centre For Development Of Teleomatics (C-DOT)	Executive Director
Dr B V L Narayana	Centre For Railway Information Systems (CRIS)	Director
Gp Capt G D Sharma, VSM (Retd)	Centre For Joint Warfare Studies (CENJOWS)	
Commander L R Prakash (Retd)	Centre for Development of Advanced Computing (C-DAC)	DIRECTOR
Mr. R Chandrashekar	Centre For Joint Warfare Studies (CENJOWS)	
Air Cmde T Chand (Retd)	Centre For Joint Warfare Studies (CENJOWS)	

Name	Organisation	JobTitle
Capt Ranjit Seth (IN)	Centre For Joint Warfare Studies (CENJOWS)	
Uma Sudhindra	IIM Vizag	Member, Board of Governors
Professor Dr Sharad Sinha	National Council of Education Research and Training (NCERT),	Head,RMSA Project Cell
Professor Chandan Chowdhury	Indian School of Business (ISB)	Associate Dean
Dr Arunima Chakravorty	DPS Bhagalpur & DPS Greater Ranchi	Principal
Dr. Vatsala Joshi Pande	Lok Sabha	OSD (Reasearch) to Hon'ble Speaker
Mr.Pavitrans Rajan	Cyber Security Reaserach Center	PEC
Mr.Bharat Panchal	National Payment Corporation of India (NPCI)	Senior VP & Head-Risk Management
Ms.Sanjukta Mookherji Sahani	JaagoTeens , an NGO	Volunteer
Ms.Sumitra Goenka	Ratein Infotech India Pvt Ltd	Director
Ms.Savita Kakar	DRDO	Scientist F
Ms.Rita Shrivastava	Central Research Laboratory , Bharat Electronics Limited	Member (Senior Research Staff)
Ms.Ambika Khurana	IBM	Government & Regulatory Affairs
Mr.Ajay Ranjan Mishra	Ericsson	Director - Digital Transformation Consulting
Dr Jenny Shabnam	Angika Development Society	
Mr.Tulsidas Bhoite	Lokmat Digital	Editor
Mr.Krishna Kumar Thevar	Economic Times	Journalist
Mr.Nitin A Gokhale	BharatShakti	Founder
Mr.Rahul Aggarwal	PWC	Partner Cyber Security
Mr.Milind Tichkule	Political Activist	
Col Y S Pathania	Centre For Joint Warfare Studies (CENJOWS)	SECRETARY
Mr.Kaushik Acharya	DPS Bhagalpur	Senior Head Master
Mr.Mukesh Chandra	DPS Bhagalpur	Teacher
Ms.Neha Minnat	DPS Greater Ranchi	Teacher
Mr.Aritra Choudary	DPS Bhagalpur	Student
Mr.Hemanjay Harsh Choudary	DPS Bhagalpur	Student
Mr.Deshmani Kumar Das	DPS Bhagalpur	Student
Mr.Yash Dubey	DPS Bhagalpur	Student
Mr.Sanskar Jain	DPS Bhagalpur	Student
Mr.Aananyan Jaiswal	DPS Bhagalpur	Student
Ms.Shreya Jaiswal	DPS Bhagalpur	Student
Ms.Pragya Mishra	DPS Bhagalpur	Student
Ms.Arindam Narayan	DPS Bhagalpur	Student
Mr.Abhishek Kumar Prasad	DPS Bhagalpur	Student
Mr.Naman Raj Sharma	DPS Bhagalpur	Student
Ms.Astha Singh	DPS Bhagalpur	Student
Mr.Sarvjeet Singh	DPS Bhagalpur	Student

Name	Organisation	JobTitle
Ms.Aditi Srivastava	DPS Bhagalpur	Student
Mr.Aryan	DPS Bhagalpur	Student
Mr.Karuna Kumari	DPS Bhagalpur	Student
Mr.Saket Kumar	DPS Bhagalpur	Student
Mr.Yash Raj Mishra	DPS Greater Ranchi	Student
Mr.Abhigyan Pandey	DPS Greater Ranchi	Student
Mr.Vivek Kumar prasad	DPS Greater Ranchi	Student
Mr.Aaditya Vardhan Singh	DPS Greater Ranchi	Student
Mr.Aditya Shaswat Singh	DPS Greater Ranchi	Student
Ms.Parantika Deeksha Srivastava	DPS Basant Kunj	Student
Mstr.Setu Goenka	Modern School	Student
Mr.Manish Pant	IT4Nirman	Volunteer
Mr.Rishi Kalia	IT4Nirman	Volunteer
Dr Ashish Gupta	IT4Nirman	Volunteer
Mr.Shiva Jangid	IT4Nirman	Volunteer
Mr.Paresh Chaudhari	IT4Nirman	Volunteer
Mr.Dheeraj Gupta	IT4Nirman	Volunteer
Mr.Rohit Bhambri	PWC	DIRECTOR CYBER SECURITY

Contents

Introduction ^{p2} / Digital thrust has fuelled cyberattacks ^{p3} / Advanced attacks have targeted India ^{p4} / Key cyber security initiatives launched by the Government of India ^{p6} / Building blocks for a secure nation ^{p7} / Building block 1: Securing government systems ^{p8} / Building block 2: Securing the business cyber ecosystem ^{p11} / Building block 3: Creating a 'cyber secure society' ^{p14} / Building block 4: Building technological and human capacity for cyber security ^{p16}

Creating a cyber secure society



www.pwc.in



Introduction

India has experienced rapid digitisation in the past few years. The increase in digitisation has led to a rise in the inherent risks in the cyber landscape. Attackers are using more innovative strategies to exploit vulnerabilities and launch cyberattacks on governments and other organisations. In India, cyberattacks have been launched to disrupt the social, political and economic balance of the country. Countries such as the USA, China and Russia are building cyber capabilities to steal data, deny services and even stealthily monitor targeted countries. Some nation states have formed cyber hacking groups that aim to steal data from other nations. The growing number of attacks has made sensitive data vulnerable to theft, weakened the fabric of citizen security and also led to monetary losses.

Handling such cyber-related issues with diplomacy is only going to offer short-term solutions. The world is headed for an inevitable cyberwar. It is often rightly said that the third world war will be fought using the Internet and in cyberspace. Amidst this cyber cyclone, it is important to strengthen our cyber defence to ensure the security of citizens and the nation in the long run.

While India has undertaken proactive measures towards ensuring cyber security in the digital landscape, these measures do not scale up to the initiatives undertaken by other countries. The International Telecommunication Union (ITU) assesses cyber security in different countries and ranks them based on five pillars of cyber security: legal, technical, organisational, capacity building and cooperation. There has been a drop in India's ranking on ITU's Global Cybersecurity Index from 6 (score = 0.706) in 2014 to 23 (score = 0.683) in 2017.¹

Faced with imminent risks, India has to further strengthen its cyberspace as the threats are only going to become more severe in the future. This report presents our point of view on how India can address risks and create a cyber secure society.

1. TU. (2017). Global cybersecurity index (GCI). Retrieved from https://www.itu.int/dms_pub/itu-d/obj/str/D-STR-GCI.01-2017-R1-PDF-E.pdf (last accessed on 6 November 2017)

ITU. (2009) Cybersecurity guide for developing countries. Retrieved from <http://www.itu.int/ITU-D/cyb/publications/2009/cgdc-2009-e.pdf> (last accessed on 6 November 2017)

ITU. GCI 2014. Retrieved from <http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI-2014.aspx> (last accessed on 6 November 2017)



Digital thrust has fuelled cyberattacks

1.1
billion

telephone subscribers
2nd largest in the world

Facebook users
Social media penetration

241
million

1.15
billion

digital IDs
Largest digital ID programme

Internet users
2nd largest in the world

463
million

Unprecedented growth in technology has blurred boundaries by connecting people, and transforming the way we work and how governments serve their citizens. Digitisation is enabling the youth to work from their villages, allowing people to give talks at seminars, attend family functions remotely, perform digital *darshan* and transfer money to their near and dear ones instantly. The Digital India programme launched by the Government of India, which aims to provide government services digitally and promote digital literacy, along with building a secure digital infrastructure for the country, is driving this transformation.

Digital trends in India²

Digital payments have also seen an upsurge, with mobile banking transactions alone growing threefold since 2014. It is envisaged that with these initiatives in place, India's digital economy will grow from 270 billion USD to around 1 trillion USD in the next 5–7 years.³

However, this is also opening up gaps which can be exploited. The number of incidents reported by the Indian Computer Emergency Response (CERT-In) was 27,482 till June 2017. Cyber adversaries are becoming more sophisticated and resourceful. The impact of cybercrime is increasing, with attacks growing not only in volume but also in variety. Out of the more than 100 countries that were hit by WannaCry (an advanced ransomware attack),⁴ India was the third worst affected.

Cyberattacks can deliver economic blows, derail India from its projected growth trajectory and worsen relations with our neighbours, unleashing a state of anarchy. ***Considering both the benefits of technology and the need to safeguard against cyberattacks, it is imperative for a growing digital economy like India to focus on cyber security and build a cyber-resilient environment.***

- TRAI. (2017). Highlights of telecom subscription data as on 31st May, 2017 [Press release]. Retrieved from http://traai.gov.in/sites/default/files/Press_Release_No50_Eng_13072017.pdf (last accessed on 25 August 2017)
Unique Identification Authority of India, Government of India. (2017). Retrieved from <https://uidai.gov.in/> (last accessed on 23 August 2017)
Francisco, S. (2017). India becomes Facebook's largest user base with 241 mn users, overtakes US. Business Standard. Retrieved from http://www.business-standard.com/article/current-affairs/india-becomes-facebook-s-largest-user-base-with-241-mn-users-overtakes-us-117071400251_1.html (last accessed on 23 August 2017)
Internet live stats. Retrieved from <http://www.internetlivestats.com/internet-users/india/> (last accessed on 23 August 2017)
Bhakta, P. (10 Aug 2017). Digital transactions in July touch 859.2 million. The Economic Times. Retrieved from <http://economictimes.indiatimes.com/industry/banking/finance/banking/digital-transactions-in-july-touch-859-2-million/articleshow/59994667.cms> (last accessed on 23 August 2017)
Electronic Transaction Aggregation & Analysis Layer. Retrieved from <http://etaal.gov.in/etaal/auth/login.aspx> (last accessed on 23 August 2017)
- Financial Express Bureau. (24 May 2017). India's digital economy set to grow from \$270 bn to \$1 tn by 2024, says Ravi Shankar Prasad. Financial Express. Retrieved from <http://www.financialexpress.com/economy/indias-digital-economy-set-to-grow-from-270-bn-to-1-tn-by-2024-says-ravi-shankar-prasad/682805/> (last accessed on 23 August 2017)
- Kumar, C. (14 May 2017). Ransomware attack hits at least 100 systems in India. The Times of India. Retrieved from <http://timesofindia.indiatimes.com/india/ransomware-attack-hits-at-least-100-systems-in-india/articleshow/58663696.cms> (last accessed on 23 August 2017)



Advanced attacks have targeted India

As cyberspace expands, so do the attack potential and malicious intent. Recently, notorious ransomware such as WannaCry and Petya crippled the security of countries across the globe, compromising several systems. Further, hackers and attackers are defacing websites to revolt against existing policies and promote their own agenda.

a) Ransomware: WannaCry

Cybercriminals took advantage of the EternalBlue vulnerability, wrote the malicious program WannaCry and injected it into the computer systems of many organisations, encrypting their hard drives and freezing whole systems. Among the more than 100 countries infected,⁵ India was the third worst hit nation, with over 40,000⁶ computers affected.

b) Ransomware: Petya

Similar to WannaCry, Petya also exploited the EternalBlue vulnerability to propagate without any user action. However, Petya took a different multi-level approach which was more sophisticated than that of previous variants such as WannaCry. Petya encrypted the master boot record (MBR) of the machine when executed as an administrator.⁷ When executed as a normal user, it encrypted specific files on the system, using several different methods to ensure that it affected as many machines as possible.



5. Kumar, C. (14 May 2017). Ransomware attack hits at least 100 systems in India. The Times of India. Retrieved from <http://timesofindia.indiatimes.com/india/ransomware-attack-hits-at-least-100-systems-in-india/articleshow/58663696.cms> (last accessed on 6 November 2017)
6. ET Bureau. (17 May 2017). India third worst hit nation by ransomware Wannacry; over 40,000 computers affected. The Economic times. Retrieved from http://economictimes.indiatimes.com/articleshow/58707260.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst (last accessed on 6 November 2017)
- PwC. (2017). Cybersecurity alert: WannaCry ransomware attack. Retrieved from <https://www.pwc.com/vn/en/publications/2017/20170516-pwc-newsbrief-wannacry-ransomware-en.pdf> (last accessed on 6 November 2017)
7. PwC. (2017). Petya ransomware. Strategic report. Retrieved from <https://www.pwc.com/vn/en/assurance/assets/pwc-petya-strategic-report.pdf> (last accessed on 6 November 2017)

c) Personal data collection in the guise of better customer service

Smartphone usage has seen exponential growth in the last few years. Billions of mobile applications (such as Facebook, Twitter, Google, WhatsApp, Instagram and Skype) are available for free on Android, iOS and other platforms. Many of these applications access personal information such as photos, contacts, locations and other applications stored on smartphones as a prerequisite to their usage. Once the user data is collected by the applications, the retrieved data is analysed to derive critical information such as monthly expenditure, places visited, online activities, locations where photos were snapped, tagged names on photos, and several behavioural trends and patterns through continuous tracking. In addition, while these application providers may on one hand sell user data to other third parties to generate additional revenue, on the other hand, they may engage subcontractors to perform the above analytics on their behalf, leading to even more severe privacy concerns.

d) Nation state cyber espionage

In under a decade, there has been a rise in cases of nation states exploiting cyber vulnerabilities to breach the critical information infrastructure networks of rivals with the motive of espionage. China's GhostNet program targeted 103 countries,⁸ StuxNet against Iran,⁹ Red October,¹⁰ Shamoon¹¹ and Shamoon 2 malware of Iran,¹² etc. More recently, Snowden's files disclosed that India is among the top five targets of spying by the National Security Agency (NSA),¹³ USA. Also, in 2017, there has been a lot of discussion around the alleged influence of Russia in the 2017 US Presidential Elections,¹⁴ North Korea,^{15, 16} and China's¹⁷ organised cyber-offensive forces, and reported leaks of submarine designs¹⁸ used by the Indian Navy. These reports suggest that (1) specialised cyber teams have been formed by nation states and (2) cyberwarfare is now a reality.

Several developed nations have begun to take serious measures against the growing threats in cyberspace, especially those to interconnected critical infrastructure,¹⁹ and have set up their own cyber command centres.

8. Moore, M. (29 Mar 2017). China's global cyber-espionage network GhostNet penetrates 103 countries. The Telegraph. Retrieved from <http://www.telegraph.co.uk/news/worldnews/asia/china/5071124/Chinas-global-cyber-espionage-network-GhostNet-penetrates-103-countries.html> (last accessed on 6 November 2017)
9. Scarborough, R. (18 August 2013). In classified cyberwar against Iran, trail of Stuxnet leak leads to White House. The Washington Times. Retrieved from <http://www.washingtontimes.com/news/2013/aug/18/trail-of-stuxnet-cyberwar-leak-to-author-leads-to/> (last accessed on 6 November 2017)
10. Kaspersky Labs. (14 January 2013). Kaspersky Labs identifies operations "Red October," an advanced cyber-espionage campaign targeting diplomatic and government institutions worldwide [Press release]. Retrieved from https://usa.kaspersky.com/about/press-releases/2013_kaspersky-lab-identifies-operation--red-october--an-advanced-cyber-espionage-campaign-targeting-diplomatic-and-government-institutions-worldwide (last accessed on 7 November 2017)
11. Mount, M. (16 October 2012). U.S. officials believe Iran behind recent cyber attacks. CNN. Retrieved from <http://edition.cnn.com/2012/10/15/world/iran-cyber/> (last accessed on 7 November 2017)
12. <http://money.cnn.com/2017/09/21/technology/iran-hackers-destructive-new-group/>
13. <https://www.rt.com/news/nsa-india-surveillance-snowden-report-305/>
14. <https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf>; <http://www.telegraph.co.uk/news/2016/12/16/russias-cyber-warriors-should-west-do/>
15. <https://www.csis.org/programs/korea-chair/korea-chair-project-archive/north-koreas-cyber-capabilities>
16. <https://www.reuters.com/article/us-cyber-northkorea-exclusive/exclusive-north-koreas-unit-180-the-cyber-warfare-cell-that-worries-the-west-idUSKCN18H020>
17. <http://edition.cnn.com/2014/05/20/world/asia/china-unit-61398/>
18. <http://www.theaustralian.com.au/national-affairs/defence/our-french-submarine-builder-in-massive-leak-scandal/news-story/3fe0d25b7733873c44aaa0a4d42db39e>
19. <https://www.pwc.in/assets/pdfs/publications/2016/protecting-interconnected-systems-in-the-cyber-era.pdf>



Key cyber security initiatives launched by the Government of India

As forward-looking nation, India has taken some initiatives to strengthen its cyberspace. These include awareness programmes; efforts to create a strong policy environment and strengthen security monitoring capabilities, and international cooperation; and research and development to promote cyber security. Some of the key initiatives are mentioned below:

1. **National Cyber Security Policy:** The policy provides the vision and strategic direction to protect the national cyberspace. The policy was released in 2013.
2. **National Cyber Security Coordination Centre (NCCC):** The NCCC will perform real-time threat assessment and create situational awareness of potential cyberthreats to the country. It was made operational in August 2017.
3. **National Critical Information Infrastructure Protection Centre (NCIIIPC):** The organisation was created under section 70A of the IT Act. It is designated as a national nodal agency in respect of critical information infrastructure protection. It aims to protect and safeguard critical information infrastructure (CII) against cyberterrorism, cyberwarfare and other threats.
4. **Cyber Swachhta Kendra:** Launched in early 2017, the Cyber Swachhta Kendra provides a platform for users to analyse and clean their systems of various viruses, bots/malware, Trojans, etc.²⁰
5. **International cooperation:** Seeking to secure cyberspace, India has entered into nine²¹ new bilateral agreements with developed nations such as the US, Singapore and Japan in order to promote research and information sharing on cyber security. These collaborative efforts will enable India to combat advanced threats.
6. **Promoting research and development:** To promote cyber security across the nation, the government has initiated a programme to offer a public grant worth 5 crore INR to companies responsible for innovation and research in cyber security.
7. **Sectoral and State CERT:** The government has launched sectoral CERTs, starting with critical sectors such as power and finance. Further, state-level CERTs are expected to be created.²²
8. **Security testing:** There are plans to set up 10 additional Standardisation, Testing and Quality Certification (STQC) testing facilities across the country for the evaluation and certification of IT products.

According to the International Telecommunication Union's (ITU) Global Cyber Security Index, India ranked 5th in 2015, but has moved to the 23rd rank among 134 countries in 2017.²³ The security landscape of the country may be further improved with concrete initiatives and learnings from other countries.

20. PIB. (2017). Press release. Retrieved from <http://pib.nic.in/newsite/printrelease.aspx?relid=158620> (last accessed on 23 August 2017)

21. The Center for Internet & Society. (2016). Mapping of India's cyber security-related bilateral agreements. Retrieved from <https://cis-india.org/internet-governance/blog/india-cyber-security-bilateral-agreements-map-dec-2016> (last accessed on 23 August 2017)

22. PIB. (2017). Press release. Retrieved from <http://pib.nic.in/newsite/printrelease.aspx?relid=158620> (last accessed on 23 August 2017)

23. International Telecommunication Union. (2017). Global Cybersecurity Index. Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf (last accessed on 23 August 2017)



Building blocks for a secure nation

Based on an analysis of 60+ countries performed by PwC, the national cyber security strategy is categorised into four building blocks to provide holistic coverage and sufficient focus.



Building a cyber secure nation

1. Securing government systems

Protection of government assets, infrastructure and systems from cyber threats is paramount for the upkeep of our socio-economic health and military might. It is vital for safety, security, growth and sustenance of the nation's economy, protection of its citizens, wealth and infrastructure.

2. Securing the business cyber ecosystem

A healthy and resilient cyber ecosystem is required for enterprises to effectively contribute to the progress of the nation. For this to succeed, all the stakeholders need to collaborate to cohesively contribute to security

3. Creating a cyber secure society

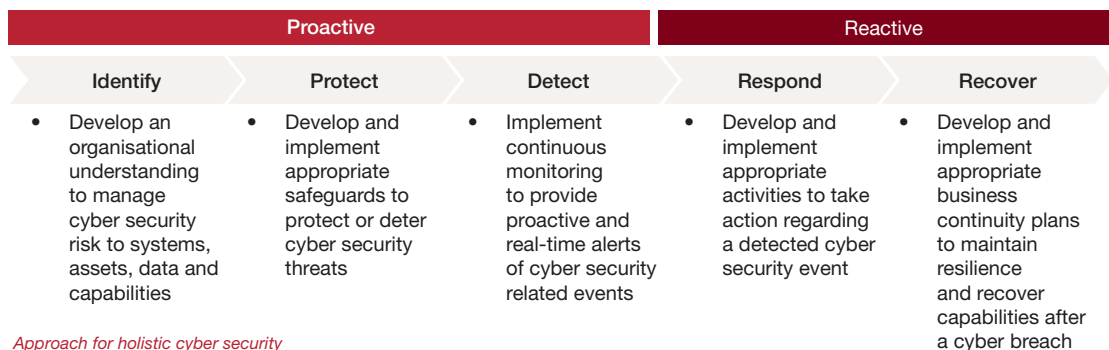
A society driven by cyber-safe culture is less susceptible to cyber adversaries. Creating awareness and training people on cyber security are required to attain a true cyber secure society.

4. Building technological and human capacity

The creation of indigenous tools and human capacity and capability is imperative to not only protect the Indian cyber space but also to make India globally competitive in cyber security.

Building blocks for a secure nation

A robust cyber security approach requires adequate proactive and reactive measures to identify, protect, detect, respond and recover processes across these four building blocks.



Approach for holistic cyber security



Building block 1

Securing government systems

Securing government assets, infrastructure and systems from cyberthreats is paramount for the upkeep of our socio-economic health and military might. It is vital for the safety, security, growth and sustenance of the nation's economy, protection of its citizens and its wealth and infrastructure. Given the sensitivity of data residing with the government, the security of government systems is of utmost importance.

Learnings from other countries

Countries across the globe have taken measures to improve the security of their governments' infrastructure.

EINSTEIN System, Department of Homeland Security (DHS), US: EINSTEIN serves two key roles in federal government cyber security. First, EINSTEIN detects and blocks cyberattacks from compromising federal agencies. Second, it provides DHS with the situational awareness to use threat information detected in one agency to protect the rest of the government and to help the private sector protect itself. EINSTEIN provides perimeter defence for federal civilian executive branch agencies. By the end of 2016, 93% of federal users were covered under this programme.²⁴ This helps in the generation of useful and actionable intelligence, thus helping administrators in identifying the emergencies and priorities and offering information on effective configuration, other than helping US-CERT in generating cross-governmental trend analysis.²⁵

Centre for Protection of National Infrastructure (CPNI), UK: CPNI provides security advice targeted primarily at the critical national infrastructure, where compromise or loss would result in detrimental impacts on the essential services

of the country. The UK has defined 13 national infrastructure sectors and each sector has one or more lead government department(s) (LGD) responsible for ensuring security of critical assets. Further, within the national infrastructure sector, they have defined specific assets as 'critical', whose loss or compromise would result in detrimental impacts on the availability, delivery or integrity of essential services, leading to severe economic or social consequences or the loss of life.²⁷

Continuous Diagnostics and Mitigation (CDM) programme, DHS, US: Federal agencies have been directed to implement continuous monitoring of their IT assets and operational environments. It calls for a three-tiered approach to risk management through defined standards and guidance across organisations, mission/business process and information systems by covering 15 continuous diagnostic capabilities. CDM offers commercial off-the-shelf tools to federal agencies to identify cyber security risks on an ongoing basis, prioritise them based on potential impact and enable their mitigation.²⁸

National Cyber security and Communications Integration Centre (NCCIC), DHS, US: As part of the DHS's information-sharing initiative, NCCIC works with the government and private sector to provide a unified response to cyber incidents. NCCIC integrates the United States Computer Emergency Readiness Team (US-CERT), Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), National Coordinating Centre NCC, NCCIC Cyber Operations Centre (COC), Discovery and Technical Analysis (DTA) and Mission Management (MM).²⁹ It maintains a common cyber platform which provides cross-domain situational awareness for cyber risk.^{30,31}

24. Executive Office of the President of the United States. Federal Information Security Modernization Act of 2014. Annual report to congress. Retrieved from https://www.whitehouse.gov/sites/whitehouse.gov/files/briefing-room/presidential-actions/related-omb-material/fy_2016_fisma_report_to_congress_official_release_march_10_2017.pdf (last accessed on 23 August 2017)

25. DHS. (2017). EINSTEIN. Retrieved from <https://www.dhs.gov/einstein> (last accessed on 23 August 2017)

26. Centre for the Protection of National Infrastructure. Retrieved from <https://www.cpni.gov.uk/about-cpni>

27. CPNI. (n.d.) Critical National Infrastructure. Retrieved from <https://www.cpni.gov.uk/critical-national-infrastructure-0> (last accessed on 23 August 2017)

28. DHS. (2017). CDM. Retrieved from <https://www.dhs.gov/cdm#> (last accessed on 23 August 2017)

29. Zelvin, L. (n.d.). NCCIC. [Presentation]. Retrieved from http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2012-10/ispab_oct2012_lzelvin_nccic-overview.pdf (last accessed on 23 August 2017)

30. DHS. (2017). NCCIC. Retrieved from <https://www.dhs.gov/national-cybersecurity-and-communications-integration-center> (last accessed on 23 August 2017)

31. National Cybersecurity and Communications Integration Center. Retrieved from <https://www.hsdil.org/?view&did=780083> (last accessed on 23 August 2017)



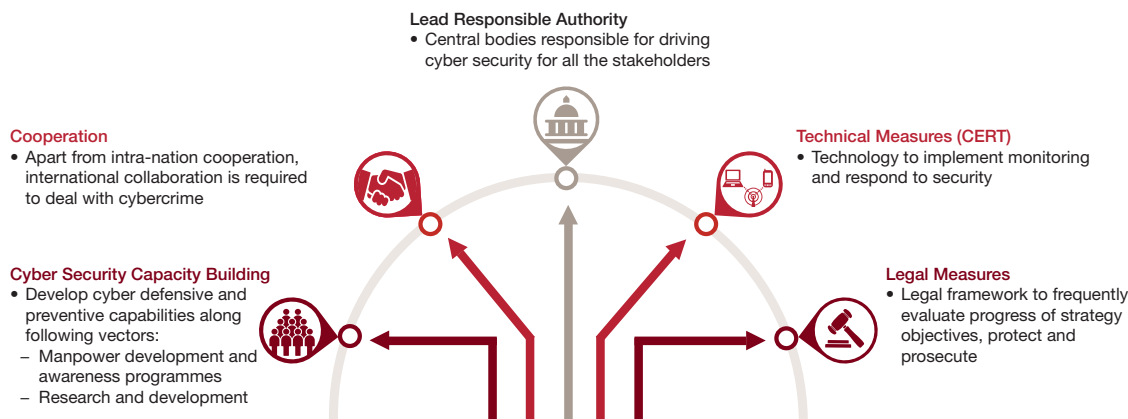
Cyber Star Exercise, Singapore: The Cybersecurity Agency of Singapore (CSA) conducts the cyber star exercise to test the cyber incident management and emergency response plans of Singapore. The scope of this exercise covers all eleven designated critical information infrastructure (CII) sectors in Singapore. This helps in improving the tiered national cyber security response plan which allows for timely response and ground initiatives at the local, sectoral and national level.

Hack Department of Homeland Security Act, US: Introduced in 2017, the act establishes a 'bug bounty programme' to encourage people to come forward and report

vulnerabilities in the government infrastructure. The main objective of this act is to incentivise ethical hackers to report gaps and vulnerabilities in federal systems before others do.³²

Mobile incident response team, Germany: The National Cyber Security Strategy of Germany for 2016 mandates the creation of a Mobile Incident Response Team (MIRT).³³ MIRT is a specialist cyber task force that will provide rapid onsite assistance to address serious cyber security threats on request and with the consent of federal authorities and operators of critical infrastructure.³⁴

Despite variations, common threads exist in the National Cyber Security Strategy (NCSS) key strategy implementation levers of most nations.



Key levers for national cyber security

32. Congress.gov. S.1281 - Hack DHS Act. Retrieved from <https://www.congress.gov/bill/115th-congress/senate-bill/1281/text> (last accessed on 23 August 2017)

33. BSI. (2016). National Cyber Security Strategy 2016. Retrieved from <https://www.enisa.europa.eu/about-enisa/structure-organization/national-liaison-office/meetings/april-2017/170426-bsi-enisa-nlo-presentation-v2.pdf> (last accessed on 23 August 2017)

34. Federal Office for Information Security. (2017). Security in focus. Cyber security strategy for Germany 2016. BSI Magazine 2017. Retrieved from https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Magazin/BSI-Magazin_2017-01.pdf?__blob=publicationFile&v=4 (last accessed on 23 August 2017)



Call to action

We believe that governments should focus on three areas, namely creating a robust policy environment, building capacity and ensuring adequate technology support for government systems.



Governance, policies, procedures and guidelines

- Prescribe detailed policies, procedures and standards encompassing all government infrastructure to provide clear definitions and interpretations of security objectives to be implemented.
- Create and support the building of capacities within user organisations on security skills development and enhancement.
- Conduct periodic and mandatory security assessments of government organisations and their ecosystems to maintain security postures and hygiene.
- Enforce all government departments to report data security breaches compulsorily to nodal agencies.
- Define third-party vendor guidelines for secure cyber practices and adherence to policies, procedures and standards defined.
- Define processes for continuous and real-time monitoring of all IT assets, interconnected networks and operational environments through a central Security Operations Centre (SOC) with advanced analytical capabilities.



Build capacities and capabilities in people to practice security

- Include security-related skills in the job descriptions of government employees by working in close coordination with the Department of Personnel and Training (DoPT).
- Identify and build cyber security skills to protect information systems and assets.
- Periodically brief senior personnel on existing and emerging cyberthreats, trends and directives.
- Create cyber awareness across government organisations and its employees.
- Initiate a bounty programme among citizens to report gaps and vulnerabilities in government systems.
- Grant security clearance and non-disclosure agreements (NDAs) for third parties, vendors working for critical establishments.



Technology to prevent, detect, respond and recover

- Define minimum security features for the hardware and software to be deployed in the government ecosystem.
- Define security reference architecture to be implemented by all government departments.
- Build capabilities and capacity for application, equipment and infrastructure testing through the deployment life cycle to detect any vulnerability and backdoors in the product/technology.
- Design, develop, implement and operate Security Operations Centre for the government with capabilities to detect, respond and recover from any breaches and attacks.
- Strengthen CERT-IN processes and infrastructure for incident response and recovery capabilities to act proficiently on requests from state and central departments/agencies.
- Assess creation of shared data repository infrastructure similar to a secure cloud, to support on-demand requirements of various government agencies to push or pull data.



Building block 2

Securing the business cyber ecosystem

Businesses today face a quandary in today's world of fierce competition. Efficiency, speed to market and customer centricity take precedence, while protection of one's digital assets takes a backseat. However, in this era of digitisation, it is imperative to have a balance between these levers.

There is a need to provide a secure business cyber ecosystem, where governments and national agencies can provide support through an adequate regulatory environment and oversight, while businesses not only follow mandates but help in creating self-regulated environments.

Learnings from other countries

Sector-specific standards: The US DHS has released specific cyber security guidelines for the manufacturing sector, in addition to the National Institute of Standards and Technology's (NIST) cyber security framework.³⁵ Such frameworks also exist for the energy, transportation and the emergency services sector, etc. Laws, regulatory mandates and standards tailored to sector-specific requirements have been created such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA)/Health Information Technology for Economic and Clinical Health (HITECH) Act for the healthcare sector and the North American Electric Reliability Corporation – critical infrastructure protection (NERC CIP) for the energy sector .

Regulatory bodies: The Monetary Authority of Singapore (MAS), as a regulator, released specific guidelines for strengthening system security and risk management for technology-enabled systems of financial institutions within the country. Guidelines have been detailed for the identification and mitigation of risks across broad processes involved in the design and implementation of IT systems.³⁶ Similar guidelines are also released by the Australia Prudential Regulatory Authority (APRA).

Sectoral Information Sharing and Analysis Centres (ISACs), US: The US has also spearheaded the formation of various sectoral ISACs, especially for critical infrastructure. The ISACs collect, analyse and disseminate actionable threat information to its various members along with tools to mitigate the identified risks. There are currently more than 20 such ISACs in the US which have collaborated with each other and federal agencies on joint advisories, white papers and reports, as well as national-level exercises with the DHS and the Foreign Exchange Management Act.³⁷

National Cyber Response Coordination Group (NCRCG), US: It serves as the US government's principal mechanism to facilitate coordination of efforts to respond to and recover from cyber incidents of national significance. NCRG coordinates with various bodies such as the US-CERT, Homeland Security Operations Centre (HSOC) and leverages existing resources for coordination and outreach activity.³⁸

35. DHS. (2015). Critical manufacturing sector cyber security framework implementation guidance. Retrieved from https://www.us-cert.gov/sites/default/files/c3vp/framework_guidance/critical-manufacturing-framework-implementation-guide-2015-508.pdf (last accessed on 23 August 2017)
36. MAS. (2013). Technology risk management guidelines. Retrieved from <http://www.mas.gov.sg/~media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Risk%20Management/TRM%20Guidelines%20%2021%20June%202013.pdf> (last accessed on 23 August 2017)
37. National Council of ISACs. ISACs and their role in critical infrastructure protection. Retrieved from https://docs.wixstatic.com/ugd/416668_2e3fd9c55185490abcf2d7828abfc4ca.pdf (last accessed on 23 August 2017)
38. US-CERT. (n.d.). National Cyber Response Coordination Group. Retrieved from https://www.us-cert.gov/sites/default/files/publications/infosheet_US-CERT_v2.pdf (last accessed on 23 August 2017)



Protected Critical Infrastructure Information (PCII) Programme, US: Established in response to the Critical Infrastructure Information (CII) Act of 2002, the PCII programme is an information protection programme to enhance information sharing between the private sector and the government. Formulated to protect critical infrastructure from cyberattacks, PCII is used by DHS and other government security professionals to assess and enhance security of critical infrastructure and take appropriate measures. Under the programme, federal, state and local government employees and their contractors can access PCII only if they meet a defined set of requirement.³⁹

Government Forum of Incident Response Security Teams (GFIRST), US: GFIRST comprises a group of tactical and technical security response teams who work together to understand and handle computer security incidents and encourage proactive and preventative security practices.⁴⁰

National Cyber Security Drill, Korea: Korea's CERT and Coordination Centre (CC) have been organising cyber security drills for the past 10 years with the aim of testing for security vulnerabilities and developing the capabilities of stakeholders in handling cyberthreats.⁴¹

Cleaner Internet initiative, Singapore: The Infocomm Development Authority (IDA) of Singapore issued the Secure and Resilient Internet Infrastructure Code of Practice (SRII-CoP) in 2011. This code, under the telecommunications regulatory framework, allows Internet service providers (ISPs) and the IDA to make more informed decisions so that early warning to emerging cyberthreats can be developed and appropriate pre-emptive measures can be taken. This was further extrapolated in Singapore's Cybersecurity Strategy that ISPs should to ensure a cleaner Internet and should function as gatekeepers, managing gateways and enabling information flow across the Internet.⁴²



39. DHS. (2017). PCII programme. Retrieved from <https://www.dhs.gov/sites/default/files/publications/pcii-fact-sheet-2017-508.pdf> (last accessed on 23 August 2017)
PCII programme. (n.d.). Non-disclosure of protected CII. Retrieved from https://www.dhs.gov/xlibrary/assets/pcii_faqs.pdf (last accessed on 23 August 2017)

40. US-CERT. (n.d.). GFIRST. Retrieved from <https://www.us-cert.gov/government-users/collaboration/gfirst> (last accessed on 23 August 2017)

41. Sung Jung, M. (28 March 2017). How to organize a national cyber security drill. [APNIC]. Retrieved from <https://blog.apnic.net/2017/03/28/organize-national-cybersecurity-drill/> (last accessed on 23 August 2017)

42. DA. (n.d.). National cyber security masterplan 2018. Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Singapore_2013_AnnexA.pdf (last accessed on 23 August 2017)



Call to action

We believe an inclusive approach is required to create a secure business ecosystem, where the government, industry sectors, standard bodies and business all have to play their role in creating a secure environment.



Sectoral regulator

- Identify the critical assets and processes as well as risks emanating from them.
- Mandate industry-specific processes, guidelines, standards and reference security architecture.
- Prepare and communicate guidelines for incident detection, mitigation and response.
- Create an ecosystem for independent validation and verification of security controls applicable to an entity.
- Mandate the formation of sectoral CERT and drive its operations to ensure security across various entities.
- Create a platform for cyber security information sharing and knowledge transfer among entities in a particular sector as well as across sectors.
- Mandate necessary disclosure of the incidents or breaches in a particular entity in a timely manner.
- Define third-party vendor guidelines for secure supply chain practices such as having NDAs, background checks and relevant security certifications.
- Conduct cyber drills and large attack simulation exercises.



Government

- Create a sector-specific platform with the regulator to coordinate security activities.
- Extend technical and investigative support to entities in the event of a cyber security incident or breach.
- Facilitate coordination and cooperation between sector-specific entities and entities in other sectors for security intelligence sharing.
- Promote organisations or entities that adopt security practices through some sort of funding or incentives.
- Define the reporting guidelines and subsequent disciplinary actions and guidelines for entities in the event of a lapse in security on an organisation's part.
- Promote and assist the standards body to enable them to make sector-specific standards and guidelines.
- Encourage small and medium sector enterprises to adopt cyber security practices by providing incentives.



Standard bodies

- Build the capacity and capability of the standard body to develop sector-specific standards.
- Engage industry bodies, academia, the government and law enforcement agencies to develop and define standards, mechanisms and guidelines which are in sync with the requirements of the industry.
- Facilitate the deployment of standards across various entities in a particular sector by building an ecosystem for its smooth compliance and implementation by handholding organisations to achieve their objectives.
- Sustain and maintain standards on a regular basis by updating them to ensure they remain consistent with technological innovation and security practices.



Building block 3

Creating a ‘cyber secure society’

Citizen participation is key to make any initiative a great success. Responsible behaviour of citizens can pave the way for a strong foundation to create a cyber-safe culture and secure a nation’s cyberspace. A society driven by such a cyber-safe culture will be far less prone to cyberattacks.

There is a need to sensitise both enterprises and citizens regarding their rights and obligations when in a cyberspace. Awareness about secure online behaviours and training people on cyber security topics and best practices can help in protecting people from falling prey to cyber criminals, thus leading to the formation of a secure cyber society.

Learnings from other countries

Cyber Aware, UK: A cross-government awareness campaign to drive behavioural change among businesses and individuals delivered by the Government of UK (Home Office) in conjunction with the Department for Digital, Culture, Media & Sport alongside the National Cyber Security Centre. For wide outreach, this campaign is run using social media.

Stop. Think. Connect Campaign, US: Conducted under the DHS, this initiative is a national public awareness campaign to increase the understanding of cyberthreats and empower the American public to be safe and secure online.⁴³ The key objectives of the campaign include elevating the nation’s awareness of cyber security, engaging the public and communicating approaches and strategies for the upkeep of public safety online. It is associated with nearly 100 network partners to propagate cyber security awareness.

Massive Online Open Courses (MOOCs), UK: MOOCs are offered throughout the year. These are fast becoming popular in the UK as a medium of spreading cyber security awareness among the masses.⁴⁴ More than 25 of UK’s universities have begun offering cyber security courses.



43. DHS. (2016). Stop. Think. Connect. Retrieved from <https://www.dhs.gov/stopthinkconnect> (last accessed 23 August 2017)

44. Cyber degrees. (n.d.) Free online cyber security courses (MOOCs). Retrieved from <http://www.cyberdegrees.org/resources/free-online-courses/> (last accessed on 23 August 2017)



Office of the eSafety Commissioner, Australia: Australia's Office of the eSafety Commissioner provides a range of information and resources designed to meet the cyber safety needs of children, parents and teachers.⁴⁵

- **Pre-service teacher programme:** This programme provides training and education to teachers about cyber safety and enables them to suitably educate their students.
- **Virtual classrooms:** These classrooms cover issues such as cyber bullying, communicating online, the Internet and law, and digital rights and wrongs and cater to children based on their age groups.

ThinkUKnow, Australia: This is Australia's first nationally delivered crime prevention programme. All Australian police forces are part of the ThinkUKnow cyber safety programme. It provides cyber safety presentations that are aimed at parents, teachers and children from grades 3–12, covering a range of topics including sexting, cyber bullying and online child exploitation.⁴⁶

Call to action



Building a cyber secure society

- Encourage and enforce ISPs to provide clean Internet to citizens, which is devoid of any virus/botnet/DDoS malwares.
- Involve the community, civil society, non-profit organisations in spreading cyber security awareness and expanding the reach by identifying the cyber security awareness champions for respective organizations and communities.
- Mandate schools and colleges to provide basic cyber security training to students.
- Decide the most appropriate mode of dissemination of cyber security-related awareness material through social media, MOOCs, electronic and print modes, street plays, etc.
- Organise national- and international-level seminars and workshops in association with industry bodies.

45. Office of the eSafety Commissioner. Retrieved from <https://www.esafety.gov.au/> (last accessed on 23 Aug 2017)

46. ThinkUKnow. Retrieved from <https://www.thinkuknow.org.au/> (last accessed on 23 Aug 2017)



Building block 4


Building technological and human capacity for cyber security

New innovation and cyber norms should focus efforts on creating both capabilities and capacities to defend against latest cyberthreats emerging from paradigm shifts in technology. With the ever-expanding cyberspace, attackers are exploring new and innovative ways to attack technology infrastructure. Indigenous technologies also provide the additional assurance of being secured against vulnerabilities/backdoors in custom products. In addition to technological capabilities, it is imperative to have trained manpower to implement the necessary cyber strategies.

To build technological and human capacities, emphasis should be laid on the creation of niche tools and a workforce that protects the Indian cyberspace.

Learnings from other countries

Research and development (R&D) through cyber security clusters: Several countries across the globe have established cyber security 'clusters' to foster innovation and promote research and development in the field. These clusters are areas with a high concentration of cyber security companies with special incentives and growth accelerators. Some of these cyber security clusters are described below:

	Number of cyber security companies	Salient features
Greater Baltimore Cluster, US	10,000+	<ul style="list-style-type: none"> Government initiatives such as the System for Award Management (SAM), NSA's Small Business Office, FedBizOpps, etc., have helped boost the local industry and have encouraged private contractors to enrol as federal suppliers. Public-private partnerships (PPPs) for commercialisation of intellectual property have helped with the development of niche products.
Hague Security Delta (HSD), Netherlands	400+	<ul style="list-style-type: none"> Promoted collaboration with industry, academia and the government. Created vision 2020 that is focused on making innovation the centre for cyber security, bringing diversity in the field of security (at least 20%) and enhancing partnerships with other clusters.
Beersheva, Israel	250+	<ul style="list-style-type: none"> Attracted about 20% of global private sector investment in the cyber security industry. Leading technology companies have setup up Centres of Excellence in the city in collaboration with Ben-Gurion University of the Negev. It also has dedicated funds for cyber security such as Jerusalem Venture Partners (JVP) cyber labs.
Berlin-Brandenburg cluster, Germany	250+	<ul style="list-style-type: none"> Established cooperative networks, such as security and safety made in Berlin-Brandenburg (SeSamBB), which comprises security experts from multinational corporations, SMEs and university research institutions for interdisciplinary projects in internal and public security.
Ottawa security cluster, Canada	180+	<ul style="list-style-type: none"> Files many patents in the aerospace, defence and security sectors.
UK cyber security clusters	600+	<ul style="list-style-type: none"> Focused on research and development in the field of cyber security.



Law Enforcement Cyber Centre (LECC), US: LECC assists law enforcement, including police officers, digital forensic investigators, detectives and prosecutors to investigate and prevent cybercrime. Some of the programmes include:

- **FBI Cyber Investigator Certification programme:** This is a multi-level online training programme that is designed to teach advanced technical skills.⁴⁷
- **National Initiative for Cybersecurity Careers and Studies (NICCS):** The main objective of the NICCS is to grow the cyber workforce through a robust, searchable catalogue that allows users to find cyber training programmes based on location, delivery method and speciality area.⁴⁸
- **Computer Crime and Intellectual Property Section (CCIPS):** CCIPS provides training to state and local law enforcement, prosecutors and government officials. These trainings are available as online courses and cover various topics such as cybercrime, privacy, computer forensics and electronic transactions.⁴⁹

College of Policing, UK: It works with the police services in England and Wales to provide cyber training and awareness for investigators to increase their ability to understand and respond to cybercrime. Major subjects include managing victims of cybercrime, case file preparation for digital evidence and investigative opportunities of the dark web.⁵⁰

Call to action



Capacity building

- Encourage schools, universities and colleges in defining cyber security courses and subjects.
- Organise summer schools/specialised coaching for students to make them aware of and to promote cyber security.
- Offer scholarships for students pursuing courses in cyber security, specifically those conducting doctorate research in the field of cyber security.
- Organise cyber security-related challenges and competitions at a national level to generate interest and find innovative solutions to cyber security issues.
- Establish cyber security training infrastructure for awareness and skill development. These could also be built by private organisations and could be adequately certified by the government
- Ensure cyber capacity building for law enforcement agencies as well as its personnel.



Promoting research and development

- Set up investment funds focused on cyber security initiatives/start-ups.
- Offer tax incentives and subsidies to cyber security start-ups.
- Create incubation and research centres in collaboration with academia and industry.
- Induce domestic market demand by focusing on key purchasers (e.g. the government, defence, banking, financial services and insurance [BFSI], etc.)
- Create platforms for start-ups to demonstrate their cyber security innovation and technology.

47. Cyber Investigator Certificate Programme. Retrieved from <https://fbi-cicp.cert.org/lms/> (last accessed on 23 August 2017)

48. DHS. (2013). DHS launches NICCS. Retrieved <https://www.dhs.gov/news/2013/02/21/dhs-launches-national-initiative-cybersecurity-careers-and-studies> (last accessed on 23 August 2017)

49. The United States Department of Justice. (n.d.). CCIPS. Retrieved <https://www.justice.gov/criminal-ccips> (last accessed on 23 August 2017)

50. College of policing. Retrieved from <http://www.college.police.uk/Pages/Home.aspx> (last accessed on 23 August 2017)





DELHI PUBLIC SCHOOL
BHAGALPUR



DELHI PUBLIC SCHOOL
GREATER RANCHI



CONFERENCE ON CYBER SECURITY, DATA PROTECTION AND BIG DATA ANALYTICS ANALYTICS BY CKS AND CENJOWS

“It’s important to inculcate the right use of technology in children from an early age”, said the HRD Minister Prakash Javadekar during the release of the Book “Cyber Security - Citizen 2030” at New Delhi recently.

New Delhi, Apr 13, 2018 (Issuewire.com) - “Conference on Cyber Security, Data Protection and Big Data Analytics by CKS and CENJOWS at New Delhi -11th April 2018”

A conference on Cyber Security, Data Protection and Big Data Analytics was organized in Delhi on 11th April, 2018 at the Constitution Club of India, Delhi. The programme was organized by CKS in association with CENJOWS. Union HRD Minister Shri Prakash Javadekar was the Chief Guest of the program.

Many renowned dignitaries of the country attended the conference. Several topics related to the cyber security had been raised in the conference. This is the fourth such conference organised to discuss on the subject.

The Union HRD Minister Shri Prakash Javadekar released the “Cyber Security of Citizen 2030 book” at the event, a collection of articles by various stakeholders. Mr Javadekar emphasized that information related to technology should be given to the children. He urged the public to send in more suggestions as part of the govt.’s move to reform school curriculum. He mentioned that Use of technology in welfare schemes under PM Modi’s leadership has helped India save nearly ₹57,000cr. Use of technology in governance has even helped in curbing cases of fraudulent scholarships, added the Minister. It’s important to inculcate the right use of technology in children from an early age, said the MHRD Minister.

Mr Vinit Goenka, CKS who has been championing the cause of Data Sovereignty welcomed the PM Modi’s decision of localization of Data servers and emphasized on the need to ensure Data Sovereignty, Data Localization and Right to be forgotten.

Lt Gen Vinod Khandare, AVSM, SM (Former DG, Defense Intelligence Agency), Lt Gen Vinod Bhatia from CENJOWS, Former Rajya Sabha member Journalist Mr Tarun Vijay and Mr. Vikrant Khandelwal of ABVP graced the conference. Mr Tarun Vijay spoke about conducting special program for parliamentarians to sensitize them on the subject.

“Overdependence on foreign suppliers of hardware only serves to makes #Indian data vulnerable to misuse and cyberattacks”, said Vice Chairman, Lt. Gen. VM Patil at #CyberandDataSecurity2030 Conference in New Delhi.

“It is up to #India’s younger generation to take the lead in creating appropriate mechanisms to ensure data sovereignty”, said Chairman, Lt. Gen. Dr. DB Shekatkar. He added Despite #India poised to become the world’s largest repository of personal data, proper safeguards are yet to be in place.

Stalwarts such as Microsoft’s Senior Attorney Manager Ms. Meenu Chandra, Mr Anil Bhasin, Regional VP India and SAARC, Palo Alto Network, Shri Bharat Panchal, and SVP and Head Risk Management of National Payment Corporation of India, Commander L R Prakash from CDAC Chennai, Dr Unnat Pandit Operations Head of Atal Innovation Mission, Niti Aayog, and Chinmaya Goyal from Niti Aayog, Mr Ambarish Bakaya from HPE, Mr. Rajat Dhar, Founder of Finogent Advisory, Rear Admiral Sudharshan Shirkhande expressed their thoughts at the conference.

In technical session, Sanjaya Das, former Additional Member of the Railway Board, Dr Janmejay Thakur, Technical Director, National Information Centre as well as former MD of CRIS, Ms. Vandana Nanda also expressed their views. The first panel discussion was Need of Data privacy in the age of emerging technology. Mr. Karma Bhutia, Founder of Ishippo, moderated the debate. Mr. Rahul Sharma, Founder of The Perspective Mr. Tabrez Ahmed, Director of UPES Law School, Mr. Chinmaya Goyal of Planning Commission, Khushboo Jain, advocate Supreme Court, Sanjukta Mukherjee from Jaago Teens NGO and Anoop Chaturvedi of HP Enterprise were also present in the panel. In the second panel opportunities related to big data was discussed by Mr. Kazim Rizvi, from the Dialogue, Dr Avik Sarkar Head Data Analytics Cell, Niti Aayog, Rohini Raina, Managing Partner of Finogent Advisory, Mr.Nirmalyo Banerjee of Aeronube Technology and Mr. Saurabh Rai from Tech Mahindra Business Service.

Media Contact

— Center for Knowledge Sovereignty
— info@cksindia.org



Source : Center for Knowledge Sovereignty- CKS

Categories : Defense , Education , Government , Internet , Security

Tags : #Cybersecurity #DataPrivacy #MHRD #PrakashJavadekar #VinitGoenka #DataSovereignty #India #DataBreach