THE NEED FOR CYBERSECURITY IN INDUSTRY, EDUCATION & GOVERNMENT

CYBER SECURITY & CITIZEN 2030

STRATEGY RECOMMENDATIONS

CENJOWS

Centre for Knowledge Sovereignty

IMC Chamber of Commerce and Industry

CYBERSECURITY AND CITIZEN 2030

STRATEGY RECOMMENDATIONS

THE NEED FOR CYBERSECURITY IN INDUSTRY, EDUCATION AND GOVERNMENT

COMPILED BY

Centre for Knowledge Sovereignty

authorvine

Website: www.authorvine.com
Email: contact@authorvine.com

First Published by Author Vine 2019

Title: Cybersecurity and Citizen 2030
Price: ₹ 599 | $ 9.99
ISBN: 978-81-944894-5-0

Preface

In the past years, the Governing board of Centre for Knowledge Sovereignty has been aspiring to create awareness and educate the citizens of India in the area of data and cybersecurity. In recent years the need for cybersecurity has become more prominent, not only in the requirement but also in the knowledge of the people. The unique demand for cybersecurity is due to its applicability in all areas and industries. As will be seen in the following chapters, the need for cybersecurity varies from the food industry to strategic requirements. In the contemporary world, cybersecurity refers to everything from skill development at school age to protect the countries citizens along with protecting the economy against any attacks or unintentional leaks.

Centre for Knowledge Sovereignty, a think tank, was conceptualised to target discussions and make recommendations in multiple areas and highlight cybersecurity and technology at a national, political and strategic level. The first effort at a large scale that was made by our organisation was in 2017. During this time a set of roundtables under the banner of Cybersecurity Citizen 2030 were held, where multiple stakeholders ranging from school students , academicians, corporates, experts on cyber security to defence representatives were invited, who together deliberated on nation's requirement

for data protection and cybersecurity. The same dialogue and suggestions were made a note of and published in book form in the first Cybersecurity and Citizen 2030 publication. The Publication was released by Union Minister Hon'ble Shri Prakash Javadekar ji and also by Former Chairman of ISRO Padma Shri A S Kiran Kumar ji. Several inputs from the meeting were then also submitted to Justice Srikrishna Committee on Data protection. The list of attendees for this event has been attached in the annexure of this book for the reference of all readers.

Through the dialogue in these roundtables, the governing board of Centre for Knowledge Sovereignty began to seek a compilation on data policies for India and how the sovereignty of the same would advantage the country. In the following months, no such writing was found. A few of my colleagues and a few of the governing members of the organisation decided to write a book to spearhead the idea for India.

In May 2019, the first ever book on the concept of Data Sovereignty in Indian context, "***Data Sovereignty: Pursuit of Supremacy***" was then released in Mumbai and eventually in New Delhi, Bangalore, Pune, Jaipur, Chandigarh. This book has been instrumental in leading India's thought leaders and has been instrumental in driving the nation towards a discussion towards the need for Data sovereignty.

Regarding the venture into cybersecurity and safety of the country Centre for Knowledge Sovereignty and I have insured regular interaction with all governing members and the authors of the book Data Sovereignty. In these meetings

and official conferences like the 2017 Cybersecurity Citizen 2030 discussions have revolved around the increasing need for cybersecurity at a national level. Further, with the recent advancements in different technologies such as Deep Fake technology, and the current limitations in technology that can detect detection in that has increased the urgency in the requirement for protection. These events and the military background that many of the stakeholders share the focus on the imperative need of cybersecurity and a corresponding strategy and policy framework, procurement of ingenious technologieswereat the forefront of all present.

CKS in association with CENJOWS and IMC Chamber of Commerce and Industry, invited stakeholders to discuss about the cyber security strategy looking at the fact that NCSC is also formulating the policy framework in Jan 2020. The meeting again represented the government, education, economy and trade associations. These stakeholders gave their unique views and their experiential and professional opinion on the necessity of cybersecurity.

The collection of the dialogue was then analysed and compiled into a report(MoM) that was then submitted as recommendations to Lieutenant General Rajesh Pant (Retd) at NCSC.

Further, Centre for Knowledge Sovereignty then called for articles from all attendees and multiple other stakeholders which were compiled and have now been published in the Second Edition of Cybersecurity Citizen 2030.

Centre for Knowledge Sovereignty and I hope to encourage greater participation from all citizens of India in our journey

and thus have chosen the name of these roundtables and the corresponding book with great deliberation.

I want to implore all readers to delve into this book to assess the need of cybersecurity on their own reading the opinions of all stakeholders and understanding the variety of industries that would benefit from the same, thus effecting our economy.

Lieutenant General Dattatrey Shekatkar PVSM, AVSM, VSM (Retd)
Chairman at Centre for Knowledge Sovereignty
Former Director General Military Operations
Chancellor of Sikkim University
Head -Shekatkar Committee on Defence.

Note of Thanks

On behalf of CKS and its Governing Council, I take this opportunity to thank everyone who has contributed towards the goal of making India a cyber secure nation. I extend my gratitude to all the speakers, guests, attendees of these roundtables and the contributors of the articles in this compilation. I also thank the research and coordination team of CKS for their relentless effort.

This event wouldn't have been possible without the cooperation of IMC Chamber of Commerce and Industry and CENJOWS.

I hope book will assist the policy makers in designing the new cybersecurity strategy for India in 2020.

I hope we will continue getting the support of all of you in future as well in making India a cybersecure nation.

Vinit Goenka
Secretary
Centre for Knowledge Sovereignty

Table of Content

Articles Written by Attendees

Making India a Cyber-security Superpower: A Vision and Mission

Hon'ble MP Loksabha Anantkumar Hegde
Former Union Minister of State for Skill Development and Entrepreneurship , Currently on Standing Committee on Science & Technology, Environment & Forests of Parliament

India has always been a nation of resilience, knowledge, and truth. Since ages, adversaries that have tried to dominate us and erase our civilization have never succeeded. Our grit, determination, and values have helped us overcome these times of adversity and emerge stronger and stronger. Once we were determined to succeed, nothing could come between us and our goals. This is the spirit we need to channelize to win the war on cybercrime and defeat those adversarial entities that seek to demoralize us and deny us our rightful place in history by bothering us in the cyberspace.

Recently we came across reports of spy software being used on a social media app to snoop on Indians. This episode, along with many others, clearly shows that there are powers out there that are interested in spying on Indians for reasons unknown. When seen in the context of increasing cyberattacks on infrastructure, retailers, manufacturers, and government agencies, it becomes apparent that we are at war. This is a war that we have not initiated, and this is a global conflict that will define the very contours of our geopolitical existence in the days to come.

Understanding the Context

As India celebrated its 72nd Independence Day in 2019, our country is working on multiple fronts to address national priorities, including making growth more inclusive, leveraging our democratic dividend, providing nutrition and food security, and delivering universal access to healthcare, essential services, employment, and sustainable livelihoods. Our government, under the able leadership of Prime Minister Shri Narendra Modi, is doing its bit to address these issues on priority, and cybersecurity is an area that deserves more attention, resources, collaboration, and intervention.

The rising attacks on various digital elements of our economy indicate high levels of interest among groups working to creating disruption, monetizing cybercrime, and furthering the agenda of adversarial items that thrive on shaming states and disrupting economies and lives. These hackers are acting in tandem with forces that are on the payroll of countries that share a similar agenda. Projects that rely on new and emerging tech are being targeted as these groups are aware of the potential that such projects hold to power our digital ambitions and to take the nation forward. Little wonder that projects around smart cities, industry 4.0, connected healthcare, Defense, Space Tech, and others are, therefore, prominently on the radar of hackers.

The Need for Action

The recent trends and research reports that highlight an increasing hacker activity in our systems and networks points to the need for understanding the nature of these

threats and addressing them before they can harm our resources and data. There is an emerging need to secure our growth by adopting a mature cybersecurity posture that negates hacker activity, blocks and neutralizes malware, and prevents an unauthorized leak of data that jeopardizes citizen and national interests.

At the national level, I have identified four areas where we need to take urgent action. These are: strengthening our cyber defense mechanisms, improving our threat research capabilities, improving cyber hygiene, and standardizing security requirements (and linking it with the threat environment we face as a nation).

The malware and hacking tactics deployed by hackers are now getting more complex, stealthy, and sophisticated. Therefore, our response strategies and approaches also have to evolve, adapt, and grow to counter these aggressive cyberspace moves. With critical infrastructure being targeted frequently, the issue of cybersecurity and resilience should attract the highest levels of attention, investment, and intervention from all stakeholders across the nation.

Critical projects falling under such diverse domains as smart cities, surface, sea, and air transport infrastructure, data centers, and defense facilities form the pillars of India's economic wellbeing. Unless we scale up, turn diligent, and gear up to meet the challenge head-on, the full potential of our economy cannot be realized.

Here is my ten-fold plan to address India's cybersecurity needs

1. Build and expand the capacity of Indian businesses to counter cybercrimes using indigenous technologies and security platforms
2. Educate citizens by developing cybersecurity education and making it a mandatory part of various courses
3. Make cybersecurity compliance audits necessary for businesses of multiple sizes
4. Launch a National Cybersecurity Mission that integrates multiple departments, ministries, PSUs and government agencies in their fight against cybercrime; these bodies should be encouraged to share talent, best practices, threat intel, and other means to expand our capacity
5. National Disaster Management Authority should also have the ability to fight cybercrime and attend to a post-cyber attack scenario on critical facilities
6. Enlist and train citizen volunteers to keep an eye on cyberspace and hackers
7. Expand the scope of standards to cover specific areas connected to cyber hygiene such as passwords
8. Collaborate with friendly nations to exchange best practices
9. Work out ways to impose unacceptable levels of damage on hackers or states that attack Indian interests in cyberspace

10. Lead by example: this is an opportunity to showcase India's ability to rise to the challenge and capitalize on the global opportunity (just like when the Y2K bug appeared on the horizon)

The eyes of many generations of Indians presently studying in our schools or taking their first baby steps under the watchful eyes of their parents are on us. They are expecting action and results. This alone should be a strong enough reason for us to act in unison and with zeal to defeat these adversarial actors and their state backers once and for all.

Need for an Effective National Cyber Strategy

Dr S D Pradhan,
Former Deputy National Security Advisor and Chairman,
Joint Intelligence Committee, National Security Council Secretariat

The need for National Cyber Strategy is acutely being felt to provide a sense of direction to all stakeholders, particularly when the information networks and core national interests are threatened by states or non-state actors supported by them. The strategy would also define the goals in a given situation for all stakeholders. Strategic planning is a tool that is useful for guiding decisions and even for evaluating progress and changing approaches when moving forward to deal with serious challenges. Besides, it would convey the resolve of the country to respond to a severe cyber-attack in a manner that would inflict unacceptable damage to the adversary and their supporters and thereby deter the adversaries from harming our interests.

The activities of others using cyberspace shape the current cyber environment. The risks and challenges depend upon the actions and intents of others. The threats in this domain are assuming each day new worrisome dimensions. New methods are being adopted to achieve the objectives of cyber attackers. We are going to face more destructive attacks rather than disruptive attacks in the coming period. And cyber-attacks on our critical infrastructures have the

potentials to damage national security severely.

Given the above, several countries are preparing themselves for offensive operations. A US report suggests that about 30 nations are building cyber warfare capabilities, and more than 130 nations are acquiring 'cyber weapons.' While these capabilities and weapons would change with time, the use of artificial intelligence could significantly upgrade their destructive power. China, which is now using AI in the cyber domain, perceives that the warfare would shift from 'Informatised' to 'Intelligentised" warfare. This would not only change the nature of conflict in the future but also demand structural changes in the armed forces. There is no doubt that the AI-based cyber weapons would be far more deceptive and destructive. The cyberspace has become a new frontier of warfare. As we have to deal with the unique challenges, we need a strategy both for countering the threats and deter our adversaries from launching the attacks because of the penalty that would be imposed on them. In essence, we need a cyber-strategy to neutralise the risks from cyberspace.

To formulate a national cyber strategy, it would be necessary to assess our security environment, which is shaped by the capabilities and intents of other nations. Most advanced countries have developed cyber strategies based on offensive operations for which they have created specialised units. We would need to counter them when the situation arises. Not doing so on the plea that we are not US, China, or Russia would keep us weak and an easy victim of coercion. We should not hesitate to adopt the best practices of others- though taking in view our peculiar conditions.

The reasons for other countries to adopt offensive cyber strategies are not far to seek. Three factors are responsible for this. First, as cyberspace is largely owned and operated by the private sector, controlling cyberspace becomes very difficult. Second, early warnings, like in the physical world, are not possible in cyberspace. Hence it is easier to go in for offensive ops than defensive ops. Third, cyber threats are seen as international attacks on national interests.

A study of the national cyber strategies of the US, China, Russia, and the UK points out certain common elements in their strategy. Three factors are common to the strategy of the countries mentioned above. First, the cybersecurity is perceived as a part of national security and all are accepting the possibilities of cyber-wars. They have listed in their cyber strategies or doctrines several 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 policymakers) to prioritise operations and ensuring that various stakeholders to act as one force. USA's National Cyber Security Strategy states that the security of cyberspace is fundamental for national security and prosperity of its people. China considers that national security is closely linked with cybersecurity. "No national security without cybersecurity", said President Xi Jinping to the state-run news agency Xinhua in April 2014. The establishment of the National Security Commission (NSC) and Central

Network Security (CNS) and the Informatization Leading Small Group, with Xi as their head, also bear testimony to this line of thinking. The Russian cybersecurity strategy identifies cyber-security, privacy, and information security as vital to the national interests of Russia. UK's cybersecurity strategy aims at making the UK as one of the most secure nations to do business.

The second is the use of cyber capabilities to deter adversaries. Cyber operations are not merely seen as supplementing military operations but are also used as a deterrent. US has tasked the Department of Defense to "contribute to the development and implementation of a comprehensive cyber deterrence strategy to deter key states and non-state actors from conducting cyber-attacks against US interests." The US National Security Strategy announced in 2018 makes it clear that the US would respond offensively and defensively when attacked in cyberspace in areas ranging from critical infrastructure to space exploration to intellectual property protection. In China's concept, the deterrence of cyber operations could serve the same purpose as nuclear deterrence in an international environment. The overall Chinese strategy hinges on several military and non-military capabilities including nuclear, conventional, space and information warfare, economic, diplomatic, scientific and technological. It also depends on the collective will of the nation. They all constitute essential components of a credible "integrated strategic deterrent." The Russian strategy stresses the need to have the ability to counter cyber threats and considers cyber operations as a part of hybrid wars. In the UK's cyber strategy, which is available only in

statements of officials, deterrence occupies a key position. The Defence Secretary explaining the UK's offensive cyber operations in his speech at Cyber 2017 Chatham House Conference (in June 2017) stated that 'the UK's National Offensive Cyber Planning allowed it to integrate cyber into all their military operations'.

And the third element is that in all the countries mentioned above, there is a higher thrust on developing domestic capabilities to produce necessary IT products. They are doing away with their reliance on foreign equipment and systems.

India needs an efficient national cybersecurity strategy keeping the evolving cybersecurity environment in its calculus. The recent trends, which have changed the nature of threats in cyberspace, need attention. Strategic deterrence now incorporates a well-defined role for cyber that is likely to expand in the future, and strategic deterrence has begun to play a role in cyber deterrence strategy. Experts opine that it is logically more stable and potentially peaceful to have a system of deterrence that is structured mutually across major powers, giving no one state the ability to disrupt cyber equilibrium. Therefore, our national cyber strategy has to be based on the above three elements. The severe threats are originating from principal adversaries, who could use non-state actors. Hence the need would remain to deal with the principal adversaries, and therefore our national cybersecurity strategy must relate to our national security strategy. This requires not only an effective cybersecurity strategy but the adequate capability to quickly pinpoint the source of an attack and specialised force to undertake

offensive operations to neutralise the source of threats.

Fortunately, India has initiated steps to form the Defence Cyber Agency – a tri-service agency, which would fight wars in the cyber domain and formulate doctrine for cyber warfare. It was a much need step. The government should ensure that this agency is given full support to achieve the objectives. The use of cyberspace for military operations would also infuse jointness among the three Services. The appointment of CDS would further help in integrating the operations of Air Force, Navy and Army.

Though attribution remains a problem, a declaratory strategy with an emphasis on deterrence can dissuade the principal adversaries and groups supported by them from launching attacks on our critical infrastructure or on our core national interests. The National Cyber Security Strategy should indicate in clear terms that any breach of India's cyberspace from foreign actor would be treated at par with violations of our sovereign territory, airspace or territorial waters. We could indicate that our cyber strategy would be based on "Forward Active Defence," i.e. could take steps to neutralise the source and could use any means at our disposal to inflict unacceptable damage on the attacker. We can maintain ambiguity on the actual triggers, and such decisions can be taken later when a severe attack takes place. Simultaneously, we have to encourage research in having the capabilities to pinpoint the source of attacks. With improved investigative techniques and equipment, it should be possible. It may also be mentioned that serious attacks come from the interface of humans and human-computers, and therefore, an efficient counter-intelligence

system could help in pointing the adversary state.

An overarching national cyber strategy also demands a high-powered organisation to take decisions to deter principal adversary, to launch operations, if required, to neutralise the source of threat for the protection of national critical infrastructure and core national interests, to task different entities both government and private and ensure their compliance of directions. It is heartening to note that India may soon have a single authority or agency responsible for covering the entire spectrum of defensive cyber operations in the country for better command and control. It would help in ensuring an integrated approach towards cyber-attacks and achieve synergy between different entities.

And lastly, we should also avoid reliance on the imported equipment and systems as they could have backdoor surveillance tools that could provide critical information to foreign countries. The Parliamentary Standing Committee on Information Technology 2015-2016 had recommended that necessary incentives should be given to domestic companies to manufacture appropriate IT products indigenously. In a time-bound manner, all the organisations and companies should start using indigenous products. This should be given a more significant push now.

Cyber Security and Warfare: Indian Armed Forces

Lieutenant General Vinod Bhatia, PVSM ,AVSM, SM (Retd)

Former Director General Military Operations ,
Currently Director Center for Joint Warfare Studies

"Beyond the immediate, we are facing a future where security challenges will be less predictable; situations will evolve and change swiftly; and, technological changes will make responses more difficult to keep pace with. The threats may be known, but the enemy may be invisible. Domination of cyberspace will become increasingly important. Control of space may become as critical as that of land, air and sea. Full scale wars may become rare, but force will remain an instrument of deterrence and influencing behaviour, and the duration of conflicts will be shorter."

Prime Minister Narendra Modi in the Combined Commanders Conference - October 2014.

Prime Minister Modi's clear and categorical directions to the Combined Commanders of the Armed Forces is indicative of future threats and challenges to national security. The security challenges for the nation can no longer be defined and definite, as these are varied, conducted in many battle spaces by multiple means driven by a collective ideology , plausibly without any direct attribution and

without any overt physical military application of combat power ab-initio. " Domination of Cyberspace will become increasingly important" is a direction of the Prime Minister, unfortunately we as a nation and the armed forces have not done enough to translate the directions to capabilities.

Globally, 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 believed 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, Pakistan and China being active participants. Georgia, 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. India has been the target of of nearly 1852 attacks every minute in 2109 as per a report published by Indian cybersecurity research and software firm Quick Heal. 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. Future wars will be multi-domain multi-dimensional wars waged in many battle spaces across the full spectrum of conflict. Cyber will be the critical factor and the nation with asymmetry in cyberspace will be vulnerable to this low cost high affect warfare.

Cyber Threats – Indian Context

As far as India is concerned, our two adversaries, China and Pakistan pose major challenges in cyberspace, though the cyber threat is all pervasive and can manifest from any source, state and non state. China has set aside 90 billion US dollars for information war in the cyber domain . It is believed that the PLA's strategic cyber command is integral to the PLA's Strategic Forces Command, structured to integrate all strategic domains available to the state and directly controlled by the Central Military Commission. It has approximately 1,30,000 personnel on its rolls and pool of additional 2.5 million people who have the basic education and skills 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 India's 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. It is also rumoured that the major power grid failure in north India followed by Eastern parts of India in July 2012 including Delhi was a cyber attack engineered by China possibly to check the capabilities. During the recent Doklam standoff Chinese cyber activities were directed towards India as part of its information warfare, an important component of the three warfare strategy of PLA. 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 companies manufacturing electronic and telecom products in India.There must be on overhaul of existing rules and regulations with the aim to eliminate Chinese products from critical areas. At present it is near impossible to procure any ICT equipment which is not sourced from China. It is common knowledge that all such equipment has embedded security risks.

The threat from Pakistan is again significant, though their technology prowess is less than China, the motivation levels against their 'eternal enemy' India 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 cyberspace 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 or compromised is minimal especially if working from another country.

National Cyber Security Strategy and Structures

Twenty seven ministries in the government of India are presently dealing in Cyber with varying priorities and funding. Rajeev Bhutani in a Cenjows paper on A Comprehensive National Cyber Force Structure For India writes " India's response to cyber threats so far has been reactive and fragmented. India"s Department of Electronics and Information Technology (DEITy), under the Ministry of Communication and Information Technology (MCIT) released the country's first ever National Cyber Security Policy (NCSP) on 02 July 2013. As regards cyber infrastructure, there are as many as six agencies at the apex level, which are dealing with cyber security management: National Information Board (NIB), National Security Council Secretariat (NSCS), National Crisis Management Committee (NCMC), National Disaster Management Authority (NDMA), National Cyber Response Centre (NCRC), and National Technical Research Organization (NTRO)". India needs to create formal structures and

organisations to ensure optimal cyber usage and security. With new technologies like Internet of Everything, Big Data Analytics, Artificial Intelligence, Machine Learning, Blockchain, Robotics/Autonomous vehicles are all driven by Cyber space, the key question is are we as a nation future ready. We have over 400 million internet users but lack in critical infrastructure, legal provisions and regulations, security consciousness, secure and sovereign data farms. We have multiple cyber threats which are all encompassing and can target all our sectors from defence to financial, government, transportation, power, media and industry etc.

There is a need to evolve an all encompassing comprehensive national cyber strategy, which defines national objectives, and addresses the security concerns and threats to the nation and in particular thedefence forces and operational preparedness and plans. This Strategy should dictate capability building and enhance existing capacities for an effective cyber defence of the armed forces. An effective cyber defence policy and organisation will have to function in concert with all other government departments and organizations under the overall policy framework of the NCA. Defending the territorial integrity of India in land, sea and air and safeguarding the national interests and assets is the constitutional mandate of the Armed forces. As present and future security threats are multidimensional and multi domain including the all critical cyberspace, the armed forces will have to ensure a secure cyberspace and

exploit it as a tool for deterrence.

There is imperative that we create structures and systems which enable a secure cyberspace and exploitation to ensure a modern and prosperous India. PM Modi's national initiative of DIGITAL INDIA can only take shape if we have the requisite cyber security and cyber technology structures. India needs to create a National Cyber Agency (NCA) by an act of parliament which will be an autonomous body with the requisite authority and funds to govern and administer all aspects of cyber. The NCA should be self funded, even at an additional one rupee per internet user per month there will be adequate funding for this agency. The NCA will be responsible for cyber security in all its domains and also for creating critical infrastructure and self reliance in the mid to long term. It will be much more than a mere regulatory body. On similar lines the states too could create their respective State Cyber Agency which should follow the guidelines and instructions of the NCA. In affect the National Disaster Management Authority model exists and can be replicated with suitable modifications to meet the national cyber security needs.

The three critical aspects of cyber security are people, process and technology. There is a continuous effort to plug gaps in these 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 Cyber Agency created in 2019, 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. However, the present organisation fall short of meeting even the present day needs leave aside the future threats and challenges.

Challenges for the Armed Forces

The cyber domain is huge and there are going to be 500 million internet connected devices by 2020 in India. Cyber capabilities are also a major factor of deterrence much like a nation's nuclear and conventional military capabilities. The Internet has also become a weapon for political, military and economic espionage.The dependence of cyberspace by the military makes it a vulnerable domain for attack by inimical elements. 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 raising of the Defence Cyber Agency security will improve and procedures will be streamlined.

The Indian Armed Forces 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 should 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 cyberspace. 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 an optimal 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.

Most mega armed forces like United States, Russia and China have raised cyber commands with a huge number of cyber warriors who are both professionals and possess an unmatched passion for cyber war fighting. Most Western

countries like the UK, Germany and the Netherlands have also entrusted this responsibility to their defence forces. There is an urgent need to establish a tri-service Cyber Command as envisaged by the Naresh Chandra Task force and the Shekatkar Committee, which should function directly under the Chief of Defence Staff who will be a single point of contact to Cabinet Committee on Security (CCS). It should be headed by a three-star general (CinC) from Army/AF/Navy. HQ Cyber Command will have a real-time coordination with NCA and all other organisations. It will be responsible for both Cyber Defence and Offence.

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 cyberspace. 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. Deterrence cyber capabilities are not discussed in open domain, but it goes without saying that this aspect should

be the mandate of Defence Cyber Agency, as a purely defensive approach is a recipe for disaster. However, to be effective we also need a dedicated and trained workforce, build a cyber culture in the armed forces and have lateral partnerships with other cyber agencies, industry, academia and experts 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.

(First published as CENJOWS paper)

Securing Our National Interests in Cyberspace: Winning The Game

Lieutenant General Dattatrey Shekatkar PVSM,AVSM, VSM (Retd)
Chairman at Centre for Knowledge Sovereignty
Former Director General Military Operations
Chancellor of Sikkim University
Head -Shekatkar Committee on Defence.

Hostile forces frequently launch cyberattacks on Indian projects, infrastructure, and websites to violate our security, data, and I.P. and social harmony. In the past, they have used the Internet to incite violence, spread misinformation, harm our digital interests, and incite acts of sabotage against society and promote an environment of terror and confusion in the country.

A constant attempt is also being made to recce our defense installations and other sensitive areas to gather information to keep an eye on us. Adversarial entities are deploying hackers who are well versed in breaking into systems deployed by us.

Fake and malicious news reports spread on the Internet during episodes of geopolitical stress or even elections, or some social tensions harm national sovereignty, interests, and security and the rights and interests of organizations and individuals. We know that a nation with adversarial intentions is using the services of social media manipulators

well-versed in local languages. Those hired are also better aligned to exploiting differences of opinion prevailing here.

When combined with cyberattacks and the spread of malware, misinformation becomes a force multiplier for hackers and their/state/non-state actors.

Countering cyberattacks

The trouble starts with deciding which adversarial hacking activity to counter. There is right now a focus on defending preset silos concerning servers and infrastructure of significance to the country. This strategy has, however, failed to deter or halt the major threats our nation faces. Increasing reports of snooping by our neighboring nations bent on mischief and to monitor our troop movement bear testimony to this.

Chinese hacking group APT40 is ahead of the curve in this regard. Though having operated as a military intelligence-gathering operation mostly focused on traditional maritime targets since 2013, they have been expanding their operations globally since at least 2017. In this duration, they have managed to compromise numerous systems, including those of universities, to steal high-end research. APT40 has repeatedly targeted engineering firms, research institutions, and defense contractors working on naval technology in the U.S., probably to help China's own undersea weapons research catch-up with the West. This includes theft of original research before it is classified, potentially putting

Beijing in a position to out-innovate the U.S. military. China is relying on using U.S. academics' fundamental research gains to supplement those of their universities. While posing a national security dilemma for the United States, these academics are not in a "critical industry" and are often culturally resistant to security-related oversight that might impede their work.

Our strategy to counter them should take into account these factors:

- **Time**: how soon can we detect and counter these attacks?
- **Intent/determination mapping**: how do we know why they are attacking us (is there a specific reason or they are just testing the waters?)
- **Tactics**: what exactly are they doing, and how?
- **Targets**: who or what are they attacking?
- **Teams involved**: are these state actors on their payroll, or they are mercenaries.

Once we have information on these aspects, then we can frame a coherent and timely response. The response should be on these lines:

- Detection and neutralization of the threat and the associated risk
- The attacks should be graded based on severity and complexity into pre-determined categories
- The response to an attack should be mapped to the above point. The severe the attack, the stronger

should our attack be

- Finally, we should have means to asses the damage caused by our response; at the bare minimum, we should be able to shut down the infrastructure used in the attack

PROTECTING DIGITAL SOVEREIGNTY IS VITAL

Nations are already acting to curb the movement of fake news within their jurisdiction. They have understood the need to act fast to deter criminals and disruptive elements.

Nations that are facing current and potential risks in cyberspace, have to ensure that the strategies are designed to ensure better management of cyberspace. They should also ensure that the management models remain up to date and aligned to the shifting realities around us. Germany has approved a Social Media Regulation Law according to which social media services that are unable to control hate speech, harassment, and fake news for any reason can be fined up to 50 million Euros.

Australia is planning to fine ISPs and social media entities up to 10% of their annual income or up to three years imprisonment for the managers concerned for failing to remove banned content in time.

Egypt's new Anti Fake News Law allows agencies to monitor individual accounts on social media having over 5000 subscribers.

Thailand's Cyber Security Law mulls 7 years of

imprisonment for people disseminating fake news. The Philippines considers falsifying news as a criminal act that is punishable by six months of imprisonment and a fine of almost 3,000 USD.

Singapore has cleared a Protection from Online Falsehoods and Manipulation Bill, which stipulates that people who spread fake news with malicious intent or to harm the public interest could face imprisonment of nearly ten years and fines of up to 1 million SGD.

The U.S. Department of Commerce can now ban American businesses from doing transactions with foreign companies that seek to harm the U.S.

We must understand that fake news is not just a "government problem". It is a problem that impacts society as whole and shapes the thinking of the future generations. Several initiatives in a multi -pronged approach across sectors will have to be taken up to prepare our citizens for an extremely dynamic digital landscape.

In India, the Press Information Bureau has already set up a unit to counter fake news. This unit needs to be strengthened. There is an element of crowdsourcing involved in the effort, and that is an encouraging development unless we broad base the project; its effectiveness will always be below potential.

At a strategic level, for battling fake news in the country, the government has laid out four principles — find, assess,

create, and target (FACT). Initially, the government's FACT check module is going to be manned by Indian information service officers. The officers will trace online news sources and publicly available social media posts round-the-clock for any potential fake news. They will also monitor posts by social media influencers to ensure that fact-checking hygiene is maintained and adhered to while sharing information online.

Make winning a habit

It must be every Indian's responsibility to protect our national interests and democracy from fake news assault.

To win the game, we need not just have to beat the enemy but also stay ahead of his ability to harm us. This ought to be executed in a consistent and dedicated manner. We also need to be aware of new actors who will emerge on the scene in the future. The web is a constantly evolving mesh of information and ideas, and just like other human endeavors, this will also have a dark side to it. Our goal should be to shrink the space available for illegal activities by constantly neutralizing them. We should secure this space as a platform for innovation and evolution of our stature as a digital superpower with ample room for every Indian citizen to realize her dreams.

Neutralizing Cyber Threats: Evolving an Offensive Defense Strategy

Lieutenant General Venkatesh Patil, AVSM, PVSM (Retd)
Former Director General Military Operations,
Vice Chairman, Centre for Knowledge Sovereignty

We have to admit that when it comes to fighting cybercrime, the emphasis today is overwhelmingly on containing cyberattacks and associated strategies. However, the world we live in today is a more challenging one. With the volume of attacks against businesses and critical infrastructure is growing in double-digit figures, can we look at adopting a more robust posture to deter and 'waste' hackers efforts?

Integrated effort

Hackers and adversarial groups working across continents and timezones are launching a relentless attacks on us. These attacks are designed to keep our resources and bandwidth tied and wear us down in a war of cyber attrition. The hackers are backed by state and non-state entities that have deep pockets and employ highly trained and motivated digital world mercenaries, who will stop at nothing to harm us and our national interests.

As we speak, our adversaries are launching attacks on us through social media, fake news and psyops, designed to demoralize the nation and to force citizens to commit errors

or to be their agents for creating disruption. The money that is siphoned off in ransomware attacks and social media blackmailing is often used by these criminal elements to keep up the attacks on India.

Cyberattacks are growing in every sphere of digital operations, be it IoT, IT, and operational technologies. Equipment, people, and infrastructure in industries as diverse as oil and gas, manufacturing, telecom, smart cities, and others are attacked through sophisticated malware.

EARLY DAYS

Like other new and innovative technologies that came before it, techniques based on IoT, AI and machine learning are right now going through its initial adoption phase in India and elsewhere. The immediate questions asked include: can we hive out a manual process? How do we improve data transmission speeds? Is it possible to make our machines learn? When the answer is yes, the solution, in most instances, is a fresh and new technology that is deployed for the first time. However, the rush to adopt and use these new possibilities has left many CISOs encountering a growing challenge in the way of security.

Our industry and allied sectors are still getting used to these technologies and are on the first stage of the learning curve.

Over the last few decades, Supervisory Control and Data Acquisition (SCADA) systems have played a significant role in industrial operations. Industries like oil and gas, energy/smart grid, agriculture, manufacturing, and utilities have implemented SCADA systems and networks to collect data and automate processes, and are looking to automation

systems for more effective ways to operate. Attacks on such critical infrastructure could cause billions in damage. As a result, some businesses will find it challenging to get back on their feet.

In the last five years alone, mass rapid transit and power and water systems across the globe have been attacked and shut by hackers. These attacks are designed to manipulate the behavior of the masses and, inflict unacceptable damage to the economies of the countries involved. Attacks on sizeable critical infrastructure systems like the command and control setup of a smart city could disrupt the scale that we have never seen before.

Moving towards a holistic approach

The threat of cybercrime is today an omnipresent one and is growing in both complexity and scale. Theirs is no one particular approach that can eradicate all risks. The evolution of the cyber landscape that surrounds and our growing dependence on technology across sectors places data protection at the front-of-mind for businesses of all sizes, industries, and nations. For attaining and maintaining a successful cyber deterrence posture, the focus should be on a cyber-risk management strategy that reduces risks, protects assets, data, and people and goes a long way in making us less attractive a target for our adversaries.

Our ability to immediately detect an attack and then efficiently and effectively respond to it is the most crucial step in mitigating possible financial, reputational, or compliance damage. We should also look at ways in which we can deflect these attacks using technologies such as

honeypots to deflect and study such attacks.

Every cyberattack, if appropriately deciphered, can yield a wealth of information on the source, type, and origin of attacks and the motivations of hackers and the groups that encourage them. Such data must be used to suppress the appetite of these hackers, to cause harm, while inflicting unacceptable levels of damage on their hacking infrastructure.

Components of an offensive defense push

- Multi-sectoral coordination to strike back at hackers
- Degrade their ability to attack as also disarm their malware and other weapons of disruption
- High investments in understanding not just the weapons or actors but even nation-states and the psychological makeup of the minions that indulge in cyberattacks at the behest of these adversarial states
- Impose a high cost on our cyber adversaries
- Use deflective technology to channel attacks away from the core and critical infrastructure
- Engage Indian cybersecurity companies and academic institutions in this effort

The road ahead

Given our push to delve into new economies such as Blockchain, IoT, Fintech, gaming, and artificial intelligence to push our digital dreams, we will see further investment geared towards upgrading our digital and IT infrastructure. We need to couple such initiatives with an equally forceful and impact-driven cybersecurity awareness campaigns

and complementary programs to promote and strengthen cybersecurity in the private sector.

The most important action item on our agenda should be inter-agency coordination to put up a joint front against disruptive elements. We should also build capacity in our academic institutions and rope in the brightest minds for this endeavor.

We need to take up the up-gradation of our cyber response tactics and strategies on a war footing. Our adversaries should be given a clear message. They should not be given any opportunity by our actions. Instead, our cyber posture should be threatening and combative enough, to force them to give up releasing any malware into our cyber space.

Strategy for Cyber Resilience in Aerospace Sector

Air Vice Marshal Pranay Sinha, VSM (Retd)

Advisor, CRL (Central Research Laboratory) BEL.

Introduction

Aerospace and Defence companies are especially vulnerable to cyber threats because of the sensitive nature of the industry and the stakeholders involved. Hackers in this domain are often more sophisticated than those in other sectors deriving their motivation from different sources. Cyber- attack/ Breaches here have significant security consequences at national and regional levels. With India expanding its domestic aerospace production capacity, this sector needs to be accorded a new degree of attention and resources in addition to planning and support from stakeholders connected with the eco-system. Important is to focus on cyber resilience, that means post cyber-attack, need is for rapid response to mitigate it,contain the disruption, and then qucikly to ressurect and restore the services.

Cyber Attackers in the Global Threat Environment

Cyber Attackers / Hackers are often foreign nations. Sometime they could also be other defence component suppliers, targeting intellectual property to advance their defence preparedness and to improve the quality of their weapon systems. They are usually part of Advanced

Persistent Threat (APT) groups (like those uncovered in China) that are highly sophisticated, motivated, well-funded, and highly strategic in their single-minded pursuit of sensitive and actionable information. Such groups can carry out attacks that are wider in scope and more catastrophic than those of the average business hacker, who is often just looking for bits of personal or corporate information to sell on the dark web.

APTs seek to:

- Collate classified information to enhance their technology and weapons.
- Gather intelligence to infiltrate or even subvert the defence mechanisms of other nations.
- Develop countermeasures (strategic and tactical) for the technology of other nations.
- Produce weapon systems to sell in the expanding global weapons market.
- Compromise defence contractor supply chains by targeting third-party partners.
- Gain economic advantage.

India has also seen plenty of interest from hacker groups based in various geographies. Most of the attacks are aimed at our websites though many target critical systems and subsystems, including data dumps as well.

Significant Breaches

Breaches in the Aerospace and Defence sector don't receive as much news coverage as attacks on commercial businesses, as most of them are never disclosed.

Nevertheless, there have been significant breaches in the recent past, indicating the global prevalence of this menace. Shared here are a few US organizations that have suffered a violation of classified and proprietary information due to cyber attack.

- **Airbus, 2019.** Airbus' commercial jetliner business was hit by a data breach this year. This gave intruders direct access to the personal information of some employees. There was, however, no impact on aircraft production, and to this day, the hackers' intentions remain unknown.
- **Insider Attack**. A former contractor working for once of the intelligence agencies pleaded guilty to pilfering classified material from the CIA, the National Security Agency, the US Cyber Command, and few other agencies. Some experts speculate that the information leaked was used in developing the WannaCry ransomware, used in various attacks in 2017.
- **RSA in 2011**. The company dealing with crypto systems was breached, and a set of Secure ID token seed values that are used to authenticate remote access were taken out. This episode, in turn, led to a cascade of additional breaches at other companies, which included Lockheed Martin, Boeing, and General Dynamics.
- **Boeing in 2018.** The leading aerospace company suffered a ransomware attack on some of its manufacturing equipment, led to a slow down in the production of its 787 Dreamliner and 777 wide-body

jets.

In addition, systems connected to aerospace in countries as diverse as Russia and the UK were consistently hit by hackers from around the world.

Types of Attacks

APT groups tend to explore different ways to cause a breach. Listed here are four of the most common attacks observed in the recent past:

- **Phishing**. It is a familiar and easily perpetrated attack type whereby an attacker pretends to be a trustworthy individual or group in order to deceive the target. Phishing usually occurs via an email or a phone attack to lure the target to click on an email or share sensitive information. This click could end up exposing the whole network and information flowing through it. Though less common, phishing can also occur through a physical attack. An attacker could pose as an employee to get past security and gain access to a critical facility. Thanks primarily to social media and available information publically on websites, it's quite easy to trace the personal and company information, and branding information needed to make an email appear authentic. After an employee clicks on a link mentioned in an email or gives away sensitive information including passwords, malware or ransomware can be downloaded onto his or her machine and legitimate passwords used by the hacker to log into other vulnerable systems. The hacker then proceeds to defeat the company's security protocols

and control systems to gain access to more classified information.

- **User Password.** Password guessing is a common technique used by attackers to quickly uncover relatively simple and weak ones through the use of automated guessing tools. Businesses can enhance their protection by enforcing the use of highly complex alpha-numeric passwords or even multi-factor authentication methods that are less likely to be guessed by any means.
- **Third Parties**. Irrespective of a company's cyber security maturity, its interactions, and exposure to third party applications and emails can expose it to significant risks. To avoid this, companies should, at all times, evaluate the supply chain and vendors before they get access to any company information or websitesor servers.
- **Rogue Employees.** Sometimes, employees can pose as a insider threat to the company and the industry itself. Threat actors often recruit agents in order to steal data before and after they join a company that is of interest to them. Monitoring and alerting security teams on anomalous behavior and interactions in employee activity can aide in reducing the likelihood or severity of a breach.

Cyber Resilience Strategies

Here are a few steps a company or a government agency can take to enhance security and controls.

- **Strategy to Reduce the Phising Risk .** Even highly

trained and competent employees can be easily deceived by the convincing psychological tactics deployed by hackers in email phishing scams. The use of antiphishing software can aid in identifying malicious emails through the use of algorithms that scan email content and attachments before they are opened. When the software finds a suspicious email, the program removes it from the recipient's mailbox and alerts the IT team to investigate.

- **Cyber Security Awareness.** Companies should necessarily encourage employees to use complex passwords that are updated frequently and not used anywhere else. Other steps companies should deploy are as follows:
  - » Preventing the use of software systems that don't have the provision for a sophisticated level of password security.
  - » Passing a mandate making passwords for sensitive operations to be changed periodically.
  - » Password sharing and the use of system default passwords should be discouraged.
  - » To strengthen these measures further, companies should also ask users to change their passwords at least every 90 days.
  - » Periodical Cyber Security Awareness Training programme needs to be conducted.
  - » Regularly Table TopExercicses should be conducted wherein mesure to contain/ mitigate multiple type of attacks should be practised.

Cyber security needs careful planning and the involvement of motivated staff. Hiring an experienced leader or C-suite person to lead and drive security efforts can help in encouraging participation across all aspects. Employee awareness training is also critical. For most security frameworks, such as the National Institute of Standards and Technology (NIST) 800-53, of USA recommends annual training on the detection and management of suspicious emails. This standard can be used as guidance to reduce the likelihood of a compromise even in India.

- **Regular Technology Upgrades and Updates**.In addition to meticulous planning and organizational awareness, many technology safeguards can help with cyber security. To list a few common ones:
  - » **Multi-factor Authentication**. The use of two-factor authentication adds a layer of complexity to the authentication process by requiring the use of additional code or token delivered to or generated from a smartphone application or a key fob. Businesses that require more stringent security needs may go for a three-factor authentication. This method goes way beyond the traditional twin-factor authentication by needing a biological verification that could include a thumbprint or retinal scan.
  - » **Patch Management Programs.** As developers deploy software updates, they introduce unintended bugs that can present new vulnerabilities. Sometimes these vulnerabilities

are quite well known. Thus threat actors will try and exploit them. Hence, companies must locate and address these vulnerabilities rapidly. Along with staying abreast through technical bulletins and peer-to-peer exchange of knowledge, teams can use scanners and other commonly available tools to aide companies in identifying and prioritizing vulnerabilities. Once a vulnerability is identified, a patch should be immediately assessed and applied from a centralized system and a team to ensure a systematic and automated program should be deployed to patch any further exploitable vulnerabilities promptly.

CONCLUSION

Today for Aerospace and Defence companies, Internet Technologies is a must for optimising their organisational decisions making and in incresing their productivity through speedier information transcations. But, at the same time vulnerability of data theft and frauds have increased manifolds as stakes are very high. Therefore, need is to focus on resilience strategies as only cyber security is not enough. To realise this aim one of the most important contributing factor is conduct of regular Cyber Security Awareness Training programme for the company employees along with other measures as suggested above.

Growing With and Through Cyber and Data Security: A Roadmap

Mr Vinit Goenka

Secretary, Centre for Knowledge Sovereignty (CKS)
Member Governing Council - CRIS, Ministry of Railways, Government of India.
Former Member IT Taskforce - Ministries of Shipping, Road Transport & Highways, Government of India

India is at an exciting phase of growth. Today while we are counted among the largest and most significant markets in the world, we are also the largest repository of talent and skills. India's digitization and last-mile engagement projects are among the best in the world, and the explosive growth in data traffic in the last few years has shown that our appetite for digital growth has only been unleashed. Much more is yet to come, provided we channel our energies and diligence in deploying appropriate measures to grow and sustain this growth for generations to come.

Priorities

As a nation with a large landmass, population, and one with strategic interests spread across a wide swath of land and seas, India is bestowed with unique challenges the country is trying to address. Our remarkable progress in the last two decades has led to our infrastructure, manufacturing, healthcare, and defense sectors expanding to cover our aspirations as a nation. This, coupled with the digitization and digital transformation of industries and sectors, has made us vulnerable to a myriad of problems.

Critical infrastructure protection

Critical infrastructure is defined as systems, networks, massive data storage mechanisms, and assets that are so essential that their continued operation is required to ensure the security, socio-economic well-being, and governance continuity of a nation. By their very definition, these assets are essential for the country and its citizens.

In the past, the only means of defending these assets in the real and virtual space was isolation. Physical security meant that physical assets were access controlled. The same applied to digital assets in the virtual space where security managers used to hide such assets behind layers of firewalls and airgaps. Hackers soon found out ways to breach such systems rendering such protection means vulnerable.

States that have adversarial intentions against India seek to target our economy and capital investments by targeting our critical infrastructure through cyberattacks. These attacks are happening at two levels viz., reconnaissance – wherein malware is released that profiles the network and systems and an actual attack wherein the malware unleashes its destructive power by stealing data, shutting down services and systems or even erasing firmware or other information.

Consequently, a fresh approach is needed to secure critical infrastructure against new threats and innovative and motivated hackers.

Data privacy and sovereignty

Just like a nation has the first right of usage over the resources that exist within its borders, a similar right should ideally extend to the internet too. The primary owner of

all data created by someone is the person who created the data. The government can and should, in instances where there are implications for national security, be able to access this data. The Personal Data Protection Bill tabled in parliament introduced in the Lok Sabha recently is a step in this direction. This bill is meant to ensure that the citizens of the country retain control over their data. We will also need to work towards implementing a privacy and data management framework along with a robust framework for personal data governance.

Growing from strength to strength

In the year 1995, when India was negotiating what was then General Agreement on Trade and Tariffs (GATT) proposals on Intellectual Property, the nation had to deal from a position of need. Thus, it had to accept specific terms and conditions that were not in complete alignment with what we wanted to in a sector as vital as agriculture.

Cut to the year 2019, India decided to opt-out of the Regional Comprehensive Economic Partnership (RCEP) due to concerns around protecting our manufacturing and agricultural sectors. We chose to bargain from a position of strength, and when our conditions were not met, we decided to move on gracefully.

In statecraft, as in cybersecurity, strength leads to influence and negotiation power. No force on earth should be able to bring us to our knees. We should instead be able to dictate terms, protect our national interests and data. Cyberattacks leading to breaches will make us weak and reduce our credibility and standing.

On the other hand, by warding off attacks and imposing punitive damages on hackers and states backing them, not only do we send a strong message to the hackers and their patrons but in the process enhance our standing and expand our influence. Our strength in the world of cybersecurity will also enable us to provide a conducive and safe environment for businesses and individuals here to grow and rise to their potential.

ITS TIME TO GIVE A CLARION CALL

In the years to come, we will not be measured by our potential but by what we have achieved. A young nation that is home to over a billion dreams will always have high aspirations and ambitions. It is up to use to work towards futureproofing these dreams, and these are some of the initiatives we have to undertake to do that:

- Focus on indigenous R&D through incentivization; this will help Indian companies secure Indian assets, infrastructure, and IP and reduce dependency on foreign entities
- Develop the whole supply chain cycle from chips to cloud storage in India to avoid supply chain poisoning
- Enhance the qualitative and quantitative capacity building efforts of Indian academic institutions so that we can enable the evolution of cybersecurity talent that can meet the skill and talent needs locally first and then globally
- Develop and deploy a 10-year cybersecurity vision and roadmap for the next decade
- PSUs should be encouraged to pool resources to

develop and implement a joint cybersecurity action plan

- Streamline defense procurement to hasten the adoption of the latest tech

The Implications of Data Analytics on National Security

Mr Bhola Nath Sharma (Retd)
Former Inspector General, Border Security Force

In the last few years, the term 'big data' has become an omnipresent buzzword in the academic and professional circles and the media across the globe. Some commentators called big data as 'the new oil of the 21st century', 'the world's most valuable resource' and 'the foundation of all of the megatrends that are happening today, from social to mobile to the cloud to gaming.'

The exponential growth in big data analytics can be explained from a market-based perspective. On the supply side, data have become more readily available, and processing power has kept increasing—as predicted by Moore's Law in the 1970s. Rapid advances in instrumentation and sensors, digital storage and computing, communications, and networks, including the advent of the internet in the mid to late 1990s, have spurred and an irreversible march towards the 'big data revolution,' generating, transmitting and giving access to more and more data. Humans directly or indirectly create as much as 2.5 trillion megabytes of data each day today, and the numbers are only growing.

As increasingly large amounts of data are captured from humans, machines, and the environment, the temptation

to analyze them grows, a phenomenon sometimes known as datafication. The current deluge of data, spurred by the increased digitization of information, provides countless opportunities for data mining, a set of techniques seeking to extract hidden patterns from datasets in a variety of contexts. These new capabilities have started affecting organizations and the core processes they follow.

Interest in data analytics has been growing due to the demand for more valid intelligence products following the controversies caused by the 9/11 attacks and the absence of weapons of mass destruction in Iraq. Before 9/11, the US intelligence community lacked and missed specific pieces of information pointing to the terrorist plot. In 2002, a national intelligence estimate made a series of erroneous assessments regarding Iraq's WMD program, which were later used to justify the US decision to go to war in Iraq. These events cast doubt on the intelligence collection and analysis capabilities of the US government, especially in the domain of human intelligence (HUMINT), and increased the pressure on senior decision-makers to adapt intelligence processes to an increasingly complex security environment. Big data capabilities, it was hoped, would compensate for the limitations, and sometimes the absence of HUMINT.

Consequently, intelligence agencies around the world began to embrace more systematic and sophisticated data collection and analysis techniques. Given the widespread use of the term 'big data,' one would expect to find a new account of what it means, what it does, and how it works in the national security context. However, the field of security studies has, thus far, paid little attention to this concept.

THE CHARACTERISTICS OF BIG DATA: VOLUME, VELOCITY, VARIETY, AND VERACITY

The expression 'big data' is often understood as a set of enormous datasets. But what exactly qualifies as an extensive dataset? Volume is interpreted and processed differently in multiple fields and at different points in time. For a social scientist, a dataset including hundreds of thousands of entries may seem significant, but would not appear so to a computer scientist. Similarly, while computer scientists might have considered a database of hundreds of thousands of entries to be very large in the early days of computing, today's researchers work with billions of entries.

A 2010 study found that the amount of data produced globally was 1.2 zettabytes or 1,200,000,000,000 trillion gigabytes. It is expected that by 2020, worldwide data production will reach 35 zettabytes. The desire and ability to process such large volumes of data constitute a significant component of the definition of big data, but capacity alone is not sufficient to define big data. Early descriptions of big data describe how large amounts of data put heavy demands on computing power and resources, thus causing a 'big data problem.' As the world keeps producing more and more data, this problem is still with us. Processing capabilities for all these data now lag behind storage capabilities. In other words, we have access to massive amounts of data but are not able to use them all. Volume, therefore, should be considered not in isolation, but concerning the ability to store and process data. The definition of big data must comprehend not only numbers or volume but the capacity to use these data.

In a narrow sense, counter-intelligence and security aim to protect intelligence agencies against penetration by adversary services. A broader and more universal understanding of counter-intelligence and security encompasses defense against significant threats to national security, including espionage, but also terrorism and transnational crime. One security application of big data analytics, specifically through NLP capabilities, is the identification of malicious domains and malicious codes (malware) in cyberspace. Automated data analytics can be used as a part of broader systems to defend computer networks. In the field of cybersecurity, network-based intrusion detection systems monitor internet traffic, looking for specific signatures or codes that deviate from the norm or have already been identified as malware. Such systems help analysts to spot advanced persistent threats and automatically block cyber attacks. Cyber attacks take place at the speed of light, and this raises interesting questions about the diminishing role of humans in national security decision-making. When network intrusion detection systems analyze vast amounts of data to block cyber threats automatically, big data analytics effectively replaces humans. Yet significant data capabilities are not a panacea, and the inability of algorithms to take into account the broader context of an attack can make it hard for machines to detect social engineering scams on their own.

Conclusion: To date, security studies researchers have not explicitly defined or instituted a framework for assessing the significant data phenomenon. To fill this gap in the available literature, I have explored the characteristics,

technology, and methods of big data and have situated them in the context of national security. Our exploration of big data in traditional intelligence activities—requirements, collection, processing, analysis, dissemination, and counter-intelligence and security—suggests that technological advances have allowed security professionals to collect and process more extensive and more diverse amounts of data, sometimes rapidly, so that they can be analyzed and intelligence can be disseminated more effectively. These strengths, and the limitations of traditional intelligence disciplines like HUMINT, explain why big data tools have played an increasingly dominating role in the national security processes.

Looking Glass: Stemming Cross-Border Communal Harmony Disruption Attempts and Curbing Social Media Pollution

IPS, 1996 Ajay Yadav

Inspector General, Communications and IT, Central Reserve Police Force

Disagreements are an inevitable component of democracy. No two individuals often agree on everything. So when one extrapolates this paradigm to the level of a nation as big as India, it can be gathered that there will be social chasms and more extensive disagreement of opinion on various issues among the masses. As a nation, we are mature enough to discuss and arrive at a consensus on most occasions or even agree to disagree. That is symptomatic of our democratic credentials and a testimony to the resilience of our people. The problem arises only when a state actor or actors with adversarial intentions try to fan emotions in the guise of a local and incites people to disrupt and destroy.

The backdrop

In the seven decades of our existence as a model democracy, we have often taken pride in displaying our democratic credentials. While our neighbourhood saw coups and armed uprisings, India remained an island of peace with every single transfer of power being done peacefully in adherence with the will of the people. In times of war or peace, the nation often resorted to debates and discussions to examine

matters threadbare in a peaceful manner.

With the arrival of newer means of communication and enhanced connectivity, such conversations intensified with each side of the discussion adopting these new tools to influence the other. In the background, other entities backed by states(s) saw an opportunity to widen the chasm by injecting fake news, misinformation and outright lies to fan communal violence to keep our law enforcement agencies tied up and to discredit the government of the day at the state and central levels.

We have seen innumerable instances of this happening in the last one year. There was an instance of social media mercenaries paid by a certain country in our neighbourhood tweeting in Marathi just before elections on a topic that had polarized the people of Mumbai. The tweets were coming in at regular frequency and contained local nuances and messages. The exercise was carried with a degree of precision and diligence designed to maximize the objectives of the parties involved.

In the UT of Jammu and Kashmir, mobs are being motivated and incited through social media, instant messaging channels and by circulating morphed pictures and fake stories. This is being done on an industrial scale with the participation of hoards of paid minions from across the border and a few locals who are acting as the eyes and ears of these handlers who are running these social media sweatshops.

There are innumerable such examples. In many cases, our response has not been up to the expectations of our citizens and agencies connected with defending our national interests.

THE BATTLE FOR PERCEPTION

Today's conflicts are fought for wining minds and to create the right impression. If you can promote the right images for yourself or your cause, then a big part of the battle is over. You just need to ensure then that this perception is managed and sustained across social and online touchpoints for the target audience.

We have our neighbouring nations indulge in a battle for perception time and again. Many of these battles are directed against India and to show the country in poor light. Active and casual social media users turn into unwitting allies in this game. The key to winning geopolitical skirmishes lies in managing the perception internally within the country and outside.

THE NEED FOR AN INTEGRATED STRATEGY

To win the battle of minds and to keep disruptive elements at bay, we need to understand the tactics deployed by them and counter them in cyberspace and beyond. The following are some of the tactics that we can implement to defeat them:

Build focused teams to study the tactics, strategies and messaging adopted by the other side. This should necessarily include their motivations, objectives and the width and depth of their activities

We need to have a social media intelligence unit that monitors the social media activities of nations with adversarial intent and responds appropriately in a very short time

Both these teams should come up with an activity guide and set of responses to contain the adversarial activity

Use active social media users and influencers to promote trends that are favourable to us and drown those that are against

All responses should be timely, measured, to the point and framed to counter a specific tactic deployed by the other side

Social media or IM activity designed to fan communal disharmony, destabilize financial markets and to lower our standing in the world should be contained on priority

Increase the cost of operations for them by countering them and not letting them attain their objectives

Law enforcement agencies should monitor the activities of people who are aiding the narrative of the other side. It is essential to ascertain if people from those countries who are on visit visas here are indulging in mischief

Generate awareness on such activities and bring citizens on board on every initiative where their help is required

These measures are just the first few steps. With sustained and determined efforts, the nation can go a long way in leveraging social media to improve our perception, convey truth and contain elements that seek to misuse communication channels to spread communal discord and vitriol.

Cyber Security - Challenges & Solutions, especially In The Indian Context

Brigadier Navdeep Brar

DDG RTG(UP & UK) Indian Army

Ladies & Gentlemen it gives me immense pleasure to be part of this **Round Table Initiative organised under the agies of CENJOWS & CKS for the year 2019.** Having been a part of the proceedings last year one realised that a lot of targeted work needs to be executed towards achieving the stated objectives. A host of positive steps have been taken since last time we all met here &its also a pleasure to see many familiar faces.

I will take this opportunity to touch upon a few relevant issues and leave behind a few thoughts for us.

Privacy

The issue of **Privacy of the individual and our organisations,** which have to employ the medium of Internet, looms large. The Internet as we know, consists of the **visible spectrum, the not so visible portion, also called the Deep Web and the so called Dark Web.**

Hacked - It is said that the connotation of being Hacked comes only in two shades - **either you have been hacked, or, you don't know that yet.** And as was brought out last time by one of the speakers, that if an app or web service is

free, then be rest assured that you are the product.

For most of us, our **personal information** - o**ur Friends, Photos, Financial info, Medical Records, Voice samples - be it with Siri, Google or Bixby, our Phone Calls, our Texts, our Fingerprints, our Iris scans - all of it is already there.** Its too late to retrieve this information - hence the protection of this information, the privacy of this is of concern to us. **All or any of this information can be garnered together, if and when required - more so if and when we become a POI (Person of Interest).**

Privacy serves a purpose, that is why we have blinds on out windows & doors. But today the moment u search for one product to buy, see the kind of **targeted bombardment of ads** that are thrown in your face for the next ten days. Finally the product, including the colour choice that you make may not be yours.

Hence, **maybe there is a case in point to be out of the clutches of the Visible Spectrum of the Internet, to employ a Neutral encrypted protocol to protect basic Privacy.**

Response Mechanism

The response mechanism in case of a Cyber Attack needs to keep the **OODA Loop as given by Col John Boyd,** to the fore. Things are happening faster than the Human Brain can comprehend and take effective counter-measures. **Warfare kind of Mindset…Attacker vs Defender** is what is required. Pilots, Ex- Military personnel, when Cyber qualified, men with such backgrounds are in demand.

Cyber Attackers are an organised sector today. They

work regular 9 to 5. Have regular holidays. This years **Ransom Attacks** were initiated on Friday evenings, to get back on Monday mornings, to see the results. Figures of more than **4000 Ransom attacks per day** are being cited for the year 2019.

Artificial Intelligence (AI)

AI augmented engines like the prototype, Mr Watson of IBM are in. Mr Watson goes through the events, co-relates them, detects suspicious activity, sounds the alert. AI can see the **propagating pattern, trace the threat, identify the threat and address the issues faster.** Presently its the optimum fusion of Man and Machine. The next logical step of course is **Machine Learning.**

AI training is a complex process - by feeding of loads of data and associative learning, a point of self learning is reached. **Training brings Structure** - at one point you stop the hand holding and let AI progress - learn from Analysis.

Advantages of AI being employed to **identify potential trouble makes** are unique. **China** has begun to construct a digital authoritarian state **by using surveillance and machine learning tools to control restive populations,** and by creating what it calls a **"Social Credit System".** Several like-minded countries have begun to buy or emulate Chinese systems. A point that need a note is that, **AI could also be used by Cyber Criminals. Hence the growing importance of Cyber Warriors.** We are looking at over **2 Million Cyber Security jobs by 2020**. However this is a field where **Passion scores over a College Degree** - it being an **Applied Skill** Set. Its neither a Blue Collar or a

White Collar job, but a New Collar type of job.

China has set its vision to be the World leader in AI by 2030. It has major implications, both Military and Non - Military. Recently I read an analytical piece about operations in Georgia, Ukraine and Syria of **Capitalisation on Deception, Psychological Manipulation and Domination of the Information Domain.** Imagine how better these operations can be executed with AI in these domains. **Fear of AI exceeding Human Intelligence and escaping Human Control has a possibility of disastrous consequences.Deep Fake,** as seen in its nascent stages has a game changing impact, which is of concern.

Everyone has a Role

Everyone of us have a role play. **Follow Cyber Hygiene, Update Software, get the Security Patches in time, keep Passwords complex, install the latest Anti-Virus**, including your smartphones. Take certain active measures by not clicking on links, Malware can be embedded by any means, **monitor the systems, watch out for screens going blank for no apparent reason, go for two factor authentication, layers of security.**

Way Forward

The first steps toward the Way Forward have been taken by us in **identifying the issues involved in securing our Cyber interests.** Identification of the multi faceted contemporary threats and the likely path of the Cyber Attackers, both State and Non State, is the way forward to shore up our Cyber Defences. **The most Critical Security Data has to be on Servers that we have direct control**

on, and physically present here and not in other nations. Yes we do understand the various levels of **encryption** but there always is a question mark attached. Getting the **best brains to sit together, exchange concepts and work out a systematic Response Mechanism** is the way forward. **Dynamic Defence is the key in this ever evolving domain. Like the Flight Simulator Emergency Training, proactive response, esp to a Cyber Attack has to be practised, rehearsed, got into our Muscle Memory.**

National Cyber Security Strategy : A Suggested Scope

Brigadier Pradeep Arora,

Former Chairman, Cyber Security Group DDP, DRDO

Introduction

National Cyber Security Strategy(NCSS) shall impact the Cyber security environment in the country in near and mid term. It is important that the strategy acts as an enabler and guides the security effort across entire spectrum of assets and activities impacted by Cyber domain.

Primary endeavour of the NCSS should be to ensure unrestricted use of cyber space to further national aim.

In this paper it is proposed to propose a strategy, various pillars and discuss other important issues important for enunciating a cyber security strategy.

Overarching Reach of Cyber Domain

The cyber domain extends across multiple technologies and mediums. It impacts almost all sectors of our economy. Today, it is also entwined into every facet of an individual's life. Unrestricted access and ability to exploit the cyber space is thus important for both military and civil applications. Denial of its use to inimical agencies is also an important aspect which must-also be kept in mind.

Whether a strategy alone will suffice or a framework also, needs to be enunciated, is also, an issue to be considered.

A framework will possibly provide an all encompassing matrix for all stakeholders and lay down an activity map providing strategic guidance.

The Strategy Design

Should the strategy design include overall vision and mission or many sectoral ones? Actually an overarching vision, mission and a number of goals, some achievable and some lofty ones, need to be articulated. Strategy then will first need to lay down multiple paths to achieve these goals and then argue the most suitable path for achieving these goals.

One more important aspect which needs to be considered, is how the cyber landscape is addressed, and, if, only one broad document shall suffice. No doubt it is the three pillars viz people, process and technology which will need to be discussed, in addition, in my opinion digital infrastructure should also, be, considered as another pillar, as it crisscrosses and impacts entire spectrum of digital and business activities.

Pillars

The strategy should, not only be, restricted to mere statement of action plan at policy level for the government sector, but, it should also address, various ways in which, the stakeholders, across suggested pillars viz. people, processes, technologies and digital infrastructure are impacted.

- The people aspect must include, right from common semi literate man to CIOs and CEOs, to Secretaries and Ministers to Government of India and even from

MSMEs to Indian MNC and MNCs in India.

- When looking at, processes, the enabling best practices, risks, its assessment and mitigation, data handling and its management, social engagement processes and the way government conducts its business should be considered among other aspects.
- As regards technologies as a pillar, it is important to address ecosystem across multiple technology layers including the cyber supply chain. It is not only the hardware but also software artefact supply chain where trust needs to be built in.
- Besides, above, as highlighted earlier, the most important pillar, which needs to be considered is, Digital Infrastructure. This pillar is actually all encompassing and impacts almost all sectors of economy thus it needs to be defended, protected and made resilient. Be it governance, financial sector or aviation each vertical today depends on digital backbone. The challenges faced by stakeholders in each of these verticals is similar yet they have their own peculiar challenges.

KNOWLEDGE COLLABORATION

Collaboration and knowledge sharing amongst various stakeholders associated with cyber security in various sectors is a very important factor which can make substantial difference in reducing vulnerability related costs. It is important for key persons in each of the specialised sectors to work together and share their experiences. Such efforts need to be given due impetus and funding. Local communities and common citizens should also have access

to support groups where from they can seek assistance on a regular basis.

It is also important to focus on sectoral collaborative platforms which will be useful as a cyber support groups. Use cases of overcoming cyber security challenges and best practices can be easily shared on such platforms.

Decriminalise Breaches

A culture of reporting and resolving without criminalising the occurrence of breaches and implied roles of stakeholders needs to be encouraged. This will ensure a learning environment which will improve overall security. Such a step will encourage people to come forward and seek professional help.

Education

Education and awareness has to start early. As the efforts to promote digital transactions and E-governance increase, associated risks also increase. Institutionalised mechanism to promote cyber education in schools, colleges and in professional courses is strongly recommended to be addressed. Training an education of entire workforce in government and corporates also needs to be given due impetus.

Measurable Audits

A culture of internal and external audits with measurable results needs to be promoted. It will have associated pay offs as accountability could be established. It will also ensure due attention and funding from the top management in both corporate and government sector.

AI and Automation

As is evident the need for warding off automated sophisticated attacks on Infrastructure is amenable to automated responses. It is thus required that adequate infrastructure is created and put in place which is intelligent and responsive. The nature of problem is well suited for deploying automated machine learning and AI systems. There is a strong case, for promoting, common, India specific standards and solutions.

R&D, Indigenous Technologies and startups

As the thrust on digital infrastructure grows, security has to be part of initial design and development, if this is not done, then costs associated with interweaving the same later it may not be cost effective. A culture of supporting and adopting indigenous solutions will bring trust in the ecosystem. To promote this, special schemes to support and encourage startup's in this field need to be brought in. As is seen worldwide custom cyber solution providers command quite a price. Thus, importance of providing simple, cheap and resilient technological solutions is key to a safe future.

Resilience

Resilience is all about standing up on ones feet after a catastrophic event. Investment in making systems resilient and evolving appropriate best practices shall pay handsome dividends and provide business continuity. Resilient hardware and design can bring about enhanced security and thus can be extremely useful in risk management.

Conclusion

In conclusion, a cyber security strategy with a focus on providing a safe, resilient and intelligent digital infrastructure to common citizens is an urgent need of the

Critical Cyber Threats: Detection and Challenges

Brigadier (Dr) Rajeev Bhutani

CENJOWS

Introduction

In today's world, the Information and Communication Technology (ICT) has permeated in to every aspect of our life. State-of-the-art technology, continually improving performance and tumbling costs have resulted in widespread proliferation of ICT. In fact, the ICT revolution has changed the world to a border-less entity as never seen before, resulting in to creation of a new world order. Today, technology has brought ICT within reach of the masses, resulting in to wide social impact. The social networking and mass communication systems have networked societies and individuals as never before. In the economy, ICT is today the lead money spinning industry. ICT is controlling and connecting every aspect of governance be it transportation, power transmission, aviation, railways, food-supply, water supply, e-governance and so on. With these attributes, ICT and its related infrastructure have now become critical. Since cyber space is the environment through which the ICT functions, it has now assumed an identity of its own. Like ICT, Cyber Space has become an important national asset spanning across all sectors, including governance and security.

New capabilities have enabled new threat vectors for Cyber enabled warfare. It has made the commission of cyber attack easier and cyber threat detection even more complex, hence it has become a favorite tool in the hands of states, non-state actors and terrorists. Due to omnipresent nature of ICT and cyber space, there are certain distinct advantages available to states acting covertly, non-state actors and terrorists:-

- Cyber space gives disproportionate power to small and otherwise relatively insignificant actors.
- Operating behind false Internet Protocol addresses (IPs), foreign servers and aliases, attackers can act with almost complete anonymity and relative impunity, at least in the short term.
- In Cyber Space, the boundaries are blurred between the military and the civilian and between the physical and the virtual; power can be exercised by states or non-states or by proxy.
- In Cyber Space, goals can be achieved without the need for armed conflict.

Cyber Threats or Modes of Cyber Attacks

Hostile actors in Cyber Space can employ a wide range of techniques or in other words Hackers utilize a wide range of tools that couple with highly sophisticated computer manipulation techniques. Hacking is a potent tool in cyber warfare, an ability to attack that requires little funding, is difficult to detect and defend against and cause massive damage.

- **Identity of a Hacker.** Each computer has its own

unique Internet Protocol (IP) address similar to the postal address of a house. The Internet Corporation for Assigned Names and Numbers (ICANN) is responsible for global IP address allocation. ICANN, a non-profit organization operating in the US, is under contract with US Department of Commerce and was previously with US Department of Defense. Despite this identification tool, hackers can mask their identity by using proxy servers.

Information is routed through multiple computers, only showing each computer's identity to the next in line. For example, a Chinese hacker could route his or her activity through a computer in Venezuela, which may further route its activity through Russia. The computer in Russia could be used to attack a computer in the United States and the United States would see it as an attack from Russia. Though, theoretically it is possible to trace the routing of a cyber attack, but practically the amount of effort spent on moving up the chain is prohibitive and at time inconclusive. Thus even if in the above case, investigators do reach the Chinese link, they will still be unsure whether China was the originator or simply another link in the chain. Proxy servers can be rented or obtained through compromised systems. In addition, free software such as the Onion router, tunneling protocol, encryption and wireless access points exponentially increase number of possible links.

Hence, despite the Unique IP address, it is not always possible to pinpoint a hacker.

- **Security Exploit**. Security exploit is a common

method used in cyber reconnaissance and cyber attack. It is a prepared application that takes advantage of a known weakness in the cyber space. It is in the form of a piece of software, data or command that utilizes a bug, glitch or vulnerability in the software of an electronic device to cause an unintended or unanticipated behavior. This can allow the attacker to take control of the computer, permitting its use for other tactics, such as Distributed Denial of Service (DDoS).

An exploit is used to gain low-level entrance to a computer.

- **Privilege Escalation**. Low-level exploits do not permit substantial control over an electronic device. Therefore, after gaining low-level access to a system the hacker searches for further exploits to attain high-level access. This technique is known as Privilege Escalation. Once security experts have identified exploit vulnerability, a patch will be issued. For this reason hackers try to keep known exploits secret and these are known as Zero day exploits and hackers may catalogue large numbers of them for their own use or to be sold in the black market. In 2006, Taiwan was hit with "13 PLA zero-day attacks", for which it took Microsoft 178 days to develop patches.
- **Trojan Horse**. Trojan Horse or simply known as a Trojan is another tool or technique employed by cyber warriors to compromise a computer or network. A Trojan appears to perform a desirable function but

secretly it is performing malicious activities. Trojans are employed to gain remote access, destroy data, download data, serve as a proxy, falsify records or shut down the target computer at will. The Pentagon, defense-related think tanks, and defense-related contractors were the target of a combined spoofing and Trojan attacks in 2008. Trojans were hidden in email attachments designed to look as if they were sent from a reliable source. The Trojan was designed to bury itself in to the system, covertly gather data, and send it to an Internet address in China. Due to the ability of hackers to route their activity through foreign computers, security experts were unable to determine if China was the final destination or if it was an attempt at framing China.

- **Distributed Denial-of-Service (DDoS) Attacks.** If the Internet is brought down in a country or region, it will do immense damage to the population, infrastructure and financial sectors in that society. The Internet relies on bandwidth and if targeted with a DDoS, this can block the selected servers and effectively jam the Internet. It is relatively simple to achieve. If enough emails are sent in a short span of time, or enough hits are made simultaneously on a selected website, the bandwidth will fail to cope with the amount of data it is being requested to move and simply clog up, just like automobiles in a main street during rush-hour. DDoS attacks may be conducted by a collective of individuals, often coordinating their efforts, or by a network of computers under the control

of a single attacker. Such networks are called botnets, with each computer in the botnet known as a bot or a Zombie. A botnet can have millions of computers all over the world as slaves. These computers could be taken control of by malicious users without the knowledge of the owner, usually through a rootkit, Trojan or virus. Sobig and Mydoom are examples of worms, which create zombies. A botnet's originator, known as a bot herder, can control the group remotely, usually for nefarious designs. Infected zombie computers are used for sending email spam or to engage in DDoS attacks. The services of a bot herder can be hired from the black market. On estimate in 2007 suggested that Chinese hackers had 750,000 zombie computers in the US alone. Estonia was the victim of a sustained DDoS attack in 2007.

- **Exploitation of Supervisory Control and Data Acquisition (SCADA) Systems**. SCADA systems control many major infrastructure systems and are increasingly being relied upon. SCADA systems are used to run power plants, control dams and even city traffic flow by controlling the traffic light system. If these can be accessed by a terrorist organization or forces inimical to your nation, they can effectively take control of that facility. One of the main vulnerabilities of this is through a mole employee or a disgruntled worker, who can be exploited by the enemy organizations to gain access to the SCADA computer system. From there they could initiate an attack to break a key facility or cause other forms of

damage. The potential of this attack can be gauged from what had happened in Queensland Australia. A hacker got in to the sewerage SCADA on Australia's Sunshine Coast. A former employee, who had access to the required passwords and knew the system, had put in glitches and deliberately released millions of liters of raw sewerage in to the water system and sparked an investigation. Because, after his dismissal, the council had failed to change the passwords and effectively allowed that employee access to the system. His motives were personal but that amply demonstrates what a terrorist could do?

- **Malware**. It is an obvious weapon or tool, which a cyber expert could use. Viruses and works can bring down systems and networks and cause great disruption to the target. An important operating system could be rendered temporarily useless or made to malfunction. The potential loss of data through such a virus or worm could have a huge implication if targeted correctly. Although, the technology and skills involved in designing, building, testing and storing these weapons may be complex and advanced, but means of delivering these weapons may be astonishingly simple. A well known example is; In 2008, highly classified US Department of Defense (DoD) networks were reportedly infected by an unknown adversary that placed 'malicious code' on USB thumb drives and then dispersed them in parking lots, near sensitive national security facilities. After a curious finder inserted the drives in to computers, the

code spread across their networks.

Another example is the use of 'Stuxnet' worm developed jointly by the United States and Israel against Iranian nuclear program. It temporarily took out nearly 1,000 of the 5,000 centrifuges Iran had been spinning at the time to purify Uranium. According to experts, the code itself is 50 times as big as the typical computer worm. Problem was to gain access to the Natanz Plant's industrial computer controls, which was cut off from the Internet – called the air gap because it physically separates the facility from the outside world. Having designed and tested the bug successfully, problem was to get this worm in to Natanz. They had to rely on engineers, maintenance workers and others – both spies and unwitting accomplices – with physical access to the plant. It was the 'thumb drive', which did the trick, allowing spread of the first variants of the computer worm. However, later more sophisticated methods were developed to deliver the malicious code.

- **Use of Internet and Social Media as a Means of Command and Communications by Non-State Actors/ Terrorists.** The emergence of more 'networked' organizations with horizontal leadership were using Internet for breakthrough in command and communications. Obviously e-mail is an instant form of communication and can easily be encoded. Seemingly innocent messages can be sent that only the recipient would understand, although a coded message is as old as terrorism itself. Email allows much greater speed in delivery and an almost guaranteed receipt. An example is the email sent by

the 9/11 hijacker Mohammed Atta:

"The semester begins in only three more weeks. We've obtained 19 confirmations for students in the faculty of law, the faculty of urban planning, the faculty of fine arts and the faculty of engineering. Best wishes from the Professor to all of you!
Mohammad"

This message clearly seemed innocent, but now knowing the events of 9/11 and who wrote it, we know that this had set the attack dates (it was written three weeks before the attacks). The 19 confirmations were the 19 terrorists who were carrying out the attack, the faculties were the codes for the targets and this confirmed which ones, and of course the 'Professor' is Osama Bin Laden.

Messages can be hidden in pictures or made to look like Spam mail so as not to attract attention. Terrorists have been known to set up an email account and change the password daily, the cells and terrorists will know the user name and daily password. Messages can be written, saved as a draft and then accessed by the whole network without being sent. This greatly reduces the possibility of interception or an evidence trail before or after an attack.

With the proliferation of Social Media – You tube, Whatsapp, Facebook, Twitter, Instagram and so on, the task of non-state actors and terrorists have become much easier by making proliferation much faster and that of government agencies much more difficult. Simple symbolism is a known method of terrorist communication. Video clips or photographs can contain a hidden code for example simple graphics such as

a terrorist holding a rifle in the left hand will be displayed. Having the same graphic with the rifle in the right hand can be a signal for a terrorist cell and may go almost undetected by the intelligence agencies monitoring it.

Challenges to Counter Cyber Attacks

The Internet technologies employ open standards for exchange of information and are not fundamentally secure. As a result, systems remain ab-initio vulnerable, which needs to be appreciated when evolving the remedial or security measures. The systems have been made even more vulnerable due to compromises affected for commercial convenience and making them user friendly.

The World Wide Web is unregulated and accessible to almost everyone. Cyber attacks happen in seconds and there will be no time for an emergency cabinet meeting for a centralized response. The first responders to an attack may not be official since it could well be civilian because most critical infrastructure is in private hands.

The Internet population has jumped from 1.15 billion users in 2007 to almost 4.48 billion active users as of October 2019, encompassing 58 percent of the global population. China, India and the United States rank ahead all other countries in terms of Internet users. The scale of ICT applications and their openness, which is conducive to tremendous growth, throw a sort of 'grand challenge' in protecting cyber assets from penetration and attacks.

Cyber weapons do not require physical proximity of the attacker to the victim. Since information is automatically and quickly forwarded on the Internet to wherever it needs to

go, it is almost as easy to cyber-attack a site on the opposite side of the world as a geographically proximate site. Cyber attacks do not leave persistent traces like chemical residue, fingerprints or perpetrator DNA since digital data can be easily overwritten to leave no trace of the original data. Thus attribution of cyber attacks is extremely difficult due to DDoS attacks.

It will be a challenge to develop a theory of cyber deterrence.

CONCLUSION

Trust, share, cooperation between private and public entities have to be done not by imposition of a law, but a more horizontal agreement among government, private sector and civil society is required.

Public awareness and education is imperative. The attack can start with one person plugging a USB drive in to an infected computer and then it spreads like an epidemic. Everyone is vulnerable; therefore we have to behave responsibly.

We are quickly moving towards an 'age of cyber warfare'. All states are now fully aware of cyber threats and are taking active steps to limit these threats, while an increasingly large number of states are also becoming meaningfully engaged with the offensive possibilities that cyber space can offer. A notable number of states now have such organizational structures in place. For instance, the United States and China both have established Cyber Commands.

Embracing Human Behaviour in Cybersecurity

Lieutenant Colonel Jaimandeep Singh
Defence Intelligence Agency

Nishant Chaturvedi
Cybersecurity Expert

"Only amateurs attack machines. Professionals target people"

-Bruce Schneier, one of the fathers of modern cryptography

Any kind of security that is meaningful and useful to people, involves people, their interactions with the environment, their relationships with others, and their myriad thoughts and biases. Various social theories have tried to model people's decisions as if they are computers or can be captured into some mathematical equations. However, they have not been able to bracket human behaviour and his actions. Fact is that people are not deterministic. They have limited cognition and their behaviour/action is also a function of context and their inherent biases. At times, this leads them to act in ways that appear to be in conflict with their intentions, whilst the repercussions, though being aware of, at that moment in time are ignored. Taking a behavioural approach to security means focusing less on how people should act, or how we expect them to act, but

more on how they actually act [1].

More than 90% of the businesses that have experienced data breaches affecting their public cloud infrastructure is due to human factors. These attacks had a significant part of 'social engineering' inbuilt [2]. Social engineering is the art of exploiting human psychology, rather than technical hacking techniques, to gain access to buildings, systems or data [3]. The term was popularized by Kevin Mitnik, a famous hacker turned security researcher, in the 90's.

"If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology" [4]. Socially engineered attacks/ threats can circumvent most of the advanced cybersecurity systems as they prey on human behaviour. They push users into performing an action or providing information through psychological manipulation. In the case of email attacks like phishing, these techniques often involves clicking on an embedded link, downloading malware like ransomware or revealing passwords and offering financial authorization.

WHY PEOPLE DO WHAT THEY DO?

Social and Behavioural psychology research tells us that people have a tendency to take a particular path when either the environmental constraints are perceived as eliminated or their behaviour is spurt-guided towards that direction. In simple words, people tend to do things when they are easy to do. Social psychologists call these catalyzing environmental factors 'channel factors' because they have a tendency to 'channel' people's actions [5].

In a security context, the employees and users behaviour

can result in unintentional actions - or lack of action - that can cause, or allow a security breach to take place. While in a structured organizations, former is unlikely, the latter is a manner of concern. Latter can be seen in terms of Psychology of Risky Behaviour. Aspect of employees in order to have an increased productivity, can follow the path of least resistance, which can be curtailed by a bigger punishment at stake than the reward. Behavioural and Cognitive psychologists have appealed to constructs such as negative emotions, self-awareness, social exclusion, lack of self-regulation, and pseudo-positive views of risk-takers to implement irrational risky behaviour. Psychologists other than lack of self-regulation, have added an emphasis on other factors such as impulsivity and sensation-seeking as well. Also they have focused on various cognitive processes that keep people from attending to, or recalling, the right kinds of security information triggers. Other than that ,the ever present aspect of Habituation is very difficult to control. Their decisions can range from downloading a malware-infected attachment to failing to use a strong password. This is part of the reason why it can be so difficult to address the security aspects of human behaviour.

Web of interconnections and the data Tsunami : Beyond human cognition

The real-world system is a complicated web of interconnections churning out data at an unfathomable rate. The complexity and interplay of systems has reached an inflexion point which is beyond what the human mind can

make logical sense off.

Security must delve deep into the systems and workflows, addressing its design, components and connections. The modern systems have many components and connections, many of these are not even known by the designers, implementers, or the end users. No system can be perfect and no technology can provide the ultimate answer to the security problems.

IS HUMAN ERROR REALLY AN ERROR

Most often in the cybersecurity context we come across the term 'human error'. It is usually quoted that most of the security breaches are due to human errors. Can anything that happens over and again and cannot be eliminated, actually be termed as an error. Using the term error gives us a false assurance that it can be eliminated. Whereas, it is the human nature which will remain the way it is. We have to model our security solutions incorporating the inherent human handicap of doing things in a non deterministic way, rather than having a false sense of modelling humans as a deterministic machine.

WHY TRAINING HAS FAILED TO ACHIEVE ITS OBJECTIVE

In a security context the human behaviour/decisions or the susceptibility to fall prey to social engineering has traditionally been viewed as a knowledge gap problem, which can be bridged by training of personnel. However, social engineering is a complex interplay of human psychology, technology and the orchestration which falls under the realms of artistic deception. It exploits the primitive human survival instincts like greed and fear,

behavioural tendencies like trust and bonding, and a myriad of other human emotions. Social engineering has multifarious manifestations and may be beyond the human capability to fathom, let alone predict.

Why existing Solutions fall short

To combat the risks of security breach, most security solutions rely on user-behaviour monitoring. These are usually rules-based or machine-learning-based solutions that ingest troves of data about employee and user actions, especially their use of IT systems. Generally, they attempt to identify divergence from what is considered "normal" behaviour for a particular employee. When an anomaly is detected, the solution flags the action. While this method can be helpful, we find that it usually falls short, for the following reasons [6] :

- The time by which the negative behaviours get detected, the breach has often already occurred. The organization is already at a disadvantage, as it cannot stop the attack a-priori.
- The "divergence from normal behaviour" creates a large number of false positives, wasting valuable business working hours.
- Serious threat actors may restrict malicious activity into the baseline of "normal" activity and may never be caught.
- Massive amounts of employee/user data is required for anomaly detection which can create privacy concerns and can have resultant potential for abuse.

What's the Way ahead

The security solutions need to incorporate the human behaviour ab initio and cater for the error margins, in the solutions provided by them. There may be a need for a paradigm shift of approaching the security solution wherein it is seen as a process rather than a product. Following can help in streamlining the process :

- We have to acknowledge that human behaviour and actions are non- deterministic and we have to model the security solutions incorporating the same. Modelling humans as a deterministic machines is fallacy which will leave a massive gap in the security apparatus.
- The businesses have to understand the workflow and automate most of the process. There should be a minimum amount of human intervention. The more the decision points are left with the users the more complex the system will become and ultimately make it more vulnerable.
- The software systems and applications needs to be viewed like data, only that much should be allowed for each employee, as is required. Only a restricted number of applications should be allowed which are essential for performing the task. A whitelist of applications depending upon the defined role of employee can help in streamlining the security process.
- Subsequently, Operating System can be user configurable, having a built-in AI-based predictive

self-learning algorithm, to assess User Tendencies and their Heuristics. This shall modulate the privileges and decide the overall user experience, the user should be allowed to have.

- Internal segmentation and the principle of hierarchical privileges should be followed to limit the damage from attacks.
- The windows through which the employees can get social-engineered should be identified and the same should be minimised as much as possible by replacing it with automated processes.

References

1. Deep Thought A Cybersecurity Story. Accessed from:https://www.ideas42.org/wp-content/uploads/2016/08/Deep-Thought-A-Cybersecurity-Story.pdf on 09 December 2019.
2. Kaspersky Blog. "Understanding Security of the Cloud: from Adoption Benefits to Threats and Concerns". Accessed from : https://www.kaspersky.com/blog/understanding-security-of-the-cloud/?utm_source=pr-media&utm_medium=partner&utm_campaign=gl_b2b-cloud-mini-report_kk0084_organic&utm_content=link&utm_term=gl_pr-media_organic_kk0084_link_partner_b2b-cloud-mini-report on 10 December 2019.
3. CSO India. "Social engineering explained: How criminals exploit human behavior". Accessed from : https://www.csoonline.com/article/2124681/what-is-social-engineering.html on 10 Dec 2019.
4. Bruce Schneier. Secrets & Lies: Preface - Schneier on

Security. Accessed from : https://www.schneier.com/books/secrets_and_lies/pref.html on 10 December 2019.

5. Leventhal, H. (1970). Findings and theory in the study of fear communications. Advances in Experimental Social Psychology, 119-186.
6. McKinsey & Company. "Insider threat: The human element of cyber risk. Accessed from : https://www.mckinsey.com/business-functions/risk/our-insights/insider-threat-the-human-element-of-cyberrisk on 10 December 2019.

Cybersecurity Citizen 2030

Dr.Vipin Tyagi

Director General, Centre for Development of Telematics (C-DOT)

Cyber Security, Public Network Security, Critical Infrastructure Security and Enterprise Security are most important strategic need for the country. Often there is lot of talk about the Cyber Security incidents, vulnerability and need for India to leap frog and take large strides. Few case studies from emerging economic giants are also mentioned which gives an impression that India is very weak in Cyber Security and situation is hopeless.

I wish to bring out that in Telecom Technology and related security, many significant technologies are available from C-DOT. C-DOT alongwith 26 manufacturers (using indigenous technology) can create National Broadband Infrastructure using DWDM, Routers, Switches, Next Generation Networks and Optical access like XGS-PON, GPON and WiFi hotspots etc. All of these are designed, developed and manufactured in India. We have world class optical, switching, packet and wireless technology available within the country from Indian manufacturers.

C-DOT has also implemented world's first standard compliant C-DOT Common Services Platform (CCSP) based on One M2M Standard for Internet of Thing (IOT)

or Machine to Machine Communication (M2M). This platform creates interoperability, removes vendor locking, provides level playing field to Indian startups in Smart City projects or public deployment of IOT anywhere.

Post Quantum Encriptors, Lawful Interception Systems, Telecom Computer emergency response team (T-CERT) systems are already available from Indigenous Technology.

Image Processing and Aritificial Intelligence based systems are designed and deployed by C-DOT.

Central Equipment Identity Register (CEIR) based systems can find out duplicate and spurious phones hence avoid misuse and grey market. The system can block these devices in network. The system is already operational in Maharashtra circle.

We need to recognize and promote our own capabilities, we are good in H/w and S/w design, why we cannot be competitive in systems? It is a myth that advance system cannot be designed and manufactured in India.

There are numerous initiative and capabilities that exist within the country, so there is need to bring together fragmented initiatives and create nationwide deployment of these solutions. There is need for allocating resources and pay attention to develop advance systems for future.

The market access and effective methodology for providing market access to Indian designed and developed products with proactive implementation of 'Make in India' and preference to Design in India policies are required.

We have to move from "Talk to Take" Indian R&D based products and solution.

Cybersecurity: Points for discussion

Dr K J Ramesh

Former Director General, India Meteorological Department,
National Geospatial Think Tank Member

1. Data gathering agencies should have a continued guidance through continuous oversight mechanism so as to generate most representative data for a robust analysis and scenarios of future projections can be made.
2. International best practices need to be brought in from time to time thru the standing oversight mechanism
3. Efforts should be made to generate primary data covering all sectors of physical, financial and socio-economic sectors of the economy so as to generate risk proofing options can be worked out
4. Data collection platform need to be auto mode sensor based IOT and AI based built in data analytics algorithms
5. Cloud based data collection, storage, data analytical platforms to be established thru regional and state/ local clusters linked thru NKN
6. Live servers and dashboards need to be configured with live access of dynamical characteristics of the variability of the indicative metrics for each of the respective sectors of development

Addressing Public Grievances on Indian Railways on Social Media

Mr Mukesh Nigam,
Managing Director, Centre For Railway Information Systems (CRIS),
Ministry of Railways

A) Digitalisation on Indian Railways

1. A few years back a senior colleague of mine attended a management course in Paris. He told me that each participant of the course was given a book with the title "Built to Last: Successful Habits of Visionary Companies". The book dwells on what makes enduringly great companies. The point put across in the book "Built to Last" is that if a management organisation is more than 100 years old, there must be a lot to learn. It's not about a great idea, a great product or a great leader. Such companies preserve a core value as well as puts emphasis to stimulate progress. These companies have their unique identity and a unique culture. It was stated that the processes that can withstand the rigours of more than a century require a very healthy look. As you may be aware, Indian Railways is more than 165 years old organisation. The processes within the organisation have been unique and robust enough to last much more than a century.
2. Ministry of Railways set up CRIS (Centre of Railway Information Systems) as a Society on 1st July 1986

and it has completed 33 glorious years. In response to computerisation, it was decided more than three decades ago to build in-house capacities. It was decided that CRIS should have a mixture of domain experts and software professionals. The mix of domain experts and software professionals is a unique feature of CRIS and has facilitated a fascinating journey of digitalisation in Railways.

3. Railways started their journey of digitalisation initially to digitalise what was the manual process. Initially CRIS was set up to develop Freight Operations Systems as freight earnings formed the mainstay of Railways earnings and it was perceived that computerisation will bring about efficiencies in freight business. Very soon, the effort of digitalisation of PRS (Passenger Reservation System) followed. It took time for these two vast systems to stabilise but on their successful rollout it was established that CRIS could manage pan-India IT applications spanning Indian Railway territory on 24X7 basis.
4. One major benefit of digitalisation was that once the manual process got digitalised the subsequent innovations in the field of IT were not very difficult to board. PRS symbolises the most popular perception of digitalisation of IR with the public.
5. Digitalisation of PRS started as a pilot project in Delhi and on its success was rolled out to four other regions. The software developed in the regions took care of trains within their area. Soon, the demand

came for a single window service so that booking for any train in the country could be done from anywhere. In view of the growing popularity of internet it was decided to provide PRS related information to public in 2000 and subsequently with ecommerce getting more mature, the system was enhanced to provide reservations through internet in 2002.So, it was not conceived that internet-based ticketing was the main objective of digitalisation of PRS. Once the commercial framework of internet-based ticketing became available PRS adoption was quick. Similarly, on the arrival of 4G connectivity and mobiles, it the internet based digitalised PRS ticketing was easier to adopt. The internet-based passenger reservation system has now taken nearly 70 percent of the work load of the passenger reservation system and out of this 70% the share of mobile ticketing is more than 60%. The launch of new website for passenger reservation in June last year facilitated seamless user experience has been widely appreciated by the public.

6. On the earning side, the emphasis of the policy makers has been to make a push towards cashless economy. In FOIS nearly all payments are cashless. While laying the objectives of FOIS cashless payments was not really the objective. However, digitalisation of the processes facilitated transition to the digital cashless economy

7. The second striking feature of railway organisation is its sheer size. Indian Railway network is one of the largest that spans every region of the country.

It has 1 lakh,20 thousand and more running track kilometres, rolling stock of nearly 4 lakhs and it runs nearly 20000 trains every day. It carries more than 8 billion passengers in a year which is more than the entire population of the world. So, in addition to its age, when we consider the volumes and requirements of Indian Railways, the enormity that confronts us is overwhelming.

8. CRIS has evolved over the years. Over the years, the portfolio of projects covered by CRIS entail the entire gamut of activities on the Indian Railways functions including e-procurement, finance management and management of assets. The design, development and maintenance of the software applications as well as the communication network under the same network under the same roof has facilitated quick pan-India roll-outs

B) ADDRESSING PUBLIC GRIEVANCES ON SOCIAL MEDIA

9. The process of digitalization has opened new vistas in the area of transparency and accountability. In the age of Information Technology transmitting data and information is easily done via social sites and applications and it became important to address the growing use of social media.

10. Complaint Management System (CoMS) is a web-based complaint receiving system for immediate redressal of passenger grievances. It was rolled out in 2010 to enable railway passengers to lodge complaints and complaints with auto assignment and

tracking features.

11. To address the sentiments expressed on Twitter and other social media handles a system was rolled out in 2016 which captures all posts on Twitter handles (@RailMinIndia,@RailwaySeva etc.) mentioning all keywords specified by business user/citizen for ticketing based on predefined rules/policies. An inbuilt NLP (Natural Language Processing) categorises 'mentions' as actionable and non-actionable. It also categorises them as negative and positive sentiments. All this is done automatically without manual interface. All 'mentions' categorised as actionable are bucketed with unique ticket number by the system automatically. Users can create a ticket for certain keywords and further different priority levels of tickets can be decided, based on keywords fed to the system by the business user. Every new mention received through Twitter is categorised, as per the sentiment analysis as negative, positive or neutral. System does automated assignment of tickets based on priority of tickets, source of mention, round robin and Login by Agent.

12. An integrated complaints platform called 'Rail Madad' has been rolled out subsequently which integrated six different channels of public complaints: Web; SMS; App; Manual Dak; Social media; and, IVRS Helpline 139.

13. Out of all channels of reporting of public complaints, Helpline and Social Media are the most popular. As

per analysis of their recent performances, the average disposal time of complaints in Helpline was 7hrs21 minutes and in Social Media it was 6hr 15 minutes. Use of IT in addressing public grievance redressal has, therefore, shown very encouraging response.

C) Issues in Intel gathering from Social Media

14. There is a threat of data leakage, theft and misuse of data by malicious actors. The issues of privacy protection are also equally important. In view of the vast numbers that the applications in CRIS serve, they are targets of malicious actors. Nearly 5 lakh malicious attempts are made to breach the security layers in CRIS every month.

15. Over more than three decades, CRIS has developed an expert network practice specializing in state-of-the-art IP networks including Internet Gateways and network security. These experts work in close coordination with the software application and system experts for architecting new solutions, their deployment, performance optimization and sustenance. CRIS has developed most of the applications in-house and customized them according to the Indian Railways requirements.

16. There is a common Internet gateway for all Internet facing applications of Indian Railways viz. www.indianrail.gov.in, www.ireps.gov.in, www.trainenquiry.com, www.indianrailways.gov.in (websites of Railway Board, all zonal railways, PUs, Training institutes etc.), FOIS e-payment, UTS

on Mobile, HHT for TTEs, Mobile Van ticketing, Track Management System (TMS), Claims, Parcel etc. hosted at CRIS DC. It has multilayer security with Security event co-relation and alerting through Security Information and event management (SIEM). There is a dedicated internet gateway for NGeT (www.irctc.co.in) due to its higher performance and scalability requirements. The Network Operations Center (NOC) ensures smooth operation with dedicated 24x7 monitoring for ensuring the desired level of performance, availability and for addressing security threats for all the applications hosted in CRIS.

17. CRIS maintains a regular liaison with cyber security agencies of Govt. of India such as CERT-IN, NTRO, National Cyber Security Controller etc. for real-time monitoring of threats, their effective mitigation and also for timely upgrades in the security sub-system. An Information security policy has already been defined & implemented by CRIS. For sensitive IT applications/systems, security audits are also conducted through external agencies like STQC etc. CRIS has nominated a dedicated team headed by a CISO for ensuring compliance to security policies & related functions like issuing security guidelines/ alerts, security posture assessment, risk analysis & mitigation etc.

Securing India's Railway Infrastructure: The Challenges and Solutions

Ms Vandana Nanda,
Former Managing Director,
Centre for Railway Information Systems (CRIS), Ministry of Railways

Cyber attack on railways and other transportation infrastructure is no longer a hypothetical scenario. Major railways across the US, Europe, and Asia have already witnessed a cyber-attack. The combination of glaring vulnerability and grave potential to cause mayhem, economic damage and even loss of human lives, make railways around the world the perfect target for both economically motivated criminal groups and hostile station-state actors.

Indian Railways--India's economic lifeline

India owns one of the largest railway networks in the world. That, however, is only a part of what renders it an exemplary and affordable mass mobility system. The intricate matrix of connectivity it provides across a vast and widely populated country, coupled with an impressive frequency of trains to the remotest areas, makes it a very convenient mode of transport for a large majority of Indians and the budget tourists.

Risk of Cyber Attacks

Though there is much variation, all modern railways use

computer systems to monitor and manage the physical assets through IT, in railways operation. These operational technologies (OT) converge with the IT networks, where they can easily be infected with malware. For most railways, cyber-security consists mainly of commercial security products like firewalls and other government-approved antivirus tools. This approach is similar to the cyber-security mechanisms in place at most small or medium-sized businesses, that are not critical to national security. This type of security may be adequate for some sectors, but it is nowhere near enough to keep a highly-targeted critical national transportation infrastructure protected from those who wish to do it harm.

Indian Railways(IR), in keeping with its sheer size and volume of operations, has large areas of its day-to-day operational requirements run through a maze of IT-based programmes. Some small applications are locally made and maintained. However, those that are country-wide applications, are centrally developed, controlled and maintained- even if locally operated by the field operatives. The security set-up for such pan-IR critical programmes are multi-tier and designed to be one step ahead of the next cyber attack, but then one can never be sure. Since the world of cyber security is a dynamic world, the efforts of improving upon the existing security architecture has always to be 'a work in progress'. As such, there is always scope for more to be done and that too within the financial constraints of running the largest transportation network (in terms of passengers carried) in the world.

There can be a dozen or more operational technology (OT)

assets that, if compromised by a cyberattack, could cause significant disruption to railway service. These assets include the rolling stock itself, the station operations, and related infrastructure. For a moment,let us visualize a scenario in which a multi-national Indian IT firm is contracted to handle IR's critical softwares. An employee, a national of a country inimical to the interests of India, working for the Indian IT firm having offices in China or even the USA, could cause havoc if he were able to, through the company network, gain access to either data or operational details of any of IR's critical operating softwares. Such a possibility would be remote, if not totally ruled out, in a situation where the cyber security set-up is with IR's in-house IT arm.

CYBER-SECURITY PARADIGMS N THE SECTOR.

There are three main aspects that can be considered in this context:

- The main is the change in technology cycles
- The newly deployed system's overall lifecycle
- The cost of the change.

Indian Railways is the pioneer within govt. ministries to have introduced computers in its offices a good 50 years ago. It has, over the years, developed a healthy workforce of computer savvy personnel who have developed some of the largest and complicated softwares running in the world. The need for a bigger role for this ready workforce to expand the IT framework to even more areas of IR's working, is the need of the hour. Further emphasis needs to be laid on opting for a paradigm transition from any kind of proprietary technology that IR may be still using

– switching instead to the latest AI based technologies available. This should not entail entering into any long-term commitments due to short shelf-life of IT software today.

Such an approach could help the system become more adaptable and flexible and in the long run, allow for the rapid adoption of technological advances. These could also cause changes in system lifecycles, IT systems, but within central control.

Finally, the cost factor has to be considered. The overall rule of thumb is that the older the technology , the more expensive it is to operate and maintain because of the increasing scarcity of essential components and software. These impact the economies of scale.This would therefore require, a dedicated, time-bound programme of upgrading technology-both software as well as hardware, with allocation of funds at the beginning of the cycle and with lock-in allocations every year, till completion of the cycle.

THREAT LANDSCAPE

The threat landscape surrounding the railway sector is evolving. This is a natural outcome of different railway-related business concerns becoming more integrated over time.

However, most of the cyber-security challenges that are part of the overall threat and cyber-security paradigm are not specific to certain attacks. In fact, they are not restricted to malware and viruses even. In this sector, there is a far more lethal aspect of terrorism to be taken into account.

This is why, for railways, there is more to the concept of

cyber-security management when compared to the 'run of the mill' protection measures, that other sectors use. Like for instance, there are many pressing issues concerning cyber-security governance. These include security operations management, risk mitigation, and compliance enabling activities that need near-constant attention to be able to sustain a reasonable level of maturity.

ROLES AND RESPONSIBILITIES

On the Indian Railways, all pan-India software applications are written,run,monitored and maintained by a central organization which is the IT arm of IR. This organization, consisting of a dedicated team of software professionals, also keeps a 24/7 watch on all the application throughout the year, monitoring them on a real time basis to avoid any hinderance in the operations of the Indian Railways. They take responsibility for the fail-safe running of the applications and intervene as and when any glitch-either in the software or in the hardware-occurs in the running of the systems pan-India.

This central organization has been upgrading and updating the security features in all it's applications to prevent any cyber-attack -despite the user base being large and spread all over the Railway network. In order to bolster the organization's ability to invest more in cyber-security related upgrades in a timely manner,when allocating scarce resources, this body should be given primacy in allocation of funds as the cost of preventing a cyber attack is not measurable in financial terms. The track record of this central organization has been exemplary in letting any

cyber attack affect any of it's critical software applications.

Keeping these aspects in mind, we can safely conclude that the railway sector has an all-too-real opportunity to address different cyber-security concerns at the highest possible levels. The top-level management is ultimately accountable for cyber-security for the whole organization, with the responsibility to ensure the assets, operations and data are adequately safeguarded.

The central IT organization has to be directly responsible for validating cyber-security resourcing requirements and investments for the management of all cyber-security related work for railway's ICT. Further ,it should consider an integrated solution approach--

- Infrastructure wide solution that protects all weak points and possible entry points for malware
- Offers redundancy to prevent disruption of vital services
- Ensures protection of customer, employee and corporate data
- The infrastructure should not be allowed to be used as a conduit for further attacks on other entities

In addition, towards achieving this end, there is an acute need for an overall disaster recovery(DR) plan to be put in place, besides for each of the pan-India software applications operating in the Railways.The team in charge of DR would be a dedicated team specifically trained in the art of cyber warfare and quick response to cyber attacks.

CONCLUSION

It is an axiomatic assumption that cyber-security is going to be a necessary aspect of various railway businesses, even as the industry embraces new-age technologies. The digital railway projects across the nation and the pressing need to integrate with various other modes of transport will slowly but surely make it necessary for the railway community to give a very high priority to cyber-security.

With a central IT organization working for the last 32 years under the direct control of the top management, the safety of data and software/hardware assets is secure within the Railway. In future even if private entities are given to run on-board services on privately owned trains, or some other railway working is transferred to other than govt entities, train operations will need to continue with IR for reasons of securing the digital operations and also for national security. It is therefore imperative that the way forward for protecting Indian Railway's critical ICT infrastructure is by continuing the existing experienced formation and facilitating this IT arm of the Railways in a way, that it keeps abreast with the ever changing terrorism of cyber-attacks.

Social Media Is A Tool Which Can Be Gravely Misused

Ms Vandana Nanda,

Former Managing Director,

Centre for Railway Information Systems (CRIS), Ministry of Railways

1. US Presidential elections of 2016 were under the scanner for manufacturing narratives to influence voters.
2. Due to fear mongering/rumour mongering on social media, innocent people in Uttar Pradesh were mistaken as child lifters and killed.
3. Army soldier was honey-trapped by ISI over social media in Rajasthan.
4. Some Indians were brainwashed by the ISIS through social media.
5. Delhi Police personnel mobilised in short time to register their protest.

Therefore, through fake news, misinformation, disinformation, untruths, distorting facts, etc. being spread over social media, large swathes of the masses are being misguided. This can undermine faith in our institutions, subvert electoral democracy, create panic, fear and chaos, give rise to law and order problems, create divides between communities, etc.

STEPS TO BE TAKEN

Thus, Intelligence gathering today should encompass social media. For this, Artificial Intelligence and Data Analytics can be leveraged to keep an eye out for buzz words to gauge the overall sentiment of exchanges taking place in social media. Special social media cells could be created in each district for this purpose to monitor as per specific guidelines (to be) made by Govt. Based on the inputs of such an exercise, the persons in these social media cells can then apply their own mind and judge the matter at hand. If any questionable sentiment dominates or trends, the Central or State Intelligence agencies can be informed and timely appropriate action taken..

Happy & Content Population- Core Essential For A Safe And Secured Nation – A Sustainable Solution

Mr Ashutosh Vasant,

Director (Project Operation and Maintenance), RailTel

Apart from the Defence and Offence mechanisms viz physical , psychological, electronic , diplomatic, cyber security measures as discussed and debated by experts in various panel discussions , so essential to safeguard a Nation's integrity and existence, **a Happy and Content population is equally crucial if not more**, to not let chinks develop in the nation's armour .

For even the most prepared and armed to the nails nation, a dissatisfied population is the weakest link to expose and give wedge to the enemy to seep in as is proven since ages including that from the role of Vibhishan in Ramayana in defeating the most learned and most powerful King Ravan by Lord Ram.

To tackle this crucial aspect of growing frustration in youth in India due to massive unemployment and under employment as seen from the ratio of advertised vacancies to the no. of applicants in Indian Railways recent recruitment , which today has brought the society to the brink of disaster where for even an unconnected issue , the youth is ready to come

on street to damage public and private property as a sheer vent to this personal frustration, an effective and sustainable solution is being suggested with the idea that follows .

A SUSTAINABLE WAY FORWARD FOR A HAPPY AND HEALTHY INDIA

Four Biggest challenges being faced by the country:

1. Slipping economic indicators with falling domestic consumption
2. Under-employment and unemployment leading to frustration in youth , disrupting social fabric , peace and harmony with rising crime rates
3. Maddening Traffic congestion and Choking Pollution levels in Metros affecting productivity and health with pollution levels crossing 10 to 16 times the safe level
4. Challenge of sustainability of NEW SMARTCITIES. No visibility of resources for OPEX funding for the year next

Four in one viable solution:

- SHIFT the CMD and Board of Directors of ONLY CASH RICH PROFITABLE CPSUs to one NEW SMARTCITY each (174 Profit making CPSUs on date with total cash surplus of around Rs.3 lac Crore)
- Their vendor partner ECO system will follow them for pure business reasons to these new SMARTCITIES
- This will kick start investment in infrastructure , logistics , education , retail , health , entertainment,

connectivity etc driven by pure economics because of well paid consuming population now appearing in each such NEW SMARTCITY

- We will thus create 100 BOOMING CENTERS of economy across India
- Each such setup will offer gainful employment to the local youth, who no longer need to choke and block the Metros. They will find employment / business opportunities within 100 km range of their habitat .
- With source of employment close to catchment area, this will solve the problems of stretched infrastructure in Metros , reduce rising crime rates due to such under employed, frustrated youth in metros, reduce pollution , congestion and linked loss of productivity in metros and move forward towards creation of a **HAPPY & HEALTHY INDIA.**

IDEAL CPSU CMD &BoD CANDIDATES FOR SHIFTING TO SYNERGISTIC SMARTCITY LOCATIONS

1. GAIL to Jhabua
2. Coal India to Naya Raipur
3. OIL to Dholera
4. CONCOR to Bhamra port in Odisha
5. IRFC to one new SMARTCITY on Mumbai Nagpur MahasamruddhiMahamarg
6. HSRCL (High Speed Rail Corp) to Atul
7. DFCCIL to Ranchi

LOW RESISTANCE PROOF OF CONCEPT

- As Proof of Concept, p**urse string controllers i.e. CMD and Board of Directors of RailTel Corporation of India Ltd**, a Mini Ratna Telecom CPSU and the only market facing CPSU under the Ministry of Railways which is consistently profitable, consistently dividend paying and consistently debt free CPSU ,should stand **SHIFTED to GIFT** (Gujarat International Finance Tech City) , the dream project of Hon.PM to make GIFT the Financial capital of the world.
- RailTel with its reliable and secured pan India optical fiber network providing access to 70% of the country's population, will provide access to GIFT to the nation's consuming population and provide IT , ICT and Telecom services to the occupants of GIFT .
- RailTel being the World's biggest public WiFi operator on date , will provide traction to the IT/ICT/ Fintech players to look at GIFT as a business destination to associate with RailTel for Data monetization
- RailTel now being entrusted with Modernization of Railway Signalling and Telecom, a project worth Rs.1 lac Crore , will attract the world's best Signalling and Telecom vendors to GIFT to design , develop, manufacture and export the technologies to the world , creating the needed vibes at GIFT to spring forward
- RailTel will also get benefitted with these enhanced business opportunities of serving the occupants of GIFT (50 brokers , 26 Banks, DIIs, IT companies , BSE, NSE, Educational institutes , Hotel chains etc&

growing) , reduced cost of operations with reduced cost of property , rentals, medical , CCA ,HRA, logistics , travel cost for its employees as compared to any Metro , improved productivity with walk to work culture for its Corporate office employees and efficiencies of scale by developing a centralized NOC/CNOC in GIFT for its country wide operation at lower TCO (Total Cost of ownership) with 24x7 SEB power .

In turn, this sets the tone for 100 such cash rich & profitable CPSU Corporate offices to shift to one NEW SMARTCITY each across the country and solve the problem of unemployment, traffic congestion ,pollution and help make new SMARTCITIES sustainable, without further taxing the tax payer, by productively utilizing the cash surplus with these CPSUs .

In short, the first positive step towards creating a HAPPY and HEALTHY BHARAT

Acting as a Devil's advocate, every possible hole has been dug into this idea with all possible questions. The answers as arrived at, are enclosed to appreciate the logic and the necessity for a quick implementation of this idea to ensure a safe, secure and vibrant India.

1. **Why is this idea being proposed in the first place when the concern of falling demand, unemployment and slow down in consumption and GDP is being tackled with additional spending in MGNREGS, PMKISAN Yojana , Mudra Loan and a host of other similar schemes to boost liquidity in the**

hands of the masses ?

Ans: MGNREGS completes 13 years in 2019. Had the scheme been delivering, the reported rural distress should have been absent and most of the rural infrastructure works should have been completed to perfection using the money as being spent on this scheme.

Today's newspapers speak of GoI having ended up spending 80% of allotment of Rs.60,000 Crores in MNREGS till date for current FY. The Rural Development Ministry is expected to demand additional Rs.60,000 Crores to meet the need of full FY, a total of Rs.1,20,000 Crores !!!. PM-KISAN has already disbursed the allotment and so have soft loan schemes. Having distributed so much of money in offering employment & business upswing , this has still resulted in adverse election results in Maharashtra & Haryana linked to rural economic distress and the GDP figures are looking South with each passing day . It shows that either the schemes are not enough or the benefit is not reaching the targeted masses.

While MGNREGS, PM-KISAN, Farm Loan waivers etc are politically unavoidable essentials once rolled out but they are neither sustainable nor lead to productivity, accountability or ownership. Anything given as a dole is not capable of being attached with measurable KPIs/ KRAs. In short, these ultimately lead to a culture of non compliance, short cuts, loose accountability and falling productivity.

A classic case, farming for even well to do land owners in UP has become unviable with non availability of affordable labour due to masses getting used to being paid under

MGNREGS for atleast 100 days per annum without the expected output as would be called for in case of private employment . This being a dole , even the receiver is at the mercy of the grass root official and thus the cases of short payments / commissions / fudged records/ corruption are on the rise . The cost of administration and monitoring these programs is thus more than the actual impact.

Similarly, with the focus being on meeting disbursement targets than the outcome achieved, the officials at grass root level, except a few, are least concerned with what assets or output is being achieved out of employment generated under MGNREGS . Further , with vested interest groups getting into action with the quantum of funds under disposal and possible avenues for leakages , even the officials with best intentions finally give up to fall in line . In short, none of these schemes are able to generate or deliver the intended objectives.

Contrary to above, through the suggested scheme of shifting of cash rich CPSUs to one new SMARTCITY each, individual, accountable local employment opportunities will stand generated where the employee will get an opportunity based on his / her competence and capability and they need to continuously deliver to survive in his/her job. Thus the scheme will create sustainable, productive and accountable job opportunities leading to concrete and measurable productivity.

Further, the job opportunities being now in 100 plus pan India distributed booming centers of economy close to the living population, they can afford better standard

of living and take care of their families back home. The supplementary business opportunities will also trickle down to the catchment area to serve the demand of the stable salaried population coming to these new Smartcities.

This will also plug the unending influx of population to already over stretched Metros in search of jobs, stretching the already bursting infrastructure and civic amenities to unmanageable levels and the unemployed and under employed entering the crime market, being pushed to the wall for survival.

Thus the suggested solution aims at plugging all the experienced ills of the current interventions and at the same time reduce the pollution and traffic congestion in Metros by shifting further influx of population to these new booming centers of economy and move towards an accountable and sustainable society with the added advantage of making the already made investments in SMARTCITIES viable that too by using the idling cash surplus with the cash rich profitable CPSUs as seed capital. The other schemes of Govt. of India may continue as of now but can be dovetailed to meet the big picture.

2. **Why this proposal is being planned at the cost of the Cash Rich Profitable CPSUs which is expected to cause lot of dissatisfaction and heart burn amongst the shifted Management and employees of the affected CPSUs?**

Ans : The shifting of the purse string controllers i.e. the decision makers (the CMD and the Board of Directors) of cash rich CPSUs to new SMARTCITY, will act as a magnet

for that city, attracting their vendor partners to follow them for their own pure business reasons .Out of sight – out of business. Hence the vendor partners have to be where the decision makers are. This will thus help the new SMARTCITY to get seeded with paying population that can generate sustainable demand for all essential elements of a thriving city.

The shifted CMD & BOD and vendor partners that follow, will invest for their own comfort & necessity in offices, residential accommodation including new means of transport as well as communication to remain connected with their Ministry as well as field operations and production units as applicable. This will lead to a boom in the otherwise slowing down infrastructure, automobile & telecom sector, with trickle down positive movement in all sub sectors of infrastructure industry i.e. cement , steel, sand, bricks, plumbing, furniture, lighting , sanitary, tiles , interior design, engineering , architecture, automobile , tower , power plants , DG sets , air conditioning , ancillary industries and associated services (mason, carpenter, plumber , fitter, welder ,scaffolding , labour , mechanic etc). Each of this will generate additional business avenues and jobs.

This will have a snow ball effect on all essential needs of society i.e. infrastructure, health, education, law and order, banking, entertainment, logistics, services etc to start viable businesses in these new locations. This in turn will generate huge employment opportunities for the population of local catchment area. Any person declaring himself/ herself employable in the catchment area and running to a

Metro or mini metro and further choking that to death , will instead avail employment opportunity with in 100 kms of his / her residence with 100 plus such booming economic centers that will come up pan India with the suggested idea being applied for 100 NEW SMARTCITIES, creating uniformly distributed development pan India .

3. Will this not just lead to diversion of employment from Metros to the NEW SMARTCITIES keeping the net check sum unaltered?

Ans: No.

Consumption never grows keeping the stock on hand as a driving force but by sentiment. If this was true, a person with a pair of 30 clothes, one for each day of the month, would never have bought the next pair. Instead the person who has 30 pairs is the one who has the intensity to buy more, driven by his raised aspirations to graduate to the next level when the economic environment is conducive. Thus the investments of the cash surplus with the profitable CPSUs in new SMARTCITIES where their decision makers are forced to move, will lead to replication of schools, hospitals, colleges, malls, clubs, retail chains, service outlets etc as they now have paying population who can afford this. Increased consumption will lead to increased production and in turn increased employment.

4. **Will this shift not be a costly mistake politically as the shifted employees will resent and vote against the government?**

Ans: No. Instead it may be a positive swinger. Recent survey shows, given the opportunity , 40% of the population in

Delhi/NCR wants to move to a pollution and congestion free city .

With the present compromised quality of life in metros with rising respiratory diseases because of consistently poor air quality with maddening pollution , minimal time left for employees to spend with their families with more than 12 working hrs a day due to 4 plus hrs wasted in travelling to and from office with traffic congestion and unaffordability to lease / rent/ buy houses in business districts close to work place , unaffordable cost of schooling, health and living in metros are reasons enough for the shifted employees to soon realize the improvement in their quality of life as well as standard of living at the shifted location . Even otherwise, the change is proposed to be driven by mandating just the CMD and Board of Directors of Cash Rich CPSUs i.e. the decision makers to shift. Many pliant employees will shift to follow their bosses and many will be found willing to opt for such shift when given a choice amongst nationwide employee population for that CPSU. Thus except for the CMD and Directors, for rest of the employees it will be a redistribution by choice with NIL political impact.

With close to 30% improvement in bottomline of the shifted companies with reduced cost of operations due to cheaper real estate , reduced rates of HRA , CCA , Medical bills and improvement in productivity with more energetic and positively oriented employees with reduced time of travel and reduced exhaustion and the top management now consisting of only those who are really interested in professionally running the company than the ones who came on board for the metro location and short term gains ,

the employees Performance Related Pay / bonus / perks and privileges will see an assured rise .

The increased employment opportunities nationally, reduced pollution and traffic congestion in Metros and improved quality of life with reduction in crimes with increased employment opportunities triggered by this initiative is expected to be a serious political benefit to the Govt. of the day implementing this initiative .

5. Will the CPSUs not get hit with delays in business approvals from their Ministries with relocation away from Delhi/ Metros?

Ans: With almost all profitable CPSUs now being lead by a CMD than a MD before, most decision making powers rest with the CMD and the CPSU Board. Thus the day to day coming back to Ministry for decisions is not called for.

Further with advent of eOffice, email, fax, whastapp, scanners, mobiles, video conferencing etc, decisions as needed from Ministry can stand steered by these means irrespective of the CPSU's physical location. Worst case, for a few face to face meetings, just the concerned official can fly down to the ministry faster than driving from current metro location to the Ministry. The efficiency and cost savings accrued to the CPSU and more so, the professional environment to focus on core job than getting distracted with extraneous factors so prominent in Delhi/ NCR/ Metros, will go a long way in professionalizing CPSUs and making them more profitable, efficient and competitive.

6. **What is the underlying logic in suggesting the places for shifting the CMD and Board of CPSUs**

as recommended in the example in the note?

Ans: The location proposed for shifting must have some synergy with the core business of that CPSU so that the environment is conducive, helps build the business funnel , aids the growth of the shifted location or its vertical expertise and so on , so that the action results in a win-win game for all .

Keeping above objectives in mind,

CONCOR CMD and BOD is proposed to be shifted to a potent Port location as this will help uplift the port operations with improved container traffic with improved focus of management at the shifted Port location

IRFC, a pure Finance interest rate leveraging company is proposed to be shifted to one of the multiple new SMARTCITIES coming up on Mumbai-Nagpur MahasamruddhiMahamarg. This will create a potential financial capital away from Mumbai and seed the smartcity with banks and DIIs/FIIs. Mumbai bursting at its seems will see a viable alternative. This has to be sufficiently away from Mumbai so that work at the place cant be managed with daily travel to the new Smartcity. Only then the real growth of the NEW SMARTCITY will begin and traffic congestion and pollution in the existing metros can be reduced . If this is not done , situation will continue like that between Delhi-Gurgaon or Delhi-Noida which has lead to people continuing to manage the show by staying where they could afford and working by travelling , leading to huge morning- evening rush on roads, metro trains and severe congestion and pollution with loss of life and productivity

HSRCL, bullet train delivery organization with capital tied up from Japan to be relocated to Atul on the Ahmedabad –Mumbai rail route. This will help the CMD and Board to focus on the project away from the distractions and extraneous influences of Delhi/NCR and help the potential industrial town of Atul grow leaps and bounds with the vendor partner eco system of HSRCL relocating to Atul.

DFCCIL to Ranchi on the delayed Eastern DFCCIL Corridor. This will help the organization focus on speeding up delivery of the mandated network and the investments flowing in will help the much neglected town of Ranchi grow leaps and bounds

CIL to Naya Raipur , a city in the belt of Coal deposits in MP, CG, Orissa, Jharkhand ,Bihar leading to creation of employment opportunities in the new smartcity of Naya Raipur / Atal Nagar , leading to sustainability of investments as already done there while freeing Kolkatta from the terrible bottleneck of perennial traffic congestion .

OIL to Dholera , a smartcity waiting in the wings to take off and has OIL refinery and lubricant processing plant in vicinity

GAIL to Jhabua ,a neglected city that has a GAIL pumping station on the cross country pipeline and will immensely benefit with improved air , land , rail connectivity that will perforce be done once the Maharatna CPSU HQ shifts there

RailTel to GIFT. With its secured pan India network covering 70% of country's population, running the world's biggest public WiFi network with the data collected being of immense interest to the development initiatives

of the country as well as data monetization by the tech giants, managing the pan India Railways Signalling and Telecommunications upgradation etc, will offer immense upliftment to GIFT, the intended Fin Tech capital of the world.

7. If this proposal is of so high a benefit to the CPSUs why should they not opt for this shift on their own? Why should this need a mandate from Govt?

Ans: The short sighted interests of current management of the CPSUs is supporting the inertia of being where they are. Most leadership being either on deputation or on verge of retirement is interested in staying put where they have been last posted. For the country's holistic development, the hard decision with an integrated approach for pan India distributed development, has to be enforced from top. This is on the same lines as the necessity of enforcement of GST. Though the simplified tax structure of GST is beneficial to all but the vested interests as well as inertia resisting change needed enforcing the scheme from top with the needed governance structure centralized. On exactly the same lines, for the bigger interests of the country as a whole, a mandate from Govt. needs to be issued for the CMD and Board of Directors of Cash Rich Profitable CPSUs to shift to one new SMARTCITY each as identified, to find the closest possible synergy to the shifted CPSU.

Increased profitability of the CPSUs with this shift will be an added advantage to the Govt. helping generate bigger dividends and sustained cash flows for the economy.

8. What happens to the premises/ properties as

vacated by these CPSUs in Metros / Delhi/NCR? Will that not be a financial loss to the shifted CPSUs ?

Ans: A little deep dive will reveal that this action actually starts immediate saving of CAPEX and OPEX for the CPSU. In most cases, the premises vacated in Delhi/NCR/ Metros will help relocate one of the local/ regional offices of the company in the vacated location there by reducing rent outgo.

In most other cases, the property so vacated being in prime business district, will help quick market leasing of the same for significant and recurring returns. Only in certain rare cases, vacated property may have no alternate use for the CPSU. In such cases, the property can be offered as Regional/ local office to other CPSUs/ businesses on rent / lease/ sale improving returns and cash flow for the CPSU.

9. **Will the upheaval of shifting not affect the performance of these CPSUs in the FY in which this shift takes place?**

Ans: No.

With meticulous planning, the ground activities at the proposed place of shifting can start in advance. With migration to eOffice whose India's largest instance has been rolled by RailTel for Indian Railways and so for CIL, UTITSL and many others and can be so done for all other CPSUs, the needed approvals from CMD and Board can stand taken by the other functionaries in the CPSU even when the decision makers are on the move. With entire office managed from a laptop, shifting, migration and

renewed operations should begin from new location within a week of shifting.

10. Can this objective not be achieved by shifting one of the major offices of the concerned CPSU in the new SMARTCITY as proposed instead of the CMD and Board of Directors?

Ans: The fundamental objective of bringing sustainability to the investments as already done in new SMARTCITIES can not stand achieved unless the purse string controllers & the key decision makers (CMD and Board) of these CPSUs do not shift to the NEW SMARTCITY location. The vendor partner eco system of these CPSUs will shift to the new SMARTCITIES only when the purse string controllers of these CPSUs shift to them. It is only after the new SMARTCITY has citizens with buying capacity that the anticipated economic development will kick in. Hence for the bigger objective of a Happy and Healthy India, it is must for the CMD and Board of Directors (purse string controllers and decision makers) of the suggested CPSUs to shift to one NEW SMARTCITY each.

11. What if the projected benefits fail to kick in and the situation remains unchanged even after shifting of the CMD and Board of Cash Rich CPSUs to one NEW SMARTCITY each?

Ans: As discussed threadbare above, this is a fail-safe scheme driven by pure economic logic and is bound to produce the intended results.

In order to test a real Proof of Concept, a low hanging fruit in terms of mandating the CMD and Board of Directors of

RailTel, a mini Ratna Telecom CPSU under the Ministry of Railways, to shift out of Delhi and operate from GIFT in Gujarat on immediate basis, can be exercised . This is to support the vision of Hon.PM to make GIFT the Financial Transaction capital of the world ahead of Singapore, Hongkong, Dubai etc .

- RailTel with its reliable and secured pan India optical fiber network providing access to 70% of the country's population, will provide access to GIFT to the nation's consuming population and provide IT, ICT and Telecom services to the occupants of GIFT.
- RailTel being the World's biggest public WiFi operator on date , will provide traction to the IT/ICT/ Fintech players to look at GIFT as a business destination to associate with RailTel for Data monetization
- RailTel now being entrusted with Modernization of Railway Signalling and Telecom, a project worth Rs.1 lac Crore , will attract the world's best Signalling and Telecom vendors to GIFT to design , develop, manufacture and export the technologies to the world , creating the needed vibes at GIFT to spring forward
- RailTel will also get benefitted with these enhanced business opportunities of serving the occupants of GIFT (50 brokers , 26 Banks, DIIs, IT companies , BSE, NSE, Educational institutes , Hotel chains etc& growing) , reduced cost of operations with reduced cost of property , rentals, medical , CCA ,HRA, logistics , travel cost for its employees as compared to any Metro , improved productivity with walk to

work culture for its Corporate office employees and efficiencies of scale by developing a centralized NOC/CNOC in GIFT for its country wide operation at lower TCO (Total Cost of ownership) with 24x7 SEB power .

The standing invitation of the Hon.CM of Gujarat and the request by him to Hon.PM to shift RailTel corporate office to GIFT vide his D.O. dtd.10.10.19 stand as a perfect stage to initiate the idea.

Once the benefits are seen from this implementation, a parallel action of ordering CMD and Boards of top 100 cash rich CPSUs to shift and operate from a new SMARTCITY location each, can stand implemented on a war footing .

Digital Education yet to combat with Cyber Practices in New India

Dr Unnat Pandit,
Programme Director, Atal Innovation Mission, Niti Ayog
Ms. Ananya Agrawal

The increasing use of mobile and internet across our country, is an inflection point for a lot of products and services that can reach people and solve their problems in a way that has not been possible till now. The problems in traditional approach to education: Every student learns differently but content for them to learn is same. Their learning ability is taught and evaluated by mugging the content. Government of India through MHRD trying to revitalize the Indian education system introducing the technology for qualitative improvement in education through Education Quality Upgradation and Inclusion Program (EQUIP). The notional for designing the program revealed that despite increased enrolment, a significant proportion of children in Classes 5 to 8 in government and rural / private schools could not read text suitable for Class 2 students or do simple arithmetic their age-group may be expected to do.

---

[1] *Dr. Unnat Pandit is Program Director of Atal Innovation Mission, NITI Aayog, Govt. of India wherein the views expressed are personal and has no relation to any policy decision by Govt. of India or even in any forum.*

[2] *Ananya Agrawal is pursuing her internship at Atal Innovation Mission while studying for her masters in design from National Institute of Design, Ahmedabad*

The education domain demands the upgradation in Academic Process Life Cycle and Interventions through ICT Infrastructure. Internet service Providers, Ed-Tech Platforms end-to-end automation and integration of every process of an education institute, or providing state-of-the-art technology driven products and services to improve teaching-learning outcome in classroom. “Various analytics tools can be used to know where and why user engagement is low and how customers can be effectively engaged.

Startups in Education domain has pivotal role to play for making the digital mode of education equipped with all accessories to make the subject understand and expressed in simple languages. The student specific education is to be ensured through technology advancement. That will lead to make education more specific to the need of end users. Social & Emotional trait should also be monitored to evaluate the overall growth of child. The memorizing through learning and experiencing is important in digital education and should equip the student to recollect the knowledge they have gained and reproduce in simple and objectively.

In taking India a leap forge jumps in ensuring Education quality through digital mode, redesigning the curriculum is going to play an important role. The teachers engaged in curriculum design and inputs has to explore utilizing the creative talent of student and their academic engagement in school allow expressing their innovative skills in science, technology and humanities as well. Nowadays high school students reached out to access to technology, majority of parents did not have access to such technology advancement

when they were at this age. Still the lack of unwilling to give access to smartphones to their children. The appropriate use of technology is to be ensured. However, in such transition phase, the better offering of technology driven solutions will build the confidence of parents. The students and youth of country is spending over 45B Hrs on internet which includes the gaming on mobile / tablet. The time for keeping the layer of content monitoring and evaluation in force for ensuring that right content is being delivered. There is SOS need for all gaming applications to monitor, which developed outside India. The students and youth are spending their precious time on the gaming content, which does not have any validation or even standardized to Indian culture needs. The standard setting is required for any such gaming application offered through mobile or in any digital mode. The level of access is also required to define besides standard setting.

The time for multisensory, multidisciplinary, child-centric videos and educational content, technology to get the child attention span and monitoring is required especially in kids who are already equipped with mobile or tablets. Tracking their academic activities and other leisure work will certainly keep watch on their utilization. Tangible media interfaces, spatial and bodily restrictions the use of computer imposes upon the children, and how the restrictions would negatively affect the natural brain growth of children. Purpose of the app/digital medium being developed should serve the parents and teachers in understanding their interest and use of digital media for the purpose which is made it available. Additionally, the teaching methods, assignment design

outcome-based learning and differentiation with a level approach, classroom management, Support to teachers on Pedagogy and subject matter from ABRC and BRPs, DIET centers bridging the learning-gaps among children from low-income communities. The activities are also required to be planned to bring their attention and also enable them to use the physical actions to understand and apply the concept. The lack of hand-eye coordination will also derail their creative thought process. Application of knowledge will not only improve their engagement in using what they have learned but also make them practice applying their thoughts using a pencil and write.

A huge gap in the education standards in rural schools as compared to metro cities. Rural education in India needs a focused approach in improving quality. The ability of teachers to deliver the defined content and ensure that the content is learnt by student is big question for system. The rural-urban education quality gap is increasing and inclusivity, accessibility and adaptability in rural ecosystem is going to create load on improving the quality. At the rural areas, family is one of the factors that determine their child performance in education. Students in rural areas have low performance compared to students in urban areas because it relates to their parent's education as well. Majority of parents in rural areas are less educated than parents in urban areas, however their willingness to impart the best quality education is highest.

In order to bridge the gap between the urban and rural areas and ensuring quality of education to provide an equal platform for career development to students in rural areas

too. Students and teachers are still hesitant and apprehensive of technology instillation in the traditional education pattern. The time for improving utilization of technology in education is making education quality in classrooms much more interactive, innovative, all-encompassing, and meaningful. With technology making interesting inroads, news systems and learning processes have taken form, leading to a sea change to the way education is perceived in the country. The blended system of education provides different avenues of understanding the concept, helping to develop critical thinking and problem-solving skills in the learner. The language lab solutions have removed the ever-existing language barrier between different regions with easy access to fun, easy, and effective language learning resources. The innovative technological solutions have provided complete ease of communication, training, and 24X7 learning with its anytime accessible resources. The education quality in the era of New India is going to take a pole vault jump to deliver an impactful outcome.

A Case Study of Botnet Attacks in an ISP Network

ITS Shubha Bhambhani,

Principal General Manager (C&M), Bharat Sanchar Nigam Limited (BSNL)

This paper presents a case study of recent Botnet attack in a leading ISP network. Government organisations like Computer Emergency Response Team- India (CERT-In), National Critical Information Infrastructure Protection Centre (NCIIPC) continuously monitor the cyber threat surface of India. These organisations provide necessary advisories to all stakeholders for taking required actions to secure the devices from cyber-attacks.

In this case study, the characteristic of the attack was studied, a comprehensive security measures to detect and prevent similar attacks in the future has been developed and implemented. The key measure is blocking of unwanted ports in Core and Access network servers/routers. In addition to blocking, regular scanning of modems/ONTs having default credentials, rectifying the faulty modems and to prevent such attacks in future and conducting a regular security audit. The audit includes monitoring network elements to identify abnormal behaviour, monitoring system processes to identify improper usage, keeping the network elements, servers, modems and ONTs up-to-date with new patches.

Here, an attempt has been made to understand gaps which need to be fixed to comply with the policy, standards and

procedures laid down by Security agencies to protect critical infrastructure of India. The study tries to bring out the native methods, which can be issued to detect critical cyber threats and take precautionary actions to mitigate the threat and minimise the impact.

An Internet Service Provider Infrastructure is considered to be critical Infrastructure. In an ISP, the core MPLS network, the access network, the ISP nodes and the customers form the supply chain management system. For any threat to materialise, it is important to understand at which stage the failure of the supply chain management has occurred for fixing the issue. Only then one can work towards developing a secure network and be prepared to face critical cyber threats.

The growing popularity of the Internet also generates new waves of security attacks which are more advanced than their predecessors. Of these new attacks, Botnet receives a lot of publicity due to its magnitude and capability to cause severe financial loss through Distributed Denial of Service (DDoS), phishing, spam or identity theft. Bot (short for robot) is an autonomous program running on a compromised computer, and these Bots could be controlled remotely by a hacker to launch attacks at a specified time against a specified target(s). Botnets are collection of computers infected with malicious code that can be controlled remotely through a command and control infrastructure.

In one of the ISP Network, Mirai Botnet attack on ADSL modems occurred in the month of July 2017 and on FTTH ONTs in the next month itself. First instance affected the

Broadband services provided through ADSL Modems and the second instance affected the FTTH (Fibre connections) Services provided through ONTs. In both the instances, the CPEs (Customer Premises Equipment) of specific vendors were affected. Since both the attacks were first of their kind notice in the Network, it consumed considerable time for analysis.

At the first instance of occurrence, the ISP team had carried out a detailed analysis of the case, and it was found that modems supplied by specific models were affected during this attack. In depth discussions with concerned vendors, CERT-in and MeiTY , revealed that the vulnerability is because of the Default username and password, WAN side ports open, ACL disabled (No firewall), Provision to enter a command at NTP server IP address location.

During the second instance, Broadband / FTTH Services of the ISP were again affected in some parts of the country. The specialised teams carried out a thorough analysis across various network elements of access network, core MPLS, Servers and FTTH etc. While carrying out the analysis, spurious traffic was observed from specific makes of ONTs. On detailed analysis, it was found that different set of default username and password, WAN side access is open by default, in one of the makes of ONTs deployed in the ISP network. It was also observed that ACLs were disabled in ONT, VoIP Ports are open. Based on the observation and findings, blocking of ports was carried out at Core and Access Network Elements. Field units were asked to rectify and reconfigure the faulty modems to restore the services and to prevent such attacks in future.

Corrective Actions

- Blocking of ports for ONTs of affected ONTs .
- Filed units were advised to factory reset the modems, disable TR69 services, enable ACL, disable DMZ.
- Instructions issued to field units to religiously follow the security guidelines.
- Affected modem Vendors were requested to give a new PATCH and to provide updated firmware with a strong password policy, robust firewall addressing all the security concerns.
- Bringing all Broadband Network Gateways under more secured DDoS solution deployed in Core Network
- Procuring appropriate tools to identify and mitigate botnet attacks.
- Guided the filed units about the list of IP addresses which are affected/ impacted by such virus/ malware/ attacks shared by CERT-in and take necessary action
- Field units were asked to inspect the customer premises and do the required changes at customer ends.
- Necessary trainings were provided to the concerned staff, handling such security issues.
- All vendor partners were requested to analyse the safety & security of their equipment/ Network Elements/ Servers/ IoT devices/ Applications etc.
- Formation of Security Team to exclusively audit network elements, study various security measures to

be implemented, monitor the trend and take necessary action proactively.

Conclusion

Botnet attacks in the ISP network not only created a bad image for the organisation, but also customer dissatisfaction due to interruption of the services. If corrective actions were not initiated, it might have further affected thousands and thousands of customers apart from badly affecting the ISP's reputation. Although it was not clear, whether the hacker has used ISP environment to launch a real attack against another target, the potential damage to ISP network environment was very alarming. The analysis presented in this case study is expected to help ISPs to be aware of the risk and implement protective measures against the Botnets. In addition, it is emphasised that that reactive methods for network security are not sufficient and proactive methods are required. Disabling unused services, monitoring active services, keeping system and services up-to-date with patches, and conducting regular audits are important proactive measures for ensuring security of any ISP Network.

Empowering Agencies With Comprehensive Data Gathering & Technology Platforms

Ms. Hemavathy M,
Member (Senior Research Staff), CRL, BEL

Ms. Rita Shrivastava,
Sr Deputy General Manager, BEL

AVM Pranay Sinha VSM (Retd)

Introduction

The ever-growing Internet continues to touch billions of lives through **Voluminous** Data which are generated in numerous forms like formatted, unformatted, structured, semi-structured and unstructured contents. It originates from **Variety** of sources of different types which includes traditional transactional text databases, contents of multimedia, social media and from Internet of Things (IoT). The data gets generated at ferocious Velocity, and thus a pool of **Big Data** is under perpetual creation. The Advances in Information Technology is now enabling users to capture, communicate, aggregate, and analyze from this

enormous **Pool of Data**, through newer Data processing techniques, storage technologies and analysis methods. This is a paradigm shift in Data Analytics that is highlighted in this paper. However, the most important question is **'Who should be empowered to Own Data, Collect Data and Distribute Data'**. A proposal is submitted herein.

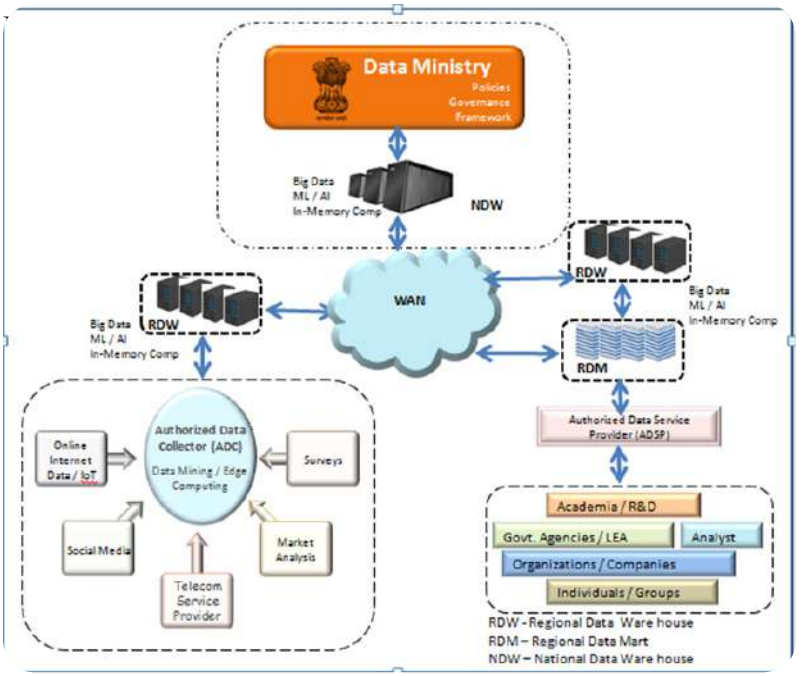
PROPOSAL

The ability of the internet and related media to deliver networking capabilities is growing exponentially, and the whole world is moving towards a more connected digital-driven economy. This gets evident from the advent of digital-centric solutions like Social Network Sites (SNS), e-Commerce, e-Governance Portal and Services. More and more small-mid and large enterprises are fast-moving to the Web to equip themselves with better opportunities by harnessing the power of Information. Big Data Analytics as a technology has been increasingly embraced by Retailers, Financial Services, Insurers, Healthcare Organizations, Manufacturers, Energy Companies, Defence Sector and Other National Security Agencies. It also facilitates for connecting and combining people/groups for a specific purpose by allowing and authenticating them and enabling to further exchange Information.

The concept being proposed in this paper is that continuously generated data be channelized into National Data Warehouse (NDW) through regional Data Warehouses (RDWs). These GoI shall be own these Data Hubs. In fact, this Proposal is for creation of a separate Data Ministry to manage this entire affair. It would be Data Ministry's responsibility to

create a robust Policy Framework of rules and regulations to ensure safety and security of the Data Hubs.

It will be the jurisdiction of Data Ministry to empower various agencies, Govt & Private, for gathering the data, ensuring that the privacy of public is not encroached. Also, it shall be ethically collected without violation of fundamental rights. These agencies will first collect data region-wise of the country and will supply to RDWs which in turn will transport these data after Extraction-Transformation and Loading [ETL] to central agency i.e NDW. After Post-processing of the data, it can then be loaded to various Regional Data Marts (RDMs), functioning under the operational zone of RDWs. And from RDMs, data can then be procured by various . This proposal of the National



Therefore a framework with the following fundamental principles is proposed:-

- It proposes creation of Data Ministry that would construct relevant framework and architecture with formulation of robust rules and regulation for smooth functioning of NDMP.
- Ensure Security, Privacy and Authenticity of data storage and distribution, keeping in view the Ethics and Fundamental rights.
- Data Ministry under IT Ministry to empower various Agencies for Data gathering which shall be region-wise and supply data to the Regional Data Warehouses (RDW) which shall transport to NDW after ETL processing.
- At NDW/RDWs, a variety of data mining technologies may be employed including but not limited to Analytics, In-memory computing, Cloud computing, Artificial Intelligence techniques like Machine Learning and Deep Learning for intelligent and speedier processing and transportation.
- The processed data shall be loaded to various Data Marts- under RDWs, from where data can be procured by various and customers like:-
  - » Agencies (Including National Security Agencies) – Defence Forces, Govt Intelligence Agencies, Law Enforcement Agencies [LEA], Police, etc.
  - » Policy Makers of GoI.
  - » Business Houses and Industries for sector-wise data collection and to derive actionable Intelligence for way ahead.

  - » Educational Institutes.
  - » Social Service Provider / Organization / NGO/ SCM/ERP.
- The System shall provide various insights into the dynamics of the various sectors and aide Govt Bodies in formulation of Policies, Advisories and Guidelines on a continual real-time basis and Prediction for:-
  - » Human Resource Development and Skill Mapping.
  - » National Level Planning for every citizen e,g based on qualification, skill-set and opportunity Database, Helping citizens in need, providing access to needed services and many more.
  - » Identification of newer Avenues/Gaps/Areas for Employment Generation.
  - » For ensuring transition and reliance on Indigenous and homegrown technologies.
  - » To evolve an efficient Feedback Mechanism for fine tuning the above System.

Technologies Involved

The Establishment of such a framework calls for a robust mechanism of Data Collection, Processing, Distribution and Ingestion methods as summarised below:-

- **Modes of Data Collection.**
- **Data Gathering and Processing Approaches.**
- **Technology trends in Data Gathering.**

Modes of Data Collection

- **Online/Web Surveys** are perhaps the data collection

method that has developed most rapidly and are more engaging than other survey methods.

- **Mobile Phone Surveys** are popular, cost-effective, and for effective decision-making.
- GPS Tracking for the movement pattern of consumers is essential, as location and in-context dynamics can be the key drivers for decision-making.
- **Web Tracking Technology using Data Mining techniques** allows monitoring websites in terms of time spend by users in surfing, when they visited, which links are clicked through and so forth for online behaviour and interests which are primarily used for advertising effectiveness.
- **Social Media Monitoring/Listening**. Many tools allow researchers to extract and analyze social media data for predicting public sentiment /perception for decision making.
- **Transactional Data**. Financial sector, mobile network operators, retailers, etc. are collecting many types of transactional data which can be utilized for the effectiveness and efficacy of financial product marketing.

Data Gathering and Processing Approaches

- Combining multiple types of data: Organizations need to integrate large and small volumes of data from internal/external sources (like IoTs) in structured/unstructured formats to yield new insights for predictive models by extracting data to monitor people and surroundings.

- Faster, efficient Technologies and Methods of Analysis: Analytical methods and machine-learning techniques are widely used to produce actionable insights at a much faster rate, with more accuracy and with maximum transparency.
- Embedded analytics: **Embedded analytics are widely employed which integrates analytic content and capabilities within business process applications. It also improves the speed and impact of data collection as it does not require sending data across network and getting processed by multiple algorithms.**
- Data Discovery: **To develop products and services based on big data, organisations need a capable data discovery platform for data exploration that should limit the depth of information exploration and have low complexity of analysis.**

Future Technology Trends

- In-Memory Technology: **To speed up the big data processing In-Memory techniques are widely utilized. In a traditional database, the data gets stored in storage systems equipped with hard drives or solid-state drives (SSDs) wherein In-memory technology stores the data in RAM, and hence increasing the speed of storage and operations (read/write) multi-fold.**
- Machine Learning: **Today's most advanced machine learning and artificial intelligence systems are moving "beyond traditional rule-based algorithms to create systems that understand, learn, predict,**

adapt and potentially operate autonomously.

- Intelligent Security: **Organizations' security log data can provide significant information about past cyber-attacks/events. Organizations can use this information to predict, prevent and mitigate future attacks by incorporating big data analytics capabilities with AI based automated response to events/incidents.**
- Edge Computing: **Here, Data Analysis happens close to the IoT devices/sensors instead of in a data centre/cloud. Hence it hasless data flowing over their networks, which can speed-up the analysis process andsave on cloud computing costs. It allows organizations to delete IoT data that is only valuable for a limited amount of time, reducing storage and infrastructure costs.**

Role of BEL as Information & Communication Technology (ICT) Provider

To establish a robust, secured National Data Management Platform (NDMP) under the aegis of Data Ministry, the need will be to harness the indigenous potential and capabilities existing with-in the country. In this regard, the domain expertise of Bharat Electronics Limited can always be leveraged. BEL, as a Defence PSU, can contribute to various facets of Data gathering and analysis framework. Paramount importance is to address security needs through various layers and dimensions (Defense-in-Depth) as depicted in Fig 2. It illustrates the security architecture for providing end to end security.

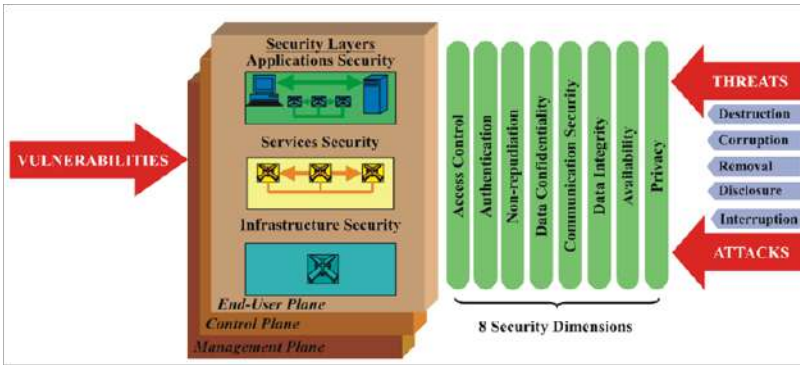


Fig 2. Security Architectural Elements in ITU-T Rec. X.805

CORE ICT TECHNOLOGIES & BEL'S IN-HOUSE CAPABILITIES:

- **System Integrator (SI Role):** BEL can contribute as a System Integrator, Setting up of State/Central Data Hubs/Centre for Data gathering eco system of Empowering Agencies with comprehensive Data gathering and Technology Platform.
- **4G Long Term Evolution (LTE)/5G:** LTE based customizable eNodeB and User Equipment (UE) by utilizing the design services of the selected technology partner. Design and development of proprietary security, ECCM, protocol level customization and Quality of Service (QoS) customization and smart jamming for the 4G network. Even 5G is getting standardized and momentum in India (TRAI has recently launched white paper on "Enabling 5G in India" along with rollout plan). BEL has planned to work in the following 5G areas - Massive MIMO, Smart Jamming for 5G network, 5G based eNodeB and UE for Defence/Civilian Network etc.

- **Switching & Routing Platforms**: In-house Switching and Routing platforms with L2 and L3 switch fabric and Switching protocols like RIP, OSPF and custom flooding protocols.
- **HW & SW Encryption Technologies:** OSI Layer 2 -Layer 7, SDH/PDH, STM1/16/64/OTN Encryption Frameworks and Appliances with SAG certifications. 1G-10G Encryption platforms are already deployed in Tri-services and various GoI agencies. BEL is successful in 100G Encryption Platform realization and is presently carrying out design & development of 400G Encryption technologies. BEL has International Certifications like Common Criteria Security certification with Evaluation Assurance Level (EAL4) for Data at Rest and Data during Transit based software security framework.
- **IOT Technologies:** Expertise available on IoT framework to meet the needs of Data gathering and analysis platform. Development of data acquisition techniques for end nodes of IoT network using various communication protocols, Architecture for IoT middleware, Predictive maintenance using IoT system, Facilitating C2I operations to derive CoP (Common operating Picture) with data fusion techniques and integrating with edge processing for real-time decision making.
- **Cloud and Data Analytics Technologies:** Expertise available with BEL on conceptualization of Cloud architectures including Compute (servers), Control

(servers), and Storage/Networking technologies based on the specific deployments. Work is in progress on Big data analytic algorithms, Forecasting or prediction modelling, Decision trees, Random forest, Time series analysis, Classification algorithms, Content based filtering, Machine Learning, Deep Learning, Complex Event Processing, Geospatial analysis.

- **Blockchain Technologies & platforms:** Expertise on Block chain technology Platform realization & on open-source blockchain framework is available.
- **Cyber Security technologies:** On the following aspects BEL can render technological support:
  - » Frameworks for Security Operation Centre (SOC).
  - » Software Unified Threat Management Systems/ Intrusion Prevention Systems.
  - » Deep Packet Inspection device along with Data leakage prevention features.
  - » Encryption appliances & Framework.
  - » Identity and Access management.
  - » End-point Security solutions.
  - » Data diodes which provide unidirectional traffic flow.
  - » Secure Phone for GSM and CDMA networks.
  - » Secure Tablets.
  - » System on Chip (SoC).

- System Hardening with OS Hardening.
- Network Hardening including Servers and NW appliance hardening.
- Security Testing with Vulnerability Assessment and Penetration Testing.
- Cyber Forensics [Mobile forensics, Network forensics, Memory Forensics].
- Data at Rest security solution for critical servers of Data gathering platform.

BEL has rich experience of deployment of Military security appliances for various programs of tri-services like Army, Navy and Air-force with highest security grading offered by Indian Cipher Policy Committee. BEL has also executed various complex Communication, Control & Information (C2I) Systems and Networks with complementing technologies of both indigenous and COTS variants for secure and robust deployments. Therefore, BEL proposes realization of Indian own ICT eco-system with home-grown equipments, networking infrastructure, indigenous hardware/application software, and security protocols. These solutions will provide complete trustworthiness of the underlying ICT infrastructure which enables effective realization of Data gathering and analysis.

Conclusion

Being said “Data is the new fuel”, the emergence of Digital based economy; the power of Information and Data is at the heart of the Five Trillion Economy mission of the country. It is the need of the hour that every bit of data generated has to be collected, collated and processed

for the economic growth of the Nation. Big Data poses opportunities, challenges and benefits for businesses and e-commerce of the country. Enhanced data sharing within stipulated rules and regulations, with efficient decision support through advanced analytics, would enable to create innovative products, services and business models. Effective usage of emerging technologies such as IoT, Edge computing, Artificial intelligence & Cyber Security, enables organisation to effectively collect and process the priceless data which can be used for betterment of various stakeholders with numerous value additions and competitive advantages.

However, at the same time, it is also felt that no economy can thrive for long on borrowed concepts, technology, products, and aspire to become a Super Power. Therefore, the need is to strike a strategic balance between vision and execution. It is time to lay a stronger foundation to harness the available Data-Pool and leverage the hidden opportunities. It is envisaged that the citizens of 2030 need to have an effective framework for data-driven decision making at their fingertips. The suggested model will go a long way in realizing this dream.

DISCLAIMER:-

The view expressed by the authors are in their individual capacity and does not represent the company policy by anyways.

Cybersecurity-A Continuous Challenge

Mr K K Minocha,

Deputy Director General Broadband USOF, Department of Telecommunications (DOT)

Everyday new cyber vulnerabilities are on the rise due to growing Digital space comprising 24×7 online phenomena for Humans, Sensor based Internet for things (IoTs) becoming ubiquitous at homes & industries & increasing usage of Chatbots: machines talking to Humans & vice versa makes Cybersecurity a continuous Challenge, multidimensional & more complex.

Article touches some of the core critical Vulnerabilities we as nation face today as do many other.

Vulnerabilities include Manufacturing supply chain (from network equipment to user devises), Telecom Service supply chain of providers with underlying vulnerabilities of Optical fibre cable infrastructure & need for End to End Trustworthiness of these chains. Emphasis also laid on user vulnerabilities and need for appropriate skills to understand them continual basis in order to cope up with them.

These require to be factored in Nations cybersecurity strategy.

Further the context of cybersecurity is everchanging due fast technological changes globally. Both local & global context will determine its shape in deep Tech era.

1.0 Introduction:

Fueled by fast changing DIGITAL frontier technologies & **24×7 online phenomena** for Human beings, Sensor based Internet for things (IoTs) becoming **ubiquitous** & increasing **usage** of Chatbots:**machines talking to Humans & Humans talking to machines**makes Cybersecurity a multidimensional complex topic with many facets affecting multiple stakeholders in ever changing scenario and involves deep local context in the life any DIGITAL nation embarking on DIGITAL Transformation keeping global developments in mind.

Digital Transformation (DT) involves primarily use of technology and data to drive innovation & better business outcomes. DT primarily relies on the following technologies: **Cloud Services, IoT, Mobility, AI & ML.**

1.1 Above complexity is captured by areal-life example in news of 14 Dec 2109 "New Orleans Declares **State Of Emergency Following Cyber Attack":**

1.2 "The City of New Orleans has suffered a cybersecurity attack serious enough for Mayor LaToya Cantrell to declare a state of emergency.The attack started at 5 a.m. CST on Friday, December 13, according to the City of New Orleans' emergency preparedness campaign, NOLA Ready, managed by the Office of Homeland Security

and Emergency Preparedness. NOLA Ready tweeted that "suspicious activity was detected on the City's network," and as investigations progressed, "activity indicating a cybersecurity incident was detected around 11 a.m." As a precautionary measure, the NOLA tweet confirmed, the city's IT department gave the order for all employees to power down computers and disconnect from Wi-Fi. All city servers were also powered down, and employees told to unplug any of their devices."

Article tries to touch **some of the aspects & gap areas** in Cybersecurity that need critical assessment & require to be factored in National Cyber Security Strategy (NCSS) as below:

2.0 Relevance of Stakeholders:

The possible stakeholders with stake in Cybersecurity are:

- Nation itself
- Society at large
- Tech innovators:Academia,R&D labs, Investors
- Tech Standard making bodies
- Manufacturing industry
- Service providers
- Ethical hackers & unethical hackers by (default)
- All direct users: Governments,Private,business institutions,individuals
- All indirect users e.g. Even DIGITALLY illiterate beneficiaries of technologies in Smart cities,at home etc.

- Municipalities local bodies & authorities
- Policy makers & Regulators
- Law makers & practitioners
- Economy at large
- Communities & Society
- Global bodies like UN, World bank etc.
- Entire Humanity at large.

3.0 Context of National Cybersecurity Strategy Development& sub strategies:

National strategy development requires to address needs, ground realities& concerns in local context of various stakeholders & substrategies to deal each group with central theme of securing nation to be meaningful keeping Global developments & aspects in mind.

4.0 Cybersecurity plans Always in Beta:

Coping Cybersecurity challenges is a continuous work in progress and cyber plan is always in BETA mode as DIGITAL technologies grow at very fast rate percolating deeply into every sector of economy & personal lives.

5.0 Guarding the unintended consequences of Technology:

It needs to be borne in mind that all technologies bring with them Good, Bad & Ugly as inseparable package as our past experiences provide us enough Learning e.g. Plastics,Nuclear, Processed foods etc. Endeavour should be to guard against unintended consequences as early as possible.

6.0 Trust worthiness of Manufacturing supply chain:

Trust worthiness of vendors is Absolute need for Cybersecurity in today's digital era.

Supply chain comprising of entire range from Semiconductor fab design, IPRs to its manufacturing and same for OEMs in creating a secured trust worthy Network equipment & User devices for a DIGITAL nation is well acknowledged cybersecurity necessity to be **put into practice for long term.**

Self-reliant Domestic Manufacturing supply chain needs to be created for long term Cybersecurity as it's a is significant gap area

Vendors must ensure that what they supply viz. All the Network equipmentto Telecom Service Providers, defense& other institutional users as well as the end user computing Devices to individuals like smart phones & Home automation devices.Furthermore, IoT sensors, Industrial automation Sensory devices for Operational Technologies (OT) need to be manufactured with assurance for security.

7.0 Trust worthiness, Readiness Assessment of Critical infrastructure:

In the UK, Government has declared 13 national infrastructure sectors: Chemicals, Civil Nuclear Communications, Defence, EmergencyServices, Energy, Finance, Food, Government, Health, Space, Transport and Water. Several sectors have defined 'sub-sectors'; Emergency Services for example can be split into Police, Ambulance, Fire Services and Coast Guard.

Whereas in USA there are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

In our country the sectors that have been designated as critical are Defence; Banking and financial sector; ICT and telecommunication; transportation; power; energy; the Ministries of Home Affairs, External Affairs and Heavy Industries; and NitiAyog.

We have to review & formulate our own definition Critical infrastructure our local context& prepare action planfor each sector.

The definition of critical infrastructure also will be in beta. Each sector of economy will have to factor in sector specific special security requirements.

8.0Threats in Operational Technology used in industries

Cyber threats are a greater risk in the OT environment than the IT environment. Where past attacks primarily targeted data theft, current and future attacks can hijack control systems and logic controllers that operate critical infrastructure with the intent to cause physical damage and outages. Utilities are concerned by the unique characteristics of OT environments, including a focus on availability, reliability and safety.

The risk that cyber-attacks pose to the OT environment is

increasing in frequency and potency as malicious actors' ability to accurately target critical infrastructure assets improves, causing even greater consequences for utility sector operators, managers, and executives

9.0 Trustworthiness of Service supply chain:

Similarly like manufacturingchain Vulnerabilities of a **untrustworthy Telecom connectivity Service supply chain** can play **havoc** with security and TSPs & ISPs have a major role responsibility to play in ensuring network secured at Physical layer & other layers of ISO data reference model.

Fundamentally internet connectivity that rules & runs businesses, governments, private institutions & our individual lives & critical infrastructure comprises of a tandem of 4-Pieces or segments of network connectivity & constitutes Internet Services Supply Chain.

Four pieces are:

1. **International** connectivity of subsea cables & Satellites
2. **Domestic** core connectivity
3. **Middle** mile or metro network connectivity
4. **Last mile** connectivity to end users

Each of above connectivity pieces needs to be trust worthy & secured.

In addition to 4 pieces **four more pieces** need to be cyber safe:

5. **Service providing** cloud (including SAFE PLAY STORES with safe APP CONTENT)

6. **End user devices**
7. **Safe apps & content** (Non malicious content)
8. **User** skills & awareness (in being digital online 24x7)

Security of the chain will be limited by weakest link of the chain.

Entire connectivity SERVICE SUPPLY chain could be serviced by a single vertically integrated operator holding unified telecom License for all pieces e.g. Bharti Airtel or BSNLetc.

Alternatively it could be interconnection of 4-different separately Licensed pieces Service providers having respective piece Licensed& regulated separately forming an end to end internet supply chain.

Each licensed connectivity piece of telecom network has its own dynamics & Ecosystem in the competitive space.

While TRAI regulates 4 pieces of connectivity remaining other four pieces are grey areas with agencies & authorities handling them impart greater attention

10.0 OFC FORMS SPINE OF DIGITAL ECONOMY:

Optical fibre cables forms a Common Thread of Connectivity service supply chain in each of above connectivity pieces.

In fact OFC forms SPINE of DIGITAL economy viz. Data centers, 5G mission critical use cases totally depend on OFC that also supports with wide number of users including smart cities, Private institutional networks etc.

OFC can be thought of as single largest passive network element (NE) of telecom& requires attention from

cybersecurity perspective too.

11.0 THE VULNERABILITY OF FIBRE OPTIC CABLES& POSSIBLE VULNERABLE LOCATIONS

Eavesdropping on fibre optic cables is a great deal simpler today than it was previously thought when newly inducted in Telecom networks.

Due to vast developments in optical technologies its well recognised that OFC can be tapped without even Service provider being able to detect the intrusion This affects Security of Data in transit or motion.

Which fibre optics are being used by whom is relatively easy to determine as the individual cables in a cable loom are marked for maintenance purposes.

In larger cities and financial centers, optical network vulnerabilities are particularly magnified for systems in multi-story, multitenant buildings, such as high-rises, where users often occupy a number of non-adjacent floors. Optical cables linking the telecommunication facilities typically travel in risers or elevator shafts where there isno existing monitoring or security capabilities. Organization simply do not realise that their information and communications are simple to extract via an easily placed tap in such easily accessible common areas. Telephone closets, cages, conduits, risers, shafts, parking garages, manholes, subways, telephone poles and many other areas are all accessible to place fiber taps.

12.0 Review of Gaps in Practices followed by TSPs make OFC vulnerable:

Assessment of Ability & Capacity to plug vulnerabilities of OFC deployed by TSPs need to be carried out carefully.

Assessment is necessitated due to increasing applications of public networks for value & sensitivity of data has raised it's criticality & so is corresponding interest of attackers& incentives to tap OFC data wealth.

At present the Casualness with which OFC cables meant for UG laying are put overhead OFC on trees, poles, on the ground along nallahs gutters (be it due to ROW issues or competitive pressures or altitudinal issues) makes them vulnerable both from QoS reliability angle as well as Cybersecurity purposes as it gives easy unhindered open access to criminals to tap OFC.

On this issue TELCOs are so far blissfully relaxed & perhaps oblivious of it have to awaken to the changed scenario and act in view of criticality & compliance requirements of personal Data protection laws similar to GDPR etc.

This Changed scenario also calls for assessment from Risk Management perspective and no longer it can be ignored. They have to make the necessary investments in cyber security countermeasures against OFC vulnerabilities as mission critical users due to their increased awareness themselves will seek security assurance from them & also as part of Regulatory compliance.

Cyber security obligations under Telecom License terms &

conditions may also need review.

13.0 SUBSEA CABLE VULNERABILITIES & DATA ESPIONAGE:

Changing scenario &increasing number of Vulnerabilities of Subsea cables calls for attention & action.

Submarine OF cables for international connectivity are owned generally by consortium of players & generally operated & maintained by such groups. Indian Licensed operators have agreements with consortium.

A new trend is emerging with few Submarine cables are owned in entirety by single investor. Recently biggies like FB & Google have started deploying subsea & on land OF cables because of high stakes.

With **increasing interest** in value of Data, corporate espionage & by other agencies hacking Submarine cables makes the sea bed of OF cables a **parallel industry**.These cables offer national data of a country to international hacking interest groups

*The **consortium agreement** may need a review as long term cybersecurity necessity.*

Quoting from a reference below captures the seriousness of problem:

"It might seem like a nightmare scenario. A terrorist organization or nefarious nation state decides to derail the global internet by faulting the undersea fiber optic cables that connect the world. These cables, which run along the ocean floor, carry almost all transoceanic digital communication, allowing you to send a Facebook message to a friend in Dubai, or receive an email from your cousin

in Australia

US Navy officials have warned for years that it would be devastating if Russia, which has been repeatedly caught snooping near the cables, were to attack them. The UK's most senior military officer said in that it would "immediately and potentially catastrophically" impact the economy were Russia to fault the lines. NATO is now planning to resurrect a Cold War-era command post in part to monitor Russian cable activity in the North Atlantic.

THE RISK IS REAL

Secret Services in the United States have detected espionage equipment illegally hooked into Verizon's fibre optic network close to a company – just before the quarterly results were about to be published. The investigating authorities

believed that terrorists wanted to bolster their finances by profiting from the gain in the price of shares."

14.0 COUNTERMEASURE SOLUTION TO OPTICAL TAPPING:

Proactive security measures, however, enable the immediate determination of anintrusion event and can identify the extract location in the fiber plant of the intruder in real-time.

A comprehensive combination of proactive and reactive security methods that not only protect the entire fiber optic carrier signal from eavesdropping, but also allow the interception of intruders, is highly desirable. Some vendors like Oyster Optics, Cienna claim to have developed patented groundbreaking optical security, monitoring, intrusion detection and breach localization solutions for

today's global optical networks.

14.1 All public& private network operators their respective clients are completely vulnerable to the tapping and stealing of their mission critical communications and information.

The underlying vulnerability of the global optical communications infrastructure has not been publicly debated mainly because suppliers, operators and users have failed to understand the severe threat and because there have been no effective solutions available until recently to counteract such occurrences.

14.2 Further suppliers & operators have not yet integrated optical security technologies & thus tapping incidents are rarely detected &never publicised for obvious reasons of brand protection and risk mitigation.

15.0 Capacity building

Capacity development & Creation of an abundant workforce of cyber professionals skilled in cyber security for all mission critical sectors with frequent skill upgradation training should find apriority for any nation conscious of protecting itself form todays evil forces hungry of datain Digital world.

16.0 Future Outlook of today's Counter measures itself are Vulnerable:

Whatever counter measures we employ today for cyber safety can't be eternal as fast technology changes throws new challenges & make the counter measures or security strategy obsolete.

17.0 Quantum supremacy -A Big DISRUPTOR

Technological Disruptions are order of the day. Latest challenge is expected from Quantum computingfrom its mighty "power"- exponentially more powerful than even the most advanced digital machines.

17.1 One of the biggest threats concerns encryption:

As per the 2019 Global Risk Report **Encryption forms the "scaffolding of digital life"**

Encryption provides the security and privacy for our online lives – from banking and homes to business and healthcare. It protects everything from sensitive personal data to state secrets.

But what is considered safe encryption today will soon be undermined by quantum computing. It has been estimated that it would take quantum power of 4,000 qubits to break today's "strong" encryption keys.

Quantum computers are yet to take off.

17.2 Estimates suggest we may see this capability by 2023, and it will take longer for these machines to become reliable. However, **weaker encryption algorithms may be threatened sooner,** and the clock is clearly ticking on all of today's methods.

17.3 At the same time the **good news is that quantum-safe encryption algorithms** are already being developed by companies including Google and Microsoft. But they are still in the theoretical and testing stages.

The main challenge is retro-fitting these new approaches into existing systems.

So what should be protected by these quantum-safe algorithms?

The Standards body ETSI suggests the following list of **critical infrastructures:**

- Government and military communications
- Financial and banking transactions
- Confidentiality of medical data and healthcare records
- Storage of personal data in the cloud
- Access to confidential corporate networks

Quantum computing is an exciting development that promises a world of opportunities. To make it safe and sustainable for larger public good, we must follow the ethics and responsible innovation. Our focus cannot be a case of power or security. It must simultaneously be both.

18.0 ITU &QUANTUM COMPUTING

ITU is also accelerating its preparations for the arrival of quantum information technologies – technologies based on the properties of quantum physics – recognizing that these technologies will be capable of solving problems far beyond the reach of classical information technologies.

This problem-solving capability presents significant threats to existing security. Approach at the same time disruption opens new opportunities as well.

A new ITU standard for **'Quantum-safe'** solutionsdescribes the networking concepts to underpin Quantum Key Distribution (QKD), a means of enabling secure encryption and authentication in the presence of the unbounded

computational power to be introduced by quantum information technologies.

The standard – ITU Y.3800 "Overview on networks supporting quantum key distribution" – describes the basic conceptual structures of QKD networks as the first of a series of emerging ITU standards on network and security aspects of quantum information technologies.

19.0 Conclusion:

Subject of cybersecurity must receive continuous attention of all stakeholders. Both Manufacturing & Service supply chains for critical infrastructure should receive both short & long term focus.

References

1. *https://www.wired.com/story/russia-undersea-internet-cables/*
2. *https://www.researchgate.net/publication/299656513_The_Vulnerability_of_Fiber-_Optics_communication_Systems_The_Role_of_Optical_Tapping*
3. *https://www.weforum.org/agenda/2019/07/why-quantum-computing-could-make-todays-cybersecurity-obsolete/*
4. *https://news.itu.int/new-itu-standard-networks-support-quantum-safe-encryption-authentication/*
5. *https://www.forbes.com/sites/daveywinder/2019/12/14/new-orleans-declares-state-of-emergency-following-cyber-attack/#47083f4b6a05*

BSE 24x7 Next Generation CSOC

Mr Shivkumar Pandey

Group Chief Information Security Officer, Bombay Stock Exchange Ltd

Established in 1875, BSE is Asia's first & the Fastest Stock Exchange in world with the speed of 6 microseconds and one of India's leading exchange groups [1]. Over the past 144 years, BSE has facilitated the growth of the Indian corporate sector by providing it an efficient capital-raising platform and thereby of significance as National Critical Infrastructure [1]. Today BSE provides an efficient and transparent market for trading in equity, currencies, commodities, debt instruments, derivatives and mutual funds [1]. In BSE's highly interconnected and interdependent financial ecosystem, cyber-attacks may have catastrophic implications for the entire financial system of India and consequently have impact on world's economy. This makes cybersecurity a critical business factor for the BSE.

In order to ring-fence itself from global cybersecurity threats, a compressive and holistic approach was taken to address the threat landscape spanning across all domains of cybersecurity and Next Generation 24x7 Cyber Security Operations Centre was built with more than 25 niche and advanced technologies like Anti APT

for protection against latest malware and ransomware & mitigation of threats like zero-day attacks, Cognitive Analysis and Artificial Intelligence, User Behavioral Analysis, Deception technology, Real-time Forensics etc. Security Analytics powered by SIEM solution is integrated across all the technologies to give a holistic view of any cybersecurity incident/event, thereby reducing false positives and achieving a pro-active threat mitigation. The technologies were chosen to obtain maximum leverage of existing technologies landscape. This ensured optimize integration of all technologies in the stack. The project was implemented with a stringent timeline of one year with agile implementation technology.

With the help of Next Generation 24x7 CSOC, overall BSE and its group company's cybersecurity posture was bolstered. BSE is now able to respond to threats with confidence at unprecedented speed and scale. It is also giving organization an advantage to defend against incidents and intrusions regardless of source, time of day or attack type. It is also helping in identifying attacks and responding before they can cause damage. Thus, safeguarding company's reputation and boosting confidence in public shareholders.

Cyber Security 2030 Predictions:

As cyber-attacks are evolving continuously, cybersecurity has a tough job keeping up. The future of cybersecurity lies with Artificial Intelligence driven anti-malware tools, and next generation firewalls that detects and learns new threats as they evolve. In terms of cyber-attacks, social engineering is a huge threat that is growing more sophisticated, as

the human factor continues to be the weak link in many cybersecurity environments. Much of cybersecurity now and in the future relies on educating and creating a culture of cyber awareness amongst individuals and teams, as this is the best path to reduce the risk of human error.

As use of IoT and connected devices is increasing at such an incredible rate, how we leave ourselves exposed to potential cyber-attacks are also increasing rapidly. Legacy systems simply do not have the capabilities to keep up with the evolving threats and relying solely on human oversight would prove largely inadequate. Capable automated systems that can monitor, detect, manage and prevent cyber-attacks in real time will be something that will drive cybersecurity as it moves forward.

REFERENCES:

1. *https://www.bseindia.com/static/about/Company_Overview.html*

Cyber Resilience for Critical Infrastructure

Mr Shankar Jadhav
Managing Director, BSE Investments Ltd, Head Strategy
BSE (Bombay Stock Exchange)

Cyber Resilience of an organization is its ability to minimize the operational impact of a cybersecurity incident, whether intentional or not, or in other words have the ability to continuously deliver the intended outcome as far as possible despite adverse cyber events and may fall back to the earlier working versions in case the current versions of the IT systems can't deliver. This cyber resilience is also a part of the organizational resilience and is a critical part since most modern critical infrastructure is run on IT systems, including the financial markets, the defence systems, the logistics and communications systems like the Net and Telecom.

Nature is inherently resilient as can be seen when living beings continue to function even when they face adversarial issues such as disease, accidents, lack of food and water, etc. The ratio of success to failure in terms of resilience is very high in nature as compared to man-made systems. It is to this resilience characteristics we see humans today evolved with so much (though very little yet) understanding of the universe and the rest of the biosphere.

Man-made systems, they say, a car today is so well designed that it is almost impossible to fail except for an accident or

some mistake. That is where cyber resilience kicks in. Can the car reduce fatalities by improving its processes – Yes – we can't drive without all doors being closed and we can't lock the door if the keys are inside the car and you try to close the door from the outside or continue to ask you to wear the seatbelts. These are programs that ensure that the car provides the functionalities it is designed for in case of some such adverse conditions. The modern car is a cyber-resilient product.

The car companies take care of such issues with their research and using Artificial Intelligence (AI) and Machine Learning (ML) with a large number of data points as they are available and being collected for many decades, through independent researches as well as from the insurance companies (buying minimal insurance is compulsory in most countries).

Normally, the critical engineering systems are made more resilient by over designing them like in the buildings and civil structures or in case of airplanes having failover mechanisms like the dual engines.

In IT systems, many went in search of failure proof systems and landed up with failure tolerant systems instead. And even these were not cost or time efficient.

The search today is for system that are almost fully automatic and reduce single points of failure (distributed), over-designed (even beyond the maximum requirements) and redundant (many have moved to n+n from n+1). Modern datacenters have n+n redundancy of all equipment and have disaster recovery sites that are online and can take over

from a failed one almost immediately. But it was difficult to come to this level of failover ability and redundancy and is possible today because of the scales at which these operate.

The cloud architecture has added a significant amount of cyber resiliency to the current systems except where lower latency is desired like in case of transactional systems or stock exchanges. Besides availability the modern system architectures are also founded on preventing data leaks and privacy & security of Data at rest and Data in motion. It is also pertinent to note that, like in nature, the systems have to be designed keeping in mind things will go wrong and organisations need to have systems in place to do root cause analysis (RCA) and to modify the systems and processes to reduce the probability of falure due to the repetition of the mistake or a similar issue.

The same can't be normally said about organisations, even critical infrastructure. One of the main issues being that the weaknesses, the mistakes, the accidents have to be informed to an outside agency and no organization likes it for various reasons. The information thus given out may be inadequate and many times watered down and hence provides much lower scope of improving the resilience of these organisations.

Since each organization tends to keep its data of failures or issues to itself and provides minimum information as required by regulation, each organization is an island of learning and only when people move from one organization to another do they bring their experience to bear on the new organization. Hence it is necessary to have people moving

from one organization to another or at least work in other organisations periodically.

Unintentional adverse events can be identified in advance or through the past experience while intentional ones can be directed by the adversaries who may normally intend to destroy, steal and change your data and to put in your systems a capability to take control of your systems and networks at the time of their liking like sleeper cells. We have to be pro-active and become hard to find or attack or hard to allow entry. One can use various frameworks like the NIST framework (Identify, Protect, Detect, Respond, and Recover).

In critical infrastructures like the Exchanges, Depositories, Brokers, etc, the regulator SEBI and RBI for Banks etc. have also come out with detailed regulation on how to be a cyber resilient organization after consultations with stakeholders. These are good starting points and generally adequate to meet the minimum standards. However, knowing that technology advances quickly and regulations may take a little time, it is better to be in the lead.

The Indian Government needs to have a dynamic cyber resilience strategy tied up to the critical infrastructure and organisations that are critical to its survival. One can even envisage a Kill switch for the connectivity/Net to prevent further damage to the systems. India also has a shortage of skilled cyber security and cyber resilience trained professionals, there is a need to develop and skill a set of people to ensure that we are ready in case of adverse events. We also need to have a special team/unit in our

defence services which can attack as well as defend in case of cyber wars. It is possible to use technology and cyber war technology to reduce the chances of humans getting hurt during border or other wars.

Indian citizens too need training and awareness of what adverse events they may face, what to do in case of cyber wars, etc.

India has about 120-150 large data centres and need a strategy to enhance their security both cyber and physical infrastructure including loss of power, connectivity, etc. With IoT coming in, there is a huge need of adopting cyber security as a fundamental working principle and ensuring cyber resilience. The Hybrid cloud and on-prem systems are likely to stay in India for a longer period of time due to various issues related to costs, availability, privacy, etc.

FEW TIPS TO BECOME A CYBER RESILIENT ORGANIZATION

1. Do your basic work well – Use checklists and online centralized systems to monitor and review routine tasks such as regular patching, permissions management, maintenance tasks, etc.
2. Cloud systems are likely to be more secure and failure tolerant, so except for low latency or other regulatory or exceptional reasons, use the cloud
3. Have your security Data-centric – use encryption, tokenization, segmentation, access management, i.e. embed security in your thoughts and ways in which you manage the processes and critical assets.
4. Applications should be designed using security as the main criterion.

5. Use software defined networking which gives you the flexibility to change over whenever there is an adverse event.
6. Use AI/ML and leverage the large companies scale to be pro-active in keeping yourself up to date in latest issues and methods to keep yourselves safe
7. Have VAPT in your veins, test, retest and make yourself fitter to minimize the risk od adverse events.

Remember cyber resilience is a continuous process and doesn't end somewhere.

Remember Resilience is not a list of checklists that one ticks off to be safe but a process through evaluations that take into account the threat environment and the risk level acceptable to the organization.

Cyber resilience is about ensuring that your organisation continues to deliver even during an adverse event with a multi-pronged approach that includes people, infrastructure, regulation, processes, and technology.

Securing Food Supply Chains from Cyber-attacks

Dr Deepa Prakash

Principal Consultant, AnnaBrahma Consultancy Services

Advisor Scientist, Kadamba

Former Scientist CSIR-CFTRI

The food and beverage industry, including the labs that are sustaining food quality and production, are as vulnerable to cybersecurity threats and cyberattacks as any other industry. The need of the hour, therefore, is to secure government, defense, and corporate, private networks, and intellectual property to protect the food supply to our armed forces and citizens.

The risk to food supply chains and institutions is not merely financial (as in some cases where institutions lost money due to a cyberattack). Agroterrorism, which involves the "intentional contamination of the food supply chains to terrorize a population and cause harm," is a growing risk. Every year nearly 3 million people die due to food-related illnesses, and over a billion tonnes of food produced globally is wasted due to spoilage.

India, with a vast population spread across diverse geographical zones catered to by various supply chains, is also at potential risk. If hackers with malicious intent gain access to our food supply chain, they could introduce

dangerous amounts of chemicals to the food being processed or treated. Programmable logic controllers, or PLCs that are used to manage and control processes in many industries such as energy plants, water treatment plants, and other critical segments, are "designed to blindly obey all commands, without paying heed to the impact they might have." What a hacker would need to do to cause a major catastrophe is to hack into these systems, and then they could cause an explosion at a chemical facility or increase ingredient dosages to a toxic level a food supply or even shut it down for a long time.

Just the ability to remotely shut down refrigeration systems for a small period can be highly detrimental to food safety. Failing to introduce a comprehensive cybersecurity program encompassing food quality and safety guidelines could potentially lead to many illnesses and even fatalities. The resultant illnesses could overload and cripple our healthcare systems for a significant duration and could lead to other socio-economic problems as well.

Groups with adversarial intent could also strike at labs preparing or processing special rations meant for specific target audiences. Thus, without firing a bullet, the enemy could theoretically cause mass causalities that could be exploited.

Cybersecurity for food infrastructure

What does cybersecurity entail? Many believe that perimeter point solutions, such as firewalls and antivirus software, are enough to secure the whole infrastructure. The identified security gaps can be linked to a lack of

security best practices at various levels. It's not unusual for a company or a warehouse or a lab to believe it is safe and secure, especially if it can't see that it's at risk.

Cybersecurity is much beyond the deployment of a point solution—it is a comprehensive plan that complies with company objectives, corporate requirements, and central and state government regulations. Once you have identified the short and long term cybersecurity needs, you can start to address cybersecurity technical requirements. This is why merely using point solutions can sometimes provide a false sense of security as they are typically deployed quickly to address an immediate need or a compliance mandate. This is where the trouble lies. A good cybersecurity strategy begins with a comprehensive risk analysis effort to determine the present state of security and what needs to be done to improve and build on it.

Food Defence Plan

To implement a Food Defence Plan as part of a Food Safety Management standard, a Threat (or Vulnerability) Assessment Critical Control Point (TACCP) is recommended (Food Safety Modernization Act Final Rule for Mitigation Strategies to Protect Food Against Intentional Adulteration).

Food Defence Plan Components

- Supply chain safety
- Step audits
- Deploying appropriate solutions
- Scaling activities to support cybersecurity
- Collaboration
- Internal security compliance mandates
- Stakeholder training and awareness

In Europe, the PAS96:2014 Guide to Protecting & Defending Food & Drink from Deliberate Attack states that "No Process can guarantee that Food & Food Supply are not the target of Criminal Activity." Cybercrime is listed as a potential threat to be addressed, and we need to list this as a threat and identify and recommend ways in which the industry and all stakeholders can be protected.

Cybersecurity implementation is a combination of many line items and tasks. It is about understanding the system, the threats, and the risks. It involves people, policies, architecture, and products.

Of course, it is the responsibility of the relevant stakeholders to ensure the design of products and solutions with security features to ensure they enable customers to comply with security standards and to provide recommendations and methodologies to guide implementation. But the end-users need to define security procedures, to mandate responsible people, and to ensure compliance with security standards.

Finally, as Industrial security is more than just IT security, a "Defense-in-Depth" approach is recommended. This approach underlines that no single item will provide security for your entire system.

In conclusion, the Food & Beverage industry is also vulnerable to cyber-attacks and cyber-threats, which increase in complexity. Therefore, cybersecurity policies should be assessed regularly using the evolving regulations and standards as part of a comprehensive Food Defence Plan.

Challenges And Opportunities In Securing India's Critical Infrastructure: Embracing A Unified Approach

Mr Vinod Kumar

Managing Director, Subex

In the last two decades, we have seen unprecedented investments in expanding India's infrastructure across sectors. Railways, highways, ports, power plants, manufacturing, communications, to name a few, have all witnessed significant enhancements in capacity. The newly augmented capacity has contributed its might to move the wheels of the Indian economy faster and in attracting more investments and rise of India as a nation to reckon with in the economic domain.

Such unprecedented growth has brought with it challenges and opportunities that are now appearing on the horizon. Securing this infrastructure and the growth story behind it has become a priority and has presented a unique challenge to all stakeholders. It has also given an opportunity – a unique one at that as well for collaboration. Our ability to secure critical infrastructure will, in many ways, be connected with our ability to grow and expand our economy and meet the aspirations of generations to come. The topic merits a more in-depth discussion, and this paper attempts to present before the reader a few points to fuel and sustain such an endeavor.

THE BACKGROUND

As per a quarterly study and analysis of threat intelligence data collected from our honeypots within the country, critical infrastructure (CI) continues to attract a significant percentage of attacks directed against the state. Rising attacks on these sectors are mostly aligned to the trends reported by other geographies monitored by us. While smart cities were the most attacked sector last quarter, this time, banking and finance got attacked the maximum number of times. In addition to traditional cyberattacks designed to listen to financial transactions, hackers are expanding their capabilities to target various aspects of banking such as cash dispensers (ATMs), PoS devices, connected kiosks, and mobile ATMs.

Back in Feb 2019, we were able to establish a clear connection between events taking place at India's frontiers, such as the Line of Control (LoC) to cyberattacks. This trend is not restricted to critical sectors alone, and we have seen a spike in cyberattacks across industries during the quarter studied. The average time to response was about 245 minutes post a geopolitical event within this window, cyberattacks (inbound and outbound) would peak. At its peak, a response came within just 19 minutes of an episode.

The rise in sophisticated inbound attacks could be easily correlated to events happening at the nation's borders. The events in our neighborhood have a direct bearing on both the volume of attacks and the quality of malware being pumped into the country. With the nation being attacked with sophisticated and defense-grade malware, the chances

of a breach remain high. The tactics deployed by hackers also keep on evolving to beat cyber defenses and any chance of these attacks being detected early.

Key trends observed and analyzed by our threat research team are summarized in table 1. This for the July-September quarter of 2019.

Trends	Explanation
Hackers are increasingly targeting connected smart home devices	Malware targeting such devices are more readily available. It is also possible that first-time hackers are targeting these devices to gain experience.
High reconnaissance activity	India continues to be in the crosshairs of state and non-state actors
Critical infrastructure continues to be a key target	Such installations are targets for sophisticated attacks launched by state-backed and experienced hackers
Attacks on Operation technology (OT) systems continue to rise	With more OT systems getting connected with IT networks, they are attracting more attacks. Hackers are targeting IT and OT systems using similar malware. As OT systems are often using older technology and security aspects are not getting adequate attention, the chances of hackers succeeding remain high.

Attacks on smart city and defense installations remain high	These two are the usual targets
Hosted botnets still active	Lack of adequate security measures, use of second-hand devices, and default passwords have all contributed to devices turning into bots. Botfarms continue to expand as newer devices get added daily.
Increased detection of military-grade malware	Some developers released a massive cache of such malware in January 2019, some of which have now ended up in the hands of hackers targeting Indian installations.

Hackers are trying hard to create an opportunity for them to exploit. With new actors and entities entering the fray daily, we do not have time on our side. We need to ramp up our defenses urgently and our cyber resilience posture to meet the challenge posed by the deteriorating cybersecurity environment in the country. The components of this posture at a foundational level can be summarized as follows:

- Higher investments in R&D around threat research around critical infrastructure
- We should work towards publishing a cyber hygiene standard for all stakeholders connected with the sector or dealing with CI in any way
- Encourage whitelisting of cybersecurity vendors to prevent supply chain contamination
- Periodic reviews, drills, and audits of standards and security guidelines to be carried out on a disaster management scale and level
- Gamify, codify and collaborate wherever possible
- Study and adopt best practices from other nations

Technology aspects of cybersecurity

Considering the immense expectations that arise from a cybersecurity perspective, it is essential to adopt a holistic approach to securing data, infrastructure, devices, perimeter, and other aspects connected with critical infrastructure. A cybersecurity platform-driven approach that addresses risks and threats related to the Internet of Things (IoT), Information Technology (IT) and Operational Technologies (OT) is therefore recommended. This will

help cybersecurity managers and teams to get a unified view of their risk exposure and threats across all points of vulnerability.

The platform should be fed by up-to-the-minute threat intelligence that is global and relevant and unify all stakeholders. It should also be able to adopt several risk mitigation and cyber resilience models while offering opportunities for risk management and also leverage artificial intelligence to evolve with each attack. Usually, there are many agencies involved in managing a critical infrastructure asset. This platform should be agile enough to enable these agencies to draw information to asses the state of the infrastructure to plan and deploy appropriate interventions if needed.

Benefits of a unified approach

An integrated cybersecurity platform will offer these benefits:

- Help agencies to respond faster in case of cyberattacks and other episodes of disruption
- Promote collaboration
- Present a unified defense perimeter to hackers, malware and other risks and threats
- Offer information to decision-makers faster
- Allow cybersecurity health checks when needed
- Help comply with the various framework and compliance mandates
- Conserve resources
- Gain a unified resource platform to secure critical infrastructure

Focus on indigenisation

India, as a nation, has been at the forefront of many technologies. India is also leading the way in the adoption of new technologies such as IoT, AI, Blockchain, among others in niche areas. Thus, it is easier to believe that we can make immense progress by focusing on developing in-house technology so that our reliance on foreign tech in critical sectors is reduced. While it may take a while for dependence on foreign vendors for hardware to overcome, in the software sector, this can happen faster. We already have a skilled workforce base, companies, and solutions in the cybersecurity sector. All that is needed is for the industry to get enough encouragement from all stakeholders so that we can put an eco-system together and move faster towards turning into a cybersecurity powerhouse.

Indigenisation will go a long way in encouraging Indian companies, and we can even look at the sector as a significant earner of foreign exchange for the nation.

The opportunity

Cybersecuring India's critical infrastructure also presents a formidable opportunity for all stakeholders. On one end, it is an opportunity to collaborate and create new avenues for growth for businesses here. On the other hand, it is also an opportunity for India to emerge as a model nation and a leader in this space. Since India is blessed with a skilled workforce and a growing entrepreneurial base, it becomes easy for us to scale up and capitalize on this opportunity. I am presenting a few aspects for the reader to ponder here. This is what we, as a nation, can become if we seize the

opportunity at hand.

- Become a leader in the critical infrastructure technology security space backed by a nurturing eco-system
- Develop a full stack play in this space so that all needs are met from within the country
- Encourage adoption of indigenous tech and support the growth of local players who are capable of helping the nation rise to the challenge
- Invest in upskilling and expanding the capacity of educational institutions to meet the growing needs of this space globally
- As a nation, we should look at the 2020s decade as India's decade of cybersecurity excellence and work towards it

With our capabilities, determination, and passion, I see plenty of reasons why we will soon emerge as a model nation in securing our critical infrastructure.

Securing India's Cyber Interests through Improved Cooperation among Businesses

Mr Ajit Mangrulkar

Director General , IMC Chamber of Commerce and Industry

(Formerly: Indian Merchants' Chamber)

Cyberspace has turned into a global shared platform for innovation, essential for business, knowledge exchange, and security. In its initial days, no one could have imagined how it would bring economies and societies together in new and complex ways making geographical boundaries irrelevant. In the broadest possible sense, cyber governance deals with evolving an understanding of how this space could be governed. It includes a framework for inter-stakeholder relations that provides the highest degree of predictability in interactions in security, trade, or politics conducted in the cyberworld or using it as a conduit — governance of the internet and cyberspace a new and essential aspect.

As countries get closer, and the perception of transnational risk increases, the need to govern this in a manner that maximizes benefits for all stakeholders while minimizing risk increases. In this context, cybersecurity also begins to connote the ability of countries to defend their national sovereignty and advance their national interests individually and cooperatively.

The initial approach to managing stakeholders' interests on the web was ad hoc, voluntary, and based primarily on business and technology ideas and concepts. The concept of non-state actors from companies and civil society working as equal partners with governments that are organized into a multi-stakeholder community such as industry bodies was adopted much later when it became clear that business interests also needed protection in cyberspace.

A global and regional collaborative approach was the right way to build a robust network of likeminded business stakeholders rapidly, but now that it is built, it needs reconsideration. This is because newer and more impactful paradigms have appeared on the horizon, and businesses are turning into vulnerable targets thanks to individuals and state-backed actors targeting them for various reasons online.

With businesses getting bogged down by financial and commercial considerations, trade associations and industry bodies provide ample grounds for collaboration and furthering various industry objectives. Such collaborative efforts as those initiated and sustained by industry bodies help frame regulations, improve the business environment, and help governments adopt the right stance at international forums. In emerging and essential fields like cybersecurity, this becomes a necessity rather than an option.

GETTING THE PRIORITIES RIGHT

Usually, collaboration at an industry body level is bogged down by these aspects:

Industry bodies evading issues of national interest

- Key industry players using the forum to further their business interests
- Lack of cohesion among members leading to a lack of consensus
- Focus on policies that have an impact on short-term business objectives
- Lack of an agreement on a shared charter of activities
- Lack of road map for promoting collaboration among businesses situated at the extreme ends of the spectrum

In the past, we have seen how some industry associations have been putting pressure on the government in areas such as foreign exchange rates, doing business with blacklisted foreign entities, trade deals and negotiations, and legislations. Instead of looking at the relationship with the government only through the watch glass of what's in it for them, industry bodies and members should adopt a holistic stance that moves faster in the direction of national and citizen interest.

Thus, members of such groupings should work towards collaboration to further our national interests as that is what will sustain the national economy and provide a better operating environment for Indian companies in the future. A long term view keeping our national interests in mind will go a long way in sustaining the operational future of our companies and thus provide the government added strength to presented a united and stronger front while negotiating trade deals and agreements either bilaterally or as a group.

The collaboration mantra for members of trade bodies

- Keep national interests above regional\businesses\ personal interests
- Collaborate and discuss matters openly at every possible instance
- Give sufficient voice and attention to smaller companies and startups
- Lead by example, follow by choice and support the government in cases of national and citizen interest
- Provide expertise and consulting help to the central and state governments wherever needed

Our broad objectives for collaboration in the field of cybersecurity among members should center around

- Harnessing the full range of proven and established professional expertise in India;
- Providing an inclusive and collaborative forum for benchmarking and shared standards for cybersecurity professional excellence;
- Enabling the development of the specialist skills and capabilities that will allow the country to keep pace with rapidly evolving cyber risks;
- Enabling a self-sustaining pipeline of talent providing the expertise to meet our national needs;
- Providing a focal point that can advise, shape, and inform national policy.

Securing Citizens Online: Navigating The Dynamic And Evolving Landscape

Ms. Sumitra Goenka

Director - Ratein Infotech India Private Ltd

CEO - TriangleGlobal

When a young nation moves forward, it moves rapidly, embracing and setting new trends. India is an example of a nation that is young at heart and mind. A dynamic nation that is at ease being part of one of the largest knowledge-driven societies out there.

India is a success story no matter how you look at it. Yes, there is still a lot to be done. But if we just look at the amount of progress we have done in alleviating poverty in the last 3 decades and in digitally enabling a large segment of our population in the last decade, we realize how far we have come since independence. This progress has to be preserved, sustained and built upon if we are to grow as a nation and occupy our rightful place in the league of nations.

The invisible enemies who are constantly striving to destabilize our nation, lower our standing and national credibility and harm our growth prospects are acting in a multitude of ways. First, they hire social media armies to pollute social media conversations, then they try and influence active social media users into believing in and

promoting a counter-narrative and finally they recruit digital denizens to continue the process of promoting communal discord from within.

THE INCREASING DIGITAL FOOTPRINT AND ITS IMPLICATIONS

The rate at which we are expanding our digital presence has major implications. The posts we share on social media are becoming increasingly personal. The data we are sharing is not just being harvested by commercial entities but is also available to anti-social elements. While social media does afford a level of anonymity, it is being misused by elements to spread fear, baseless anti-government propaganda and other dubious objectives. Regular and non-commercial users of social media are however not using this anonymity to protect themselves.

At one end social media is a distraction for the youth and the other it is could also become an avenue for stalkers and anti-social elements to harass and vilify. By spending a lot of time on social media, our youth are denying themselves an opportunity to read, learn and have a deeper interaction with society. It is also exposing them to wrong ideas and perspectives which are commonly encountered on various websites and social apps with ease.

In a crowded space with lots of noise being generated, good sources of information and knowledge often get drowned or buried. This robs our youth of avenues of intellectual stimulation while diluting their ability to rationalize.

SECURING CITIZENS IN THE DIGITAL SPACE

With the ever-present incentive for instant gratification, it is difficult and not-advisable to wean citizens away

from social media and other digital mediums. Instead, it is advisable to increase awareness, collaborate with them and increase the availability of sources of authentic and engaging information. The scope of digital literacy needs to be expanded to include a sense of understanding of risks associated with the content being shared online. So one should only be called digitally literate if one is able to discriminate between the good and the bad.

A lot has been done to empower law enforcement agencies (LEAs) to help citizens. But we have barely scratched the surface. LEAs need more help in terms of technology, pattern recognition, and data analysis to turn into a pro-active protector of citizens online.

There should be a regulatory body set up to certify smart home and security devices such as security cameras. Products should only be sold after such a certification is given. Sale of cheap and unsecured personal or asset security products should be banned as they represent a persistent threat not just to the individual but to businesses and the government as well.

The scope of cybersecurity education should be made more comprehensive and dynamic to raise awareness among children and influenceable minds. The current curriculum is inadequate in this respect.

These are but a few steps that can be taken immediately and represent a good start. The government and other stakeholders should also look at two-year plans for citizen security that is revisited every six-months. By securing citizens and digital denizens of tomorrow, we are not just securing their future but also that of the future of the nation as a whole.

Cyber Security, Data & Intelligence Gathering

Ms. Uma Sudhindra

Member- Board of Governors, Indian Insititute of Management - Vizag

Data is not just considered as the oil of today & tomorrow, but, has become the single most important factor in driving & powering economies & industries. Every small piece of information is data, from blue prints to intellectual property and the biggest question facing every intelligence agency/organisation today is how to secure & protect that data constantly?

Till 2005, cyber threats weren't even mention in the intelligence communities. For the last seven years, it has been identified as the number one threat, starting from FBI, CIA, ASIS, CSIS, Mossad, R&AW, SVR and JIO.

Digitisation of The World

With increased digitisation&centralisation of citizen data, we have enabled a plethora of services to be delivered in a transparent manner to a range of beneficiaries. However, if this data is not secured and protected, it is an easy target for various groups of hackers sitting anywhere in the world. They can be state backed hackers who will be encouraged &incentivised and ordered to attack vital spots with completely nefarious objectives.

The world has spent more than $600 billion in 2017 in

damages alone. Damages to protect ourselves from cyber - attacks. Imagine the number of developmental programs that could have benefitted from half this money. We could have overcome a few critical global challenges.

Espionage and The Cyber World

Cyber means are used to fuel misinformation & disinformation, leading to confused intel gathering by various agencies. There are cases of agencies gathering the same intel but pursuing it from different perspectives & therefore, creating either irrelevant or wasted outcomes. Cyber threats come from a wide array of actors, not all of them are cyber criminals or hackers. Some of them are nation states who are adversaries and want either political, economic or military advantages. The use of cyber tools as a means of achieving geo-political one-upmanship is becoming increasingly sophisticated and a supremely effective one.

Cyber forensics deals with wide ranging cyber threats in real time conditions. We are looking at real time monitoring at basic and complex levels. Our intelligence agencies must develop capabilities to counter mis & disinformation and pull out actionable insights from the noise in the virtual world. The process of detection, analysis & mounting defence against such real time attacks, is impossible if threat intelligence, big data and machine learning techniques are not employed.

We must remember with 24/7 surveillance, there is humungous amount of data that gets collected or generated by intel agencies. Big data analytical techniques are

imperative here to mine, extract & interpret to create a structured piece of intel from unstructured data.

Cyber Platform for Intel Gathering

Can Indian intel agencies and cyber security agencies/ departments of various ministries come together on one cyber platform that can address the numerous issues like phishing attacks, data leakages, socially targeted attacks?

To carve out actionable data from all the virtual noise requires enrichment of the data for further analysis. This enriched data will go through event & context extraction, sentimental & prominence analysis. The mined data through a dashboard should show the relevant maps, event graphs, charts and flags. This intel can then made actionable by using communications & collaboration, signals intelligence and resource handling. This platform can be based on open source technology stack and use contextual mining to pick & analyse only relevant data. The platform should also be able to mitigate risks real time with minimal damages caused.

Involvement of Tech Companies

Today, domestic disinformation is one of the biggest challenges in any country. We are witnessing it in our own capital and across the country in most cities & towns. Slow moving government policies and attempts to regulate speech & communication activities through content moderation, will compel tech companies to step in to manage like a semi-government body. The public-private partnership can work wonders if rules of engagement are clearly defined to build in transparency and legitimacy.

Future Frontiers

Countries should well look beyond the simple disinformation campaigns run on social media platforms and focus on all democratic institutions and how they are impacted by such campaigns. It is interesting to see how organisations like Russia's Internet Research Agency (IRA) through consistent outreach on Messenger focused on American infiltration movements. Intel professionals globally are being trained to be part cyber armies to target common citizens, develop trust and get them to act. In the future, this kind of real time engagement will be a big part of any cyber operation.

Finally, the media is also a contributor in its own way. Despite claims of being neutral observers and the ones to bring "breaking news" to our living rooms, the media is also exploited by bad actors and in turn feed off whatever information they get. This only serves to increase the already existing polarisation& divide. Journalists & media channels must be encouraged to be strategic about their reporting, expose false narratives and their origins and build trust & resilience in their audience. That way the breaking news & bumper ticker syndrome should decline and real news reporting make a grand comeback.

Data Sovereignty In Cyber Space With Cyber Crime And Cyber Laws: An Insight For Next Generation

Dr. Pradeep Tomar,
Assistant Professor Department of Computer Science and Engineering,
School of Information and Communication Technology,
Gautam Buddha University, Greater Noida, U.P., INDIA

Prof. Sanjay Kumar Sharma,
Dean, School of Information and Communication Technology,
Gautam Buddha University, Greater Noida, U.P., INDIA

Dr. Sandhya Tarar,
Assistant Professor, Department of Computer Science and Engineering,
School of Information and Communication Technology,
Gautam Buddha University, Greater Noida, U.P., INDIA

Abstract

This chapter addresses the role and improvement of the cyber laws in India for cyber crime. A Cyber space is a virtual space that has become as significant as genuine

space for business, instruction and governmental issues etc. The developing risk from cyber crime submitted against computers, or against data on computers, is going to start for consideration in the India. In many nations, existing laws are probably going to be unenforceable against such crime. Cyber laws, as it stand today, offers ascend to both positive and negative results. The principle negative outcomes is the advanced technology so ambiguous that many allude to it as the dim sides of innovation and that cyber criminal presently have high ground. The appropriateness and viability of our current laws should be always surveyed to confront the hazard originating from the cyber world. In this chapter we are going to firstly describe the data sovereignty with following three elements of data confidentiality, data integrity, data availability, cyber laws, cross border jurisdictions with cyber crimes, cyber crime laws of country with technological challenges. Our fundamental point throughout this chapter is to presents challenges cyber laws and cyber crime which keeps on developing as one of the most powerful dangers to the cyber clients of the cyber society in India.

INTRODUCTION

In the present time of Information Technology, the computer has picked up prevalence in each part of our lives. This incorporates the utilization of Computers by people engaged with the commission of crimes. Today, Computers assume a significant job in pretty much every crime that is submitted. Each crime that is carried out isn't really a Computers crime, yet it means that law requirement must turn out to be substantially more computer proficient just

to have the option to stay aware of the criminal component. Broadening the standard of law into the internet is a basic advance to make a dependable situation for individuals and various exercises. Since that augmentation stays a work in progress, associations today should above all else safeguard their own frameworks and data from assault, be it from pariahs or from inside. They may depend just optionally on the discouragement that successful law requirement can give. To give this self-insurance, associations should concentrate on executing cyber security plans tending to individuals, procedure, and innovation issues. Associations need to submit the assets to instruct workers on security rehearses, create intensive designs for the treatment of touchy information, records and exchanges, and join vigorous security innovation, for example, firewalls, hostile to infection programming, interruption discovery devices, and confirmation administrations, all through the associations' Computer frameworks. One of the significant difficulties confronting law improvement in this new period is staying aware of developing requests of innovation. Computer innovation changes are quick to such an extent that if a division is cutting-edge today; their gear will presumably be obsolete. Organizations are woefully behind in their procurement and use innovation. Their financial limits have not been expanded to keep pace with the quick change in innovation. This make its hard for law authorization offices to stay aware of this quick change. The criminal component isn't as tested to keep pace. They are normally all around financed and have the assets to keep buying this new innovation [1].

A few late endeavors have been proposed by different nations, for example, Brazil, Germany, China, and Russia to all the more likely direct their information sway necessities against the mastery of the US correspondences framework and administrations. [2] [3] [4] [5] [6] [7] [8]. These specialized recommendations are national email, confined steering of Internet traffic, undersea fiber optic link and restricted server farm. Be that as it may, Maurer et al. in [9] evaluated that those proposition are probably not going to ensure against the worldwide correspondences reconnaissance by outside knowledge administrations. They brought up that encryption instruments are possible answers for verifying touchy information against remote reconnaissance.

DATA SOVEREIGNTY

Data sovereignty is the concept that information which has been converted and stored in binary cyber form is subject to the laws of the country in which it is located. Data sovereignty comes into play when an organisation's data is stored outside of their country and is subject to the laws of the country in which the data resides. As per stratokey.com the advent of SaaS, cloud and hosted services data sovereignty issues have become more prevalent. With the distributed architecture of the cloud, where application data resides may not be known to the end user. Cloud and SaaS providers may host data in technically efficient locations or locations that make the most commercial sense. Unfortunately, this location may well not be in the country of residence of the user. The distributed nature of the infrastructure driving these services means that the data

hosted may fall under the laws of a foreign government. As per kempitlaw.com a breach of data sovereignty can happen on-premise and in-cloud for example in case of on-premise a server or a personal device owned or used by the cloud customer; in case of in-cloud a server owned by the cloud service provider or during transmission between servers or between a cloud server and a customer device. Data sovereignty affects four main types of actor:

- Government organizations are concerned essentially with the extent of their forces to get to information, the approvals required to practice those forces, and the office's responsibility for their utilization;
- Cloud service providers (Cloud SPs) have worries about: holding client trust and their own notoriety in the market (reputational concerns); and contract terms, arrangements, administration and consistence with lawful necessities (operational concerns);
- Corporate cloud service customers (CSCs) share Cloud SPs' reputational concerns however are for the most part front-side to them in legally binding and arrangement terms; and
- Individual cloud clients are for the most part worried about information security and unapproved access to their data.

Government agencies, Cloud service providers (Cloud SPs), Corporate cloud service customers (CSCs), and Individual cloud customers have following questions in their mind as per stratokey.com

- Finding out where information is put away isn't

constantly evident for the present age of cloud and SaaS facilitated administrations.

- With appropriated registering, for example, the cloud, information facilitated by SaaS applications can arrive in peculiar and awesome spots. While this may well minimize the expenses, and make get to quick, it leaves client's information powerless against remote governments and their related laws.
- When you move your information off the facilitated administration, is there a protected obliteration arrangement and security control?
- Data that was secured by solid protection laws, may well not be ensured in a remote purview. This can make legitimate difficulties to information get to un-defendable.
- When managing outsiders, it tends to be hard to really know the security of the information and administrations they control.

Based on the above questions following element of data sovereignty requirements are data confidentiality, data integrity, and data availability [10] and these elements helps in protecting data against cyber crimes.

Data Confidentiality

This necessity intends to shield national touchy information from being uncovered. Open organizations must have the vital prerequisites as far as characterized data that should be profoundly ensured by the Public Information Disclosure Act No. 14/2008 and the National Intelligence Act No. 17/2011. To guarantee information privacy, the most

direct technique is to encode all the delicate information for capacity, handling, and transmission. An option is to just store unclassified information in the internet, for example, clouds.

Data Integrity

This prerequisite expects to shield information from malignant alteration. The utilization of Encryption is additionally broadly used to all the more likely secure information during capacity, preparing and transmission. For examination, it is likewise important to ensure that all review information are true and considered allowable in court. Information put away in server farms might be dependent upon adjustment by insider dangers. Along these lines, the NCS necessity would apply inside this security administration.

Data Availability

This necessity guarantees that information put away in the Internet are accessible on every client recovery demand. This prerequisite is especially vital for information very still in physical servers that give a Service Level Agreement (SLA). Specialist co-ops ought to give an assurance that clients' information put away in the server farm can be promptly accessible at whatever point required. Specifically, it is imperative to guarantee the accessibility of information if there should arise an occurrence of lasting help blackout and power majeure, for example, war and crime

DATA SOVEREIGNTY IN ACTION

As per cio.com an ideal case of a client seeking after a half breed cloud procedure to handle information

power difficulties is the Company. Having offered cloud arrangements since 2007, administrative prerequisites kept the Dutch cloud supplier from setting explicit information in the cloud. This implied they couldn't get to one of their most significant applications. Also, in light of the fact that this application shared a customer's legitimate data, it should have been kept on premises. So as to tackle this issue, The Company required a half and half cloud arrangement that could incorporate with Microsoft Azure open cloud, a stage they were at that point utilizing. A hybrid cloud condition offered The Company the adaptability and versatility of an open cloud, with the security of a private cloud. While inquiring about various choices, The Company found out about Microsoft Azure Stack, an on-premises private cloud. Microsoft Azure Stack empowered The Company to have a subset of Azure administrations inside their own private server farm. Given that Microsoft Azure Stack and Microsoft Azure have reliable engineer devices, the API enabled them to construct their applications once, and afterward convey to open or private mists relying upon the information guidelines. The Company had the option to convey any applications with information power confinements on premises, while as yet using the Microsoft Azure open cloud for their different applications.

The Company picked Hewlett Packard Enterprise (HPE) for their Microsoft Azure Stack half breed cloud arrangement dependent on the expansive assortment of setup alternatives they offered just as their administrations portfolio through HPE Pointnext Services.

According to Ronald Verweij, CEO and founder of The

Sourcing Company, "HPE ProLiant for Microsoft Azure Stack allowed us to develop a single flexible solution…our legal clients access Office 365 in the public cloud while complying with security regulations by maintaining privacy sensitive applications and data in a private cloud."

DATA SOVEREIGNTY AND CYBER CRIME

As per rgtechnologies.com.au data sovereignty can be a complex legitimate issue that can influence associations around the world. In situation one, we have an Australian cloud administrations supplier that has their primary office, including deals, promoting, bookkeeping, and tasks in Australia. Be that as it may, their client assistance call focus is situated in India. Certain individual data about records must be sent to India with the end goal for them to contact customers and offer help. As indicated by Australian Privacy Principles (APP), the cloud supplier must unveil what data is being sent outside of Australia. In situation two, we have a cloud specialist co-op situated in the United States with a branch office in Australia. Their charging capacities are taken care of in their fundamental office seaward. In this manner, a lot of individual data must be sent to the United States and is dependent upon their laws. There is the potential for an association's close to home information to be subpoenaed by a remote government.

Cyber crime could sensibly incorporate a wide assortment of criminal offenses and exercises. The extent of this definition gets more extensive with a continuous partner or substitute term "computer related crime". Model exercises that are considered cyber crime can be found in

the assembled country manual on the avoidance and control of computer related crime. The Oxford Reference Online characterizes cyber crime as crime submitted over the web [1]. The Encyclopedia Britannica characterizes Cyber crime as any crime that is submitted by methods for uncommon information or master utilization of computer innovation.

Cyber crime are hurtful acts perpetrated from or against a computer or system, vary from most earthly crimes in four different ways.

- They are anything but difficult to figure out how to submit.
- They require hardly any assets comparative with the potential harm caused.
- They can be submitted in a locale without being physically present in it.
- They are regularly not obviously illicit.

An expansive definition would be any crime submitted that includes the utilization of a computer. In current occasions, this would mean pretty much every crime submitted. Should a criminal utilize a computer to monitor the thefts he's carried out or the medication he's sold, which implies that even stick-ups, breaking and entering and each medication exchange could be viewed as a computer crime [3].

CYBER LAWS & THEIR ROLES IN DATA SOVEREIGNTY

The Cyber Laws in the Indian context came into focus with the Information Technology Bill – 1999, which has

since been passed as Information Technology Act 2000. This was the first comprehensive codification of Laws in Indian directly enacted for the regulation of cyber world [11]. As per mcconnellinternational.com the laws of most countries do not clearly prohibit cyber crimes. Existing terrestrial laws against physical acts of trespass or breaking and entering often do not cover their "virtual" counterparts. Web pages such as the e-commerce sites recently hit by widespread, distributed denial of service attacks may not be covered by outdated laws as protected when it attempted to prosecute the perpetrator of the May 2000 Love Bug virus, which caused billion of dollars of damage in worldwide.

- Cyber Laws have an important role in representing and defining the norms of the cyber society.
- Cyber Laws help in giving the right to enter into legally enforceable cyber contracts.
- Cyber Laws help in maintaining the Cyber properties.
- Cyber Laws help in to carry on the online business.
- Cyber Laws help in providing legal reorganization for Electronic documents and
- Cyber Signature.

CROSS-BORDER JURISDICTION AND CYBER CRIME

As per cio.com data sovereignty, the idea that information is dependent upon a nation's laws when it is put away inside specific fringes, is getting to a greater degree a test for organizations as they move to the cloud. In Europe, "associations can be fined up to 4% of yearly

worldwide turnover"1 on the off chance that they break the Data sovereignty guidelines known as the General Data Protection Regulation (GDPR). The GDPR, a law that ensures the EU's resident's security and data, applies to not just the nations in the European Union (EU), yet to organizations that have information from associations or individuals dwelling in the EU. These guidelines can force some significant confinements for associations that direct universal business and are executing a cloud-first approach.

To be arraigned over a fringe, a demonstration must be a crime in every locale. Accordingly, while neighborhood legitimate customs must be regarded, countries must characterize cyber violations along these lines. As per web. archive.org powerful law authorization is entangled by the transnational idea of the internet. Component of participation crosswise over national outskirts to unravel and indict is mind boggling and moderate. Cyber lawbreakers can resist the regular jurisdictional domains of sovereign countries, beginning an assault from practically any computer on the planet, passing it over numerous national limits, or planning attack that give off an impression of being starting from remote sources. Such procedures drastically increment both the specialized and legitimate complexities of researching and arraigning cyber crimes. As per cybersecurity.my the jurisdiction issue in a computer intervened correspondence is anything but difficult to decide, especially if the injured individual is situated in another district. In this manner, at whatever point a crime is carried out by means of the internet, the court will confront an issue in choosing which nation's Jurisdiction does the perpetrated crime fall under.

Through courts and officials have always reverberated that there is a worldwide upheaval approaching not too far off, the advancement of the law in managing cross-fringe locale is still in its early stages. The 'newborn child' law must be additionally supported and created to turn into a full-edge set of cyber laws the clarity characterizes a nation's locale at whatever point a cyber crime is submitted. That law ought to for instance address whether a specific occasion in the internet is represented by the laws of the state or nation where the offense is submitted or by the laws of the state or nation where the objective is found [12]. Self-insurance, while basic, isn't adequate to make the internet a protected spot to direct business. The standard of law should likewise be authorized. Nations where lawful assurances are deficient will turn out to be progressively less ready to contend in the new economy. As cyber crime progressively breaks national outskirts, countries saw as shelters risk having their electronic back rubs obstructed by the system. National governments ought to analyze their present status to decide if they are adequate to battle the sorts of violations talked about in this report. Where holes exist, governments should draw on best practices from different nations and work intimately with industry to sanction enforceable legitimate assurances against these new violations. This dissects the condition of the law in various nations. It finds that solitary ten of these countries have revised their laws to cover the greater part of the sorts of crimes that should be tended to. While huge numbers of the others have activity in progress, plainly a lot of extra work is required before assaulting esteemed frameworks

and data.

In view of its finding in the E-Reading study, and in the wake of the Philippines powerlessness to arraign the understudy answerable for the "I LOVE YOU" infection, McConnell International studied its worldwide system of data innovation arrangement authorities to decide the condition of cyber security laws around the globe. Nations were approached to give laws that would be utilized to indict criminal acts including both private and open division computers. Nations that gave enactment were assessed to decide if their criminal rules had been reached out into the internet to cover ten distinct sorts of cyber crime in following classifications:

- Data-related crimes, including interception, modification, and theft.
- Network-related crimes, including interference and sabotage.
- Crimes of access, including hacking and virus distribution.
- Associated computer-related crimes, including aiding and abetting cyber criminals,
- Computer fraud, and computer forgery.

TECHNOLOGY CHALLENGES IN CYBER SPACE

In the present period of information technology, the innovation in India turns out to be further developed, law authorization organizations must furnish their computer crime specialists with the innovation required to direct

complex computer examinations. Other than access to innovation, law implementation organizations should likewise be given scientific computer support the same number of computer crime leave "impressions" on the computer just as on the Internet [5] Most examiners additionally do not have the preparation and specialization to concentrate on the arraignment of lawbreakers who use computer based and Internet framework as a methods for carrying out violations. In this manner, they should have working information on computer based and Internet examinations on the off chance that they are to deal with these crimers adequately.

A genuine model is an ongoing case in UK where a young person was absolved in the wake of being charged in court for Distribution Denial of Service (DDOS) assault that disabled the Port of Houston, a US online computer framework. Denial of Service (DoS) attack and all the more especially the conveyed ones (DDoS) are one of the most recent and most dominant dangers that have showed up in the realm of systems administration. The wildly publicized DDoS attacks against Yahoo, eBay, Amazon.com and the White House sites have uncovered the helplessness of well-prepared systems. A DDoS assault, which indicates to deny an injured individual (host, switch or whole system), is regularly similar to a DoS assault with the exception of that it includes various co-facilitated hosts to do the assault. There are two chief classes of assaults: Logic attack and Flooding attack [13].

As per kempitlaw.com challenges on data sovereignty have made headlines since mid-2013 when Edward

Snowden published his allegations about the bulk information collection programmes of US and UK security services. In the years that followed there have been several developments at both legislative and judicial level that have brought the issue of data sovereignty into sharp focus. They include the following:

- The action brought by Austrian student Max Schrems before the Irish High Court in which he challenged the Irish Data Protection Commissioner's decision that it was not required to investigate complaints that the transfer of personal data by Facebook Ireland to it US parent company Facebook Inc. violated EU data protection law
- Microsoft's ongoing litigation over the warrant to obtain information for US proceedings from its Dublin data centre, In Re Warrant.
- The UK High Court's decision effectively striking down s1 DRIPA on 17 July 2015 and
- The three UK 2015 reviews into electronic surveillance of communications content and other data and the publication of the UK Investigatory Powers Bill in November 2015.

All these stories share several common data sovereignty characteristics:

- The privileges of citizen to privacy and protection of their own data;
- The forces of the state to get, gather and utilize electronic correspondences data produced by their citizens without their understanding or information;

- The suitable balance between these citizens' privileges and state's forces; and
- In the universal setting, how these rights and powers play out on the off chance that one state gathers or acquires data not about its own, however about another state's, citizens.

IMPROVED CYBER LAWS REQUIRED

As per cji.edu following improved cyber laws are required in the following:

The Internet

The web is happiness for individuals from the law authorization network. On one hand, it encourages our capacity to convey and assemble data. Then again, it empowers the criminal component to do likewise. The criminal component really grasped the advantages of the Internet some time before those of us in the law authorization network did. Somehow or another, despite everything we oppose this device. These framework assurance devices, the product and equipment for protecting data frameworks, are unpredictable and costly to work. To stay away from problems and cost, framework producers and framework administrators routinely leave security highlights " turned off," unnecessarily expanding the weakness of the data on the frameworks. Bugs and security openings with known fixes are routinely left uncorrected.

Data Theft

Law enforcement is accused of the examination of the burglary of information from organizations, however of similarly as incredible a worry to the law requirement

network is the assurance of their own information and unapproved access to their records. This may require law implementation offices to get a security specialist to be certain that their very own information is secure from unapproved get to. The best way to guarantee that your framework is absolutely protected is to not have outside access to it. On the off chance that you approach, you will have a security hazard. In the event that you are associated with the Internet through telephone lines through a system or a modem, you can't expect that your framework won't be undermined sooner or later. Organizations can introduce genuinely basic checking frameworks on their frameworks that will flag them when there has been a "thump" at the entryway. These safety efforts will likewise aware you of a real interruption.

Child Pornography

Child pornography entertainment appropriation is a characteristic for the Internet. It offers namelessness and simplicity of moving pictures and content. The utilization of the "Net" considers the enrollment, provocation and maltreatment of minors by grown-ups and is encouraged by the "I can be anybody" nature of the Internet. The Internet helps the trade and sharing of youngster sex entertainment. The best way to not discover youngster erotic entertainment on the Internet isn't to search for it. Child Pornographers exchange pictures of exceptionally small kids, contingent upon their inclinations, to different pornographers that will exchange them to other people or essentially keep them for their own assortment.

White Collar Crime

Britannica.com characterizes White Collar Crime as violations carried out by people of moderately high social or monetary status regarding their customary occupation. In spite of the fact that crimes, for example, stalking and pedophilia stand out as truly newsworthy, most of PC crime is office in nature, including the robbery of charge cards, cash, character, or protected innovation, for example, programming or information.

To avoid the cyber crime some improvement are suggested here to protect the nation.

- Organization should secure their networked information by using latest technology.Laws to enforce property rights work only when property owners take reasonable steps to protect their property in first place.
- Governments should assure that their laws apply to cyber crimes.Governments remain the dominant authority for regulating criminal behavior in most places in the world. One nation already has struggled from, and ultimately improved, its legal authority after a confrontation with the unique challenges presented by cyber crime [4]. It is crucial that other nations profit from this lesson, and examine their current laws to discern whether they are composed in a technologically neutral manner that would not exclude the prosecution of cyber criminals.
- Firms, governments, and civil society and cyber society should work cooperatively to strengthen legal

frameworks for cyber security.A model approach is underway in the Council of Europe comprising 41 countries [13]. The Council is crafting an international Convention on Cyber Crime. The Convention addresses illegal access, illegal interception, data interference, system interference, computer-related forgery, computer-related fraud, and the aiding and abetting of these crimes.

ACKNOWLEDGMENT

The authors would like to thanks to our Hon'ble Vice-Chancellor, Prof. Bhagwati Prakash Sharma for providing us the opportunities to participate in the Round Table on Cyber Security and to provide support for this study. Many thanks from our side to all members of Center for Knowledge Sovereignty.

CONCLUSIONS

Our primary aim of this chapter introduction is the improvement of devoted Cyber Crime Cell and successful Cyber Laws for information chiefly. Data sovereignty can't ensure information security from data breaches, data loss and privacy intrusions. An open organization should utilize security best practice for a verification system, for example, two-factor authentication and data leak prevention to help ensure a higher level of confirmation, non-revocation, and access control. In spite of the advancement being made in numerous nations, most nations still depend on standard earthbound law to arraign cyber crimes. Most of nations are depending on old resolutions that originate before the introduction of the internet and have not yet been tried

in court. The general shortcoming of rules expands the significance of private segment endeavors to create and receive solid and productive specialized arrangements and the executives rehearses for data security. A model methodology is required. Most nations, especially those in the creating scene, are looking for a model to pursue. These nations perceive the significance of prohibiting pernicious computer related acts in an auspicious way so as to advance a safe domain for online business. In any case, few have the lawful and specialized assets important to address the complexities of adjusting earthbound criminal rules to the internet. An organized, open private association to deliver a model methodology can help take out the potential risk from the incidental formation of cyber crime sanctuaries. Hybrid cloud solutions are explaining information power difficulties all around the globe. Luckily, adopting a half breed cloud strategy can unravel a large number of the difficulties presented by information power. Associations with their very own private on-premises situations beat these difficulties without losing the advantages an open cloud gives. Crossover cloud enables organizations to pick what information they need to convey to the off-premises cloud and what information they have to keep on premises.

REFERENCES

[1] Paul A. Curtis, Dr. Lee Cowell," Cyber Crime: The Next Challenege" in seminar at School of Law Enforcement Supervision, 2000.

[2] Zygmunt Bauman, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon, and RBJ Walker. After snowden: Rethinking the impact of surveillance. International Political Sociology, 8(2):121–144, 2014.

[3] Biswajit Biswal, Sachin Shetty, and Tamara Rogers.

Classification based ip geolocation approach to locate data in the cloud datacenters. 2014.

[4] Robin Emmott. Brazil, europe plan undersea cable to skirt u.s. spying. www.reuters.com/article/2014/02/24/us-eu-brazil-idUSBREA1N0PL20140224.

[5] Dong Lai Fu, Xin Guang Peng, and Yu Li Yang. Trusted validation for geolocation of cloud data. The Computer Journal, page144, 2014.

[6] BambaGueye, Artur Ziviani, Mark Crovella, and Serge Fdida. Constraint-based geolocation of internet hosts. Networking, IEEE/ ACM Transactions on, 14(6):1219–1232, 2006.

[7] Jonah Force Hill. The growth of data localization post-snowden: Analysis and recommendations for us policymakers and business leaders. In The Hague Institute for Global Justice, Conference on the Future of Cyber Governance, 2014.

[8] Dana Polatin-Reuben and Joss Wright. An internet with brics characteristics: Data sovereignty and the balkanisation of the internet. In 4th USENIX Workshop on Free and Open Communications on the Internet (FOCI 14). USENIX Association, 2014.

[9] Tim M., R. Morgus, I. Skierka, and M. Hohmann. Technological sovereignty: Missing the point www.newamerica.org/ TechnologicalSovereigntyReport.pdf, 2014.

[10] Yudhistira N., Kautsarina and A. S. Sastrosubroto, "Towards Data Sovereignty in Cyberspace, www.cs.ox.ac.uk/ TowardDataSovereignityCyberspaceNugraha.pdf

[11] Na. Vijayahankar, "The role of Cyber Laws in E-Governance" 2000.

[12] Is Cyber Crime reigning on a no Man's land" by National ICT Security and Emergency Response Centre (NISER).

[13] Tomar, P. and Singh, R.Defense & Solution against Denial of Services Attacks: A Challenges" in proceeding of Second National Conference on Advanced Images Processing and Networking organized by Deptt. of Computer Sci.andEngg. & IT at National Engg. College, Kovilpatti, Tamilnadu , page 201, 2005.

Empowering Agencies with Comprehensive Data Gathering Technology Platform

Dr Faruk Kazi

Dean- Research, Development and Consultancy at Veermata Jijabai Technological Institute, Core Advisory Committee Directorate of Technical Education, Maharashtra State

Ms Ashwini Dalvi

VJTI, Mumbai

Data plays important role in detection, mitigation and investigation of crimes in cyber and cyber-physical space. Traditionally, Law Enforcement Agencies (LEAs) used to rely on data gathered in person and human intelligence. Post-event analysis was usually handled by digital forensic tools. With the penetration of Information & Communication Technologies (ICT) in all day to day activities and dependence of humans on the interconnected cyber-space, it is obvious that a criminal leaves behind traces and foot-prints in the cyber space which will be of immense importance to LEAs. However, this data is scattered in various domains of cyber-space and in different social media platforms. A comprehensive data gathering platform which crawls data across different platforms, provides meaningful linkages to the gathered data to arrive at actionable intelligence is needed to empower LEAs. This will help LEAs to address growing financial frauds, terrorist activities, drug and human trafficking and crimes against women & children.

The vast majority of data is available through Internet. The internet can be viewed in three layers, namely Surface web, Deep web and Dark web. The generic internet search is through surface web. But it makes up to only 4%-5% of the whole internet. The pages on surface web are indexed and search by search engines. In response to query user gives, the search engine shows results. These results are nothing but data gathered for given query. By referring to surface web search by popular search engines such as Google, Yahoo, Bing, one can comprehend how vast pool of data is. But data is enormous in nature beyond surface web. The surface web is preceded by deep web. The deep web is boundless collection of unindexed web pages. These pages are not reachable by surface web search engines. From data perspective deep website or deep pages are immeasurable source of information. A part of deep web is engaged and used in illegal activities is called as Dark web. This part of dark web is highly isolated even from deep web. Specific browsers like TOR are required to access dark web sites, which contain anonymous message boards, sensitive information, CSA material, online market place for drugs, weapons, etc.

With this introduction, it is very much required to understand data streams on Internet. Static and dynamic websites, social networking websites, forums, chat rooms can be viewed as data streams on surface as well as deep web. The above mentioned forms of web communication are unparalleled sources of data. Though the surface and deep web has been studied and learned individually, it lags discussion on objective based comprehensive platform

for data generation from possible data streams. Here we emphasise on objective of data gatherings from varied data streams from surface and deep web. Typically, data points from deep web could be of much of use to LEA.

Centre of Excellence (CoE) lab in VJTI Mumbai is working on comprehensive platform for data generation from cyber space. The following figure depicts the framework for comprehensive platform for data generation.

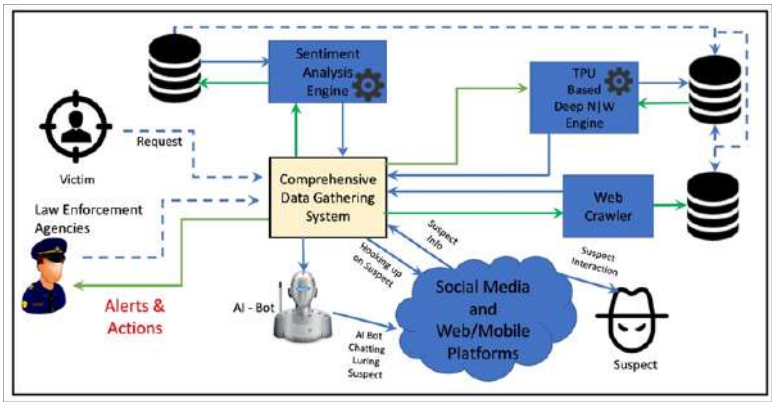


Figure Comprehensive Data Gathering Technology Platform

Each of the components of framework creates understanding of activity hubs or activity hotspot for related crime/ investigation requirement. Every daily event that creates stirs on web and mobile platform are registered using intelligent modules. Each event is marked and analysed using sentimental analysis, deep layered recurrent neural networks and understands its flow patterns using artificial immune network. These data provide the investigation agencies a clear understanding of focused platforms/groups to be investigated or quarantine for further investigation. The event information is also gathered using deception

bots with capabilities of chatting using high ended natural language processing tools. These bots can also be used to plot a decoy to generate evidence for required prosecution. Artificial Immune System (AIS) based epidemic hub detection is used to identify nodes/hubs responsible for viral percolation and spreading of information on social media platforms.

Emerging Security Technologies for Detecting critical cyber threats

Dr Munesh Chandra Trivedi
Professor, Department of CSE, National Institute of Technology

Abstract- The Cybersecurity is a major challenge now days because day to day occurring of Cyber attacks are increasing. The security professionals are required to create such strong security guidelines so that cyber attacks can be reduced. Previously all the organizations are using the reactive defense that is not sufficient for today's scenario, now the time to move for active defense. In this article, the various security paradigms are presented to prevent cyber attacks.

Introduction

In order to prevent organizations from the cyber attacks, a total security paradigm has to be followed which protect from internet-connected systems, in all respect data, software and hardware. In order to secure any organizations against unauthorized access both physical and cyber security play a major. The protection of IT Assets and reduce risk of attacking, the complete active cyber protection is required. A active cyber security model can be designed with continuous mentoring and having advanced threat prevention mechanism. Traditionally, the major focus was on securing only important system components and data

from the known threats only and less focus on less dangerous risks. But in current scenario, it is desired to have a model which secures the system completely from all types of the threats. We have to develop a proactive approach against all types of threats.

Cyber security threat vectors

A threat vector is a path or means by which a hacker can gain access to a computer or network server to deliver a payload or malicious outcome. Attack vectors enable hackers to exploit system vulnerabilities, including human operators. Popular attack vectors include the following:

- USB sticks and other portable storage devices
- Unsupported browser extensions
- Infected websites
- Orphan accounts
- Malvertisements
- Online quizzes and personality tests

Elements of cyber security

Traditionally, the major focus was on securing only important system components and data from the known threats only and less focus on less dangerous risks. But in current scenario, it is desired to have a model which secures the system completely from all types of the threats. We have to develop a proactive approach against all types of threats. The active cyber security models required coordination from complete information system, which includes all types of the security like application security, information security, network security and operational security.

The objective of application security is to reduce the unauthorized

access of data for access and modification. The information security deals with secure data during transmission. In order to secure data during transmission traditionally we are using the cryptographic techniques, in which, an encrypted or cipher text is sent from sender to receiver. The private keys and public keys are used for the encryption and decryption of data during transmission. The pure cryptographic techniques are not secure because if somehow hackers get the information about encryption and decryption method or keys used for the encryption. The steganographic techniques are used to hide the data, so that hackers may not identify whether important data is going on. The pure steganographic techniques are also not secure because if hackers get information about important data is hidden then they can steal the important data and misuse.

In today's scenario, in order to have complete security from unauthorized users, the combination of both the approaches cryptography and steganography is used to reduce unauthorized access and manipulation of data. This combination of two approaches is known as metamorphic cryptography. Here the first data is converted into cipher text then it is hiding into image, audio and video through the steganographic techniques. This two ways approach is providing a more secured approach to secure data during transmission from the unauthorized access.

Another, the role of network security is to detect threats by using strong security policy and prevent important data from the unauthorized access. The security policies are defined by the security experts of the organization by taking into considerations the various parameters. The objective of operational security is to decide to whom the control can be given or not to prevent important data and also a directives regarding course of actions

is issued to all employees of the organization that what to do and what not to do.

Why Cyber security is Important?

The data of any organization is the heart and soul now days for any organization. In order to secure data, it is required that reduce unauthorized access and also prevent cyber attacks. Some of the important issues addressed by cyber security are the following

- Protection of organization data from attackers
- Protection of organization networks;
- Protect unauthorized users from accessing digital assets;
- Reduce recovery time if a breach comes;
- Enhance confidence in the organization.

Cyber security challenges

The major challenges by hackers, data loss, privacy, risk management and changing cyber security strategies. In order to decrease cyber attacks, strategies for securing digital assets are needed to protect networks and devices.

In order to develop a active cyber security model, it is required that continuous evolution should be there Keeping up continual changes and advances in attacks and updating practices to protect against them. This requires all the elements of cyber security are continually changed and updated to protect against potential threats. This would be very difficult for the smaller organizations.

The end user protection and end-user education also play a major role in securing the organization from the cyber attacks, because if all the employees and end users are having the basic knowledge of cyber security then can easily identify what to do or what not

to do. Like when attackers send a virus to one of the employees and waiting for that employees may accidently bring and open a virus affected file in workplace on their computer so that he may attacks on the organization data through that virus. Another challenge is that less numbers of experts on the cyber security personnel with the right required skills to analyze manage and respond threats. As per the data available around 2 million unfilled cyber security jobs worldwide. It is estimated that by 2021, there will be up to 3.5 million unfilled cyber security experts jobs worldwide.

EMERGING SECURITY TECHNOLOGIES

The responsibility of data defenders is to protect data from the data thieves. While attackers or data thieves also try to explore new methods to theft the data or modify the contents of data. In order to secure the data theft a strong cyber security mechanism has to be developed. The five emerging security technologies are somehow play a major important role in improving of data security and reduce the data theft are the following:.

1. Hardware authentication

The user name and password can secure upto a certain extent only because hackers can easily track the user name and password details with simple packet capturing tools only. Also the inadequacies problem is also there with usernames and passwords. In order to have a more secure authentication, the hardware authentication can be a one of the main choice to secure the system more effectively and efficiently. The leading computer manufacture, Intel is moving in this direction. The sixth-generation Core vPro processor of Intel is having the hardware authentication feature. If we can combine hardware authentication with user credentials,

it will become a strong authentication mechanism in comparison to simple user authentication.

In case of Internet of Things (IoT) device, the hardware authentication is very important and plays a major role because in IoT Device network wants to ensure that the thing trying to gain access to it is something that should have access to it. In order to have more secure system, a model can be developed with three way validation from the end user firstly, what they know, such as a password; secondly, that they are, such as a username; and what they have, such as a token. A more secure system can be developed, if the end users are allowed to access the system onlyafter proper three way verification.

2. User-behavior analytics

As it is well known fact that simply user credentials are not enough to secure the system because when someone's username and password are compromised, the flaw in security can be easily understandable by anyone. After getting user credentials the hackers will enter into the network and initiate all kinds of malicious behavior. A more secure system can be developed If user behavior analytics is also included with user credentials, so whenever attacker try to do some malicious activity that behavior can trigger a red flag to system defenders.

The big data analytics techniques can be used to identify anomalous behavior by a user. So simply by comparing users present and past behavior, one can easily identify whether there is attacker or end user. So whenever there is sudden change in user behavior, someone else has taken over their account and a suitable action can be taken to prevent unauthorized access and prevent data theft.

3. Data loss prevention

The third another important emerging security techniques is data loss prevention. With the help of encryption and tokenization data loss prevention can be done. There are many approaches are used to prevent the data loss and data loss can be prevented from field and subfield level. This data loss prevention can benefit organization in number of ways:

- Cyber-attackers cannot monetize data in the event of a successful breach.
- If we used two ways security as discussed above i.e. metamorphic cryptography, the data can be securely moved and used across the organization. The big data analytics and business processing's can be performed on the data in its protected form. This will reduce the data risk and also reduce exposure of data.
- In order to protect payment, the organizations can use data privacy and security regulations for protection.

4. Deep learning

The fourth another important emerging security techniques is Deep learning which includes number of technologies, such as machine learning & artificial intelligence. As we have discussed in user behavior analytics, the anomalous behavior is discussed and focused in the deep learning. With the help of machine learning we can easily identify good and bad software and provide enhanced security paradigms. With use of machine learning and deep learning for anomalous the active threat detection can be achieved and we provide a better security environment and reduce time of taking corrective actions.

5. The cloud

The fourth another important emerging security techniques is cloud computing. The cloud computing is going to have a transformative impact on the security technology industry. With the help of cloud computing the organizations can virtualized their things such as security hardware, firewalls and virtualized intrusion detection and prevention systems. This concept virtualization can provide a better security platform to secure important data of organization from the intruders.

Conclusion and Future scope

Today's cyber attackers are well trained, organized, funded and use highly-targeted techniques that leave technology-only security strategies exposed. In order to have active intruder detection and prevent organizations from data theft, the organizations need to understand how they think, how they work, and what they want. The five emerging security techniques play a major role and prevent data theft up to a certain level.

References

[1] http://www.maawg.org/, last accessed: June 2013.

[2] http://www.antiphishing.org/, last accessed: June 2013.

[3] http://www.ostermanresearch.com/downloads.htm, last accessed: June 2013.

[4] http://en.wikipedia.org/wiki/Mebroot, last accessed: June 2013.

[5] http://www.emailtrackerpro.com, last accessed: June 2013.

[6] http://www.tamos.com, last accessed: June 2013.

[7] https://www.mandiant.com/resources/download/web-historian, last accessed: June 2013.

[8] http://www.majorgeeks.com/index.dat_analyzer_d5259.html

[9] http://www.winpcap.org/, last accessed: June 2013.

[10] http://www.riverbed.com/products-solutions/products/performance-management/wireshark-enhancement-products/Wireless-Traffic-Packet-Capture.html

[11] http://shibboleth.internet2.edu/

[12] http://www.aph.gov.au/house/committee/coms/cybercrime/report/full_report.pdf

Securing Cyberspace for Economic and National Security

Dr Vijay Kumar Kaul
Professor, Delhi University

Introduction

On 11 December 2019, newspapers reported a statement that Iran has 'identified and diffused a massive cyber-attack on its electronic infrastructure. It was a very large, organized and government attack.' No country or group has been named as an attacker. Iran is suffering from sanctions imposed by the USA. After withdrawing from Iran's Nuclear Deal of2015, the USA has imposed sanctions on Iran which has crippled the Iranian economy. In June 2019, the US cyber attacked the Iranian Intelligence system with a devastating effect. It was reportedly in response to an Iranian attack on commercial vessels in the Gulf. Earlier in the year 2009-2010 also, Washington used the Stuxnet computer virus, US-Israel joint creation, and disrupted thousands of Iranian centrifuge (enriching uranium) in Iran's nuclear sites.

In contrast to the use of force and the armed military attack, the vast majority of state cyber-attacks are different. These attacks are persistent, low-level attacks that may leave no physical trace. With the increased use of cyberspace for social, economic, political and military uses, these

cyber-attacks have become common in a large number of countries organized by states and non-state actors. These attacks are capable of significant damage to critical infrastructure, military assets, financial network, political and social stability, and inflict a huge economic cost. It, therefore, becomes essential for the state to develop strong cybersecurity capabilities and systems to create resistance to any cyber intrusion and attack, as well as offensive capabilities. The paper aims at examining India's standing in terms of cybersecurity capabilities and systems.

Cyberspace and Challenges

Digital evolution and creation of Cyberspace is the human mind's biggest invention. It has dramatically transformed human existence. Humans 'ability to digitize, store, analyze, and transport data around the globe has had profound effects in every sector of society and has changed the way we conduct personal, business, and political affairs. Today, approximately half the world's population is online and this number is rapidly increasing. But even those not personally connected to cyberspace are affected by its reach since the entities they rely upon to provide goods and services often use cyberspace for communications, logistics, and finance.'(1)

It has created immense opportunities and has also created a lot of challenges. The Challenges in cyberspace in the form of threats, crimes, and warfare have moved a long way: from computer virus in 1977, to hacking web sites, malicious code, to Advanced Worm and Trojan, to Identity theft(phishing) to, now in 2010 onwards Cyber Espionage

and Cyberwarfare. Forbes has predicted that "In 2020, we'll see an increasing number of cybercriminals use Artificial Intelligence (AI) to scale their attacks. AI will open the door to mutating malware based on attackers using genetic algorithms that are capable of learning, increasing their chances of success.' There are 141+42 cybersecurity subject predicted by the experts in the year 2020 which ranges from disrupting elections to targeted ransomware to privacy regulations to deepfakes and malevolent AI.(2)

India's Cyberspace capabilities

India is the second-largest country in terms of population, the third-largest country in terms of GDP on PPP and the seventh-largest country in terms of geographical area. It is a multi-cultural, multi-lingual, multi-religious country with a very fertile agriculture landmass, diversified industrial base, and a vibrant services sector. Its economy has been growing rapidly in the last two decades and has become around $3 trillion economies. It aims to achieve a $5 trillion economy in the coming years. India is also surrounded by enemy countries that have been raising a low-intensity proxy war against India. Also, the increased power of non-state actors/ terrorists to disrupt the economic functioning of the country is a serious threat. India's modern critical infrastructures like energy, telecom, ports, transportation, etc. are using digital technology and control systems. A large population of India is using the internet and smartphone and is counted as the second-largest online population. E-commerce is flourishing and generating huge data. With the increased use of digital payments, vast financial systems, and e-governance, cyberspace has become a critical area to be

protected and secured.

In general, it is perceived that India has a growing need for protection, however, it has paid little attention to cybersecurity capabilities. It lacks effective offensive and defensive cybersecurity capabilities and lacks access to mechanisms vital for confronting sophisticated malware. Global Cyber Security Index 2018 has placed India on 47thrank with strong commitment and capabilities in cybersecurity. Global Cyber Security Index 2018 prepared by ITU has examined the cyber capabilities and commitment of 194 countries on five pillars: Legal, Technical, Organizational, Capacity building and cooperation. All the countries are ranked and placed in three categories: High commitment, moderate commitment, and low commitment. India falls in the first category. The report has also projected that cyber-crimes will cost the world US$2 trillion by 2019. There will be fewer ransomware attacks but more personal data breaches as well as critical infrastructure breaches. There is a widening gap among countries in terms of cybersecurity legislation, strategies, emergency response teams, awareness, capacity to spread out strategies, capabilities and programmes.

India has enacted the Information Technology Act 2003 and the National Cyber Security Policy 2013(NCSP). NCSP is criticized on several grounds as it only talks about principles and no integrated framework is presented to operationalize cybersecurity threats etc. and there is no discussion on new technology risk. There are multiple stakeholders in the Policy which leads to ambiguity and indecisiveness. Moreover, India is still to develop DATA protection Law.

Draft legislation has been submitted to the Parliament in December 2019 and has been referred to Committee for further scrutiny and approval.

India has created a large number of cybersecurity institutions and capabilities over time. Some of these institutions are as follows: National Cyber Crime Coordination(NCCC), Indian Computer Emergency Response Team(CERT-In), National Critical Information Infrastructure Protection Centre(NCIIPC), Cyber Swacchta Kendra, National Technical Research Organisation (NTRO), Network Traffic Analysis System(Netra) of DRDO, CERT-Fin (For Financial Sector), Crisis Management Plan.

There is also a shortage of skilled manpower. NASSCOM has estimated that India needs 1 million skilled people whereas at present we have around 50000 trained workers. It needs the involvement of Universities and higher educational institutions. This will also take care of the unemployment problems in India.

Integrated Cyber Security Strategy and Policy-Need of the Hour

India needs an integrated cybersecurity strategy and policy because of ever-changing technology and threats. As mentioned above, the use of AI in cybercrime and attacks needs a new strategy and technology. Such a strategy will be based on four pillars:

Public Awareness and education: All people need to be made aware of the risk involved in the use of cyberspace, sharing their information and losing privacy. All the services available on the cyberspace take the information

of an individual and their activities as consideration. The business models of the companies operating in cyberspace keep on changing. An up to date awareness of these issues needs to be given to the people. The government should develop some mechanism for providing these services.

Technology: The second pillar of such a strategy is the development of technology to protect from the cyber threats, attack and wars. At the same time, it needs to develop offensive capabilities also to be able to send signals and impose a cost on the attackers. Technology is changing fast. There is a need to develop skilled manpower and research talent to continuously improve their capability.

Legislation: the third pillar is the legal framework to protect the data, capabilities and institutions. It should also penalize the entity for breach of privacy and data.

Cooperation: Lastly, there need to develop cooperation internally and externally. Internally, there is a need to develop a cooperative environment among the institutions looking after cybersecurity. Even for developing skill capabilities, collaboration between educational institutions and government institutions is required. The industry should also collaborate to identify new types of technology and threats. Internationally, with the growing threats of cyberwar and crime, collaboration at the UN and other international body level is required. Last year on 12 November 2018, President Emmanuel Macron of France launched the Paris Call for Trust and Security in Cyberspace urging for the development of common principles at the UNESCO Internet Governance Forum. New network and

institutions are emerging which require a collaborative mindset to protect others from cybersecurity threats and wars. There is also a need to identify and collaborate with them.

References

1. *Advancing cyber stability- PROMOTING STABILITY IN CYBERSPACE TO BUILD PEACE AND PROSPERITY, The Global Commission on the Stability of Cyberspace (GCSC), Final Report, November 2019*
2. *https://www.forbes.com/sites/gilpress/2019/12/12/42-more-cybersecurity-predictions-for-2020/#630d8efc4a56 accessed on 15th December 2019*

Intel Gathering and Social Media based Sentiment Correlation

Dr. Sandhya Tarar,
Assistant Professor, Department of Computer Science and Engineering,
School of Information and Communication Technology,
Gautam Buddha University, Greater Noida, U.P., INDIA

In the era of Open Source Intelligence and predominance of digital media, information collected through military and government intelligence is exploited commercially by various alien stakeholders to feed their vested interest and may even by a nexus operated and funded by the opponents of our country.

This clandestine intelligence gathering poses a potential threat to the sovereignty of our country as it may create strife within the community by deploying a multifaceted digital attack on the social fabric of the nation. It is worth mentioning that social media is playing a crucial role to accumulate such intelligence and antagonist facilitators are not leaving any stone unturned to manipulate and adversely affect people's sentiments to create hurdles for the government.

This is beyond doubt that niche technologies like the Internet of things, Cloud computing, Artificial Intelligence, and Big Data Analytics are being used by these adversaries to gather intelligence and manipulate or influence opinion of the masses. We should be aware of the fact that all plausible efforts are in place to manage people's sentiments against

the govt., its policies and against the decisions undertaken. They are of the belief that anyhow they have to distort the social structure of our nation by any mean ranging from religious, social, commercials and even defense.

Data is being exploited commercially and multibillion-dollar trade based upon data is taken out from India and other countries by some business giants. It is being used widely for market prediction. As quoted in recent times that, 'data is the new oil', it is quite evident that in the foreseeable future, data is going to become a source of power and earning inflated revenues. Companies are making a fortune owing to the data collected through social and digital media through payment gateways and other means they can draw trends about the potential customers by knowing their purchasing power, buying behavior and other characteristics.

For example, the U.S., Russia and China employ aircraft's of various specification and specialty. On the contrary, like other countries, China has a tendency to steal the design details to save on the huge cost of investing in setting up a design lab. Lockheed Martin's F35 Joint Strike Fighter is a perfect example of China's misdeed. Its design was compromised by Su Bin, leading to China's J-31 program.

In India, there was a time when defence operations were not questioned and were beyond selfish motives and mal-intentions of the biased politicians. But nowadays, social media is having significant impact and is influencing the mindset to raise questions that challenges the sanctity of our defence operation(s) which is an alarming situation

for our democracy where the mindset of our policymakers can be distorted by digital media with the pretext of evil ambitions.

For example, refer to the time period during the abrogation of Article 370, enemies of the state tried to create civil unrest out of the situation through the rampant use of social and digital media within and outside the country.

However, this is the perfect example to depict how a certain section of the people with their evil intentions made it a religion based affair and manufactured a propaganda out of it, and comprehensible role of social media, in this case also, cannot be repudiated. The sole intent of these adversaries is to castigate the sovereignty of our country.

Alacritous focus should be on the sorry state of our organizations in terms of data contravention and associate threats, as according to recent survey by Forcepoint and Frost & Sullivan found out that 69% of Indian organizations are at risk of data infraction with 44% of them encountering a data breach before and 25% failing to perform any breach assessment in the last annum. In addendum, not enough C-level teams are involved in cybersecurity preparation with only 34% mainly at BFSI, Telecom, Information Technology and BPO companies engaged in it [3].

There is no doubt that being a developing country we need to strengthen our data infrastructure with some fast pace cutting edge technologies and on the other hand the government has to put intense and quick efforts to develop a mechanism (hardware, software both) to deal with any mitigated scenario.

REFERENCES:

1. *https://nationalinterest.org/blog/buzz/hacked-how-china-stole-us-technology-its-j-20-stealth-fighter-66231*
2. *https://m.economictimes.com/industry/telecom/telecom-news*
3. *https://www.pressreader.com/india/the-economictimes/20191126/281745566236372*

Intel Gathering & Sentiment Analysis

Karthik Vaithianathan

Chief Technology Officer, APCO Digicon

The modern-day internet as we know today came from ARPANET that was invented in 1983 by DARPA (Defense Advanced Research Projects Agency), USA. ARPANET was the first to implement both packet-switched networking and TCP/IP protocol which connected a set of computers and enabled communication between them. Today, the internet connects computers, storage and servers across the world and has more than 4.5 billion users (almost 60% of the world's population). In India alone, an estimated 627 million users are expected to use internet by end of this year and about 96% of these users access internet from their mobile phones.

Several companies have launched "free" services through applications or shortly called as "apps" on the mobile phones. The idea is to create certain level of deep engagement with the users by offering them "value" or "service" free of cost. In return, these companies want the users to upload their personal data including name, age, gender, location, preferences, records of their activities and express their suppressed feelings/thoughts/ideas. In addition, using data

science approaches, the application providers generate huge amount of derived information from raw collected data.

Specifically in India, we also see that users from both urban and rural seek to upload their personal information in many forms – text, images and videos into the data servers of the "app" service providers (data here can be both public and private). Largely, these "app" service providers including facebook, google, twitter, tiktok, helo and truecaller belong either to the USA or to China. Through various legislatures, both the countries have free access to the data (public and private) that is being uploaded by Indian citizens. Not alone that Indian government does not have any means to have access to this data, but the profile data of Indian citizens being available to other countries could be a potential threat to the safety of our citizens.

However, even without having access to the data servers of these "app" service providers, intelligence gathering from the internet is possible and this paper describes one such approach.

On a high level, data exchanged on internet can be classified as follows:

1. Free, unprotected, genuine data (example: wiki) that is being uploaded for use of internet users across the world
2. Protected data exchange between server and client for genuine reasons (example: bank website access, secure information transfer over VPN)
3. Protected data for unlawful reasons (example: two terrorists exchange intel via VPN)

4. Pirated and incorrect information such as wrong propaganda about Indian military operation that is being spread for free (example: movies and other data that is being uploaded by non-copyright owners)
5. Malicious data and code that is being spread for wrong reasons (example: malware, spyware)

The goal of intel gathering for sentiment analysis is to ensure that we deal with cases (3), (4) and (5) effectively while leaving (1) and (2) untouched.

We propose that Intel gathering to be done by a distributed cloud-based software called IntelGagent and sentiment analysis to be done by IntelSagent. IntelGagent essentially gathers information and transactions from various IP/ Web sources, cleans and prepares the information into a set of documents. IntelSagent performs analysis on these documents using Machine Learning (ML) trained models.

IntelGagent follows two approaches:

A. Performs proactive and systematic crawling of freely available web pages including social portals to construct consolidated document structures
B. Instruments microcode (that records data and posts to IntelGagent) in important data access points so that transactions are captured and sent to the intel gathering agent

WHAT DOES MICROCODE IMPLEMENT?

Microcode shall implement various types of patterns or rules to detect data exchanges of types (3), (4) and (5). Once detected, the microcode shall post information to the IntelGagent server.

WHERE TO INSTRUMENT MICROCODE?

Microcode has to be implemented in all "access points of data" herein referred as APOD. What is APOD? All transactions in the internet follow a common model where 'users' pull or push data to a 'web server'. APOD is either end of this pipe where we have access to. This pipe could be even encrypted using VPN.

WHO ARE THE SERVICES PROVIDERS THAT MUST BE MONITORED (APODS)?

A. ***All domain hosting service providers and DNS service providers must be instrumented with microcode provided*** by CKS. Internet is made of compute servers with unique IP addresses. However, current monitoring and actions are taken only based on DNS. Further DNS service providers nor Domain Name Hosting service providers are being held responsible for actions that happen on the domain name they host. Thus, the intel gathering agent has to be essentially monitoring the transactions based on IP and not on DNS.

B. VPN service providers

C. SSL service providers

D. IXP service providers

E. CDN service providers

F. Internet and Mobile Service Providers (ISP/MSP)

SENTIMENT ANALYSIS BY INTELSAGENT

Once data collection is done by IntelGagent, we further do sentiment analysis as follows.

1. Preparation of data for analysis
2. Natural Language Processing (NLP) based pattern detection
3. Image and Video labeling using ML models
4. Training of ML models with various patterns and conditions corresponding to anamolies/attacks/ suspicious activities
5. Filtering of prepared data using ML models
6. Definition and synthesis of Sentiment

SUMMARY

There are several other approaches to gather and analyse sentiments especially for intelligence. We have given one such approach. Implementation of Sentiment analysis requires large compute and storage capability (Data Center). We propose that a central government agency is formed which will manage the data gathered and analysed for intelligence. The agency can provide secure API to other government agencies such as State Police Departments and CBI for the purpose of both giving and gathering information.

Indian culture - Threat of Cybersecurity

Mr Ajay Kashikar

Consultant, E-zest

With digitization, citizens are extensively using and enjoying social sites like Facebook, WhatsApp, Instagram, and Twitter. Everyone is eager to comment, socially, and politically wish to share, comment, and interested in knowing what others are doing.

The other side of it is, India has a high culture, and this is in our blood for generations. We believe in society, social cohesiveness, and like big data, we believe Big Family. We easily talk, get connected with anybody during the journey or at the workplace, garden anywhere... They are the best examples of how easily we share our personal information without any hesitation. The term Stranger outside India and within India means differently. We believe in social connection and share what not with strangers, and we don't mind it, nor do we bother it. This is a big issue and concern for data protection, securing India.

Discussing the data and Cybersecurity in India, we must remember that due to the digital or global impact, we cannot change our culture and values easily, and we must not. The interpretation and execution of law should be based on the deep understanding of our cultural values, mindset and

practices else implementation will fail in India. This leads to the loss of data security or weak compliances.

The compliances, rules, and regulations of Cybersecurity shall be defined by the authority maintaining these values and not based on global threat or practices or pressure of other countries. We must have our laws for protecting our data, the security of individuals, and nations.

The gap between culture and extensive usage of automation is not understood by the authority who is designing the rules and regulations and always leads to various social, legal, and constitutional issues for our nation.

Cyber Security Threats for Indian Industry

The globalization and multinationals' entry into the Indian market and digitization has started

creating data security threats very slowly to the Indian diaspora. The Indian small and medium

manufacturing industry working with these organizations are bound to follow the GDPR (General

Data Protection Regulation) and other security compliances. India has not yet enacted specific

legislation on data protection. The affected areas in the industry are

- Research and Product Development
- Designing of the new product, Drawings, photos, plant maps.
- Technology Innovations
- Accounting and Financial Services – BPO / KPO

- Manufacturing process excellence
- Customer Data of Indian buyers within India exposing to the outside world
- Technology & IT company data leakage through:
- IVR systems
- Cloud computing
- Data Centre, Disaster Recovery Centre
- GPS, GIS

For the above areas of operations in the industries, we very well know the threats for various data security, data leakage, data protection related issues while sharing the data within the companies and outside the companies, country.

Cyber Security Threat - Banking, Health & Insurance

In recent years, in spite of having cyber laws, the Credit / Debit card data of Indian customers and banks have been exposed. Many cases of cyber fraud have filed, but in reality, no great success, since India is not having stringent rules on data protection.

Health & Insurance Company's data protection is worst in India. The policyholder data related to individual for Life, Vehicle, and general insurance are readily available in the market, and this leads to major cyber / Data security issues.

The data exposed is widely used by healthcare, pharma, and automobile companies for current and future business forecasting. It may also be leading to unknown threats for cyber-attacks or may be used for war purposes by enemies.

Core Banking Systems (CBS) are not sufficient to cover

Indian Operations. Lack of vision in product development leads to cybersecurity threats

- DC / DR sites are not with the appropriate hands – controlled by the third party and not by banks
- Inadequate knowledge of IT staff/officers
- Weak Systems Audit Processes ensures paper compliances
- DCC's and Co-op bank – no uniformity of CBS leads significant data security issues
- RBI / NABARD / State Apex Banks do not have sufficient Cybersecurity / IT / Big Data processes in place

SUGGESTIONS

The above three sectors are directly contributing to our nation and are under the threat of data security. If we do not ensure the data security and it keeps leading to data exposition, our ecosystem may get paralyzed within no time by the cyber-attacks. From preventing such threats, we shall have a perfect roadmap for securing our data for the coming decades. A robust framework is a must for addressing Cybersecurity, policies, and practical implementation. Following are the general suggestions that must be in place while building the policies

- Compliance based on the cultural value of our nation
- Awareness and knowledge to the ordinary citizens for data security
- Identify the "Stranger" in the digital world – mobile, email, photos

- Legal bounding on social networking for non-capturing of location-based data of individual
- Regulatory tightening of individual identifies data (photo, PAN, AADHAR, Passport) leakage during the registration, verification, and sharing of individual identity at Mobile company outlets, Banks, automobile dealers, departmental stores.
- Restriction of non-collection of mobile Nos at the time of usage of payment devices in various malls and other payment collection outlets
- Data leakage protection from DND services with all mobile operators

The Way forward – Protection from the Threats

The roadmap has the comprehensive "intelligence data gathering technology platform" to empower agencies to correlate data from disparate sources to identify and predict attacks, following are the suggestions:

- Create a Big Data platform that can be used by different agencies to detect, identify, predict and act on threats on a need to act basis
- Use Machine Learning (ML) and Artificial Intelligence (AI) to predict attacks
- Develop indigenous technology to counter cybercrime and other threat
- Enforcement of Cybersecurity Law to have major compliances for social networking sites having protection on data privacy
- Use of process methodology techniques for policy

designing and implementation

- Education and Training to the schools on Data Protection, Data Security and Data Privacy

Cyber Security and Citizen 2030

Dr Deepak Deshpande
Chief Human Resource Officer- Netmagic Solutions

Background

Today, data security has become more important than ever. Data is the new currency. Hence, it becomes imperative to ensure Data Sovereignty for every country.

Indian government has recently taken a stand to keep the critical consumer data within its borders. A step in the right direction is the 'Data localisation policy' by Reserve Bank of India. Large global organisations having large presence in India may have some reservations but home-grown companies have largely welcomed these regulations.

Let us take a quick glance at data security issues for 2020 that are looking into faces directly and could jeopardise these efforts to fortify our cyber security policies. It's important first to ensure data security even before we talk about data. This is critical to our formulation of policies, mind-share to securing India, our cyber assets, data and our people to prepare a road map of actionable steps.

Cyber Security Challenges Beyond 2020 - Points to Ponder

We have seen major data breaches hitting reputed industries

globally. They hurt both our financial interests and hard earned reputation. Majorly, these breaches are planned attacks, others are results of human errors. Hence, our motto should be 'Security First before Data itself'. Such threats start from fake data generation to distributed frameworks.

These include:

- Fake Data Generation.
- Management of humongous data
- Real Time Security Audits & Compliance in complex network and data environment.
- Establishing of Data Prominence

Getting Ready – The Game Changer

To realise the objectives of digital India, data sovereignty and data colonisation, its important recognise the need to invest and leverage the new big opportunity India offers today. Market insights have proven that data centres is the next big opportunity in India. Mobile data consumption, the government's digitisation drive and thrust on Smart Cities is also fuelling demand for more data centres.

RBI Policies on data localisation makes it imperative to store certain types of data to be stored locally (within the country). This has generated high demand basis the market estimations that over 70-75% of this data is hosted outside India. Due to this, global companies are now reviewing their policies and are investing in establishing facilities to host data in India. The earliest adopters of local data centres are BFSI Companies.

Data Points per industry estimates and market reports:

- Data centre market has been growing over 25% in the last ten years.
- India today requires 12-15 times more capacity than what is available today.
- Major global players like Amazon, Microsoft, Google, NTT are expanding in India
- Data centre outsourcing market in India, is projected to reach $5 billion by financial year 2023-24 from the current $2 million mark.
- In India is poised to be the biggest hubs for colocation data centres globally.
- Cloud Computing Services market is growing at 40%

The government is giving a big push & establishing a national data governance centre to hold all public data, and formulate guidelines for the management of data. State agencies and even start-ups could access the data through this facility.

Data Centre World in India		
Data Center Critical (IT) Infrastructure Providers	Prominent Investors	Prominent Support Infrastructure and Construction Services Providers
Atos	Adani Group	ABB
Arista	Bridge Data Centres	Caterpillar Inc.
Broadcom	BSNL Data Center	Climaveneta
Hewlett Packard Enterprise	Bharti Airtel (NXTRA DATA)	Cummins
Cisco	Colt Data Centre Services	Delta Group

Dell Technologies	CtrlS	Eaton
Huawei	ESDS	KOEL (Kirloskar Group)
IBM	GPX Global Systems	Larson & Turbo (L&T)
Lenovo	ITI Limited	Legrand
NetApp	NTT	MTU On Site Energy
	Pi DATACENTERS	Netrack Enclosures
	Reliance Communications	Riello UPS
	Sify Technology	Rittal
	ST Telemedia GDCs	Schneider Electric
	Yotta Infrastructure	Sterling and Wilson (Shapoorji Pallonji)
		STULZ

Challenges Ahead

1. Availability of uninterrupted power supply and land banks in high demand areas.
2. Expansion is currently limited to Tier 1 cities due to power availability but the land cost are prohibitive, thus making the offerings unviable.
3. To establish and operate quality data centres, we need highly-skilled professionals in specialized functions like cooling, power, security, and network. This increases manpower costs and training budgets. Lack of clear rules & enabling regulatory framework.

4. Engineering Education Needs Serious Revamp. Fresh passed out graduates are not career-ready to take up these jobs. This gap needs to bridged. Policies to be tweaked.

Critical Threat Handling Using Native Technologies

Mr Rajkumar Mohanraj
Director, IT, Apco Digicon

Critical attacks on Data Centers are coordinated, targeted and well planned. The attackers have a well thought out plan that is made of four phases – 1) reconnaissance phase 2) prelude or setting up phase 3) core phase and 4) tail-end or data collection phase. During the reconnaissance phase, the intruder is generally spying or snooping looking for vulnerabilities and study the nature of data accesses whether it is network access or database access. It is important to understand nature of the accesses, as the attacks are designed to imitate real accesses. In the second phase, necessary code is implanted without triggering any alerts. In the core phase, the number of malware accesses multiplies and starts to bring down the system and if the attack to steal data, then the required data is extracted, packaged and sent to remote servers. In the final phase, the signature of the attack is purposefully destroyed or morphed with attempt to remove any evidence of attacks.

We propose to design machine learning based agents that will monitor and learn regular network and data accesses. Once the regular accesses are learned, any difference in access patterns are detected and considered as suspicious. In order to train the neural models, we need to collect plenty of data and use them for training. This is not an onetime activity but an on going activity. In order to implement

data gathering and machine learning modles, we suggest a centralized government agency and and a data center strategically located in the middle of our country. We propose the name for this proposed agency as Indian Cyber Space Reconnaisance and Response Agency – ICSRRA.

Using IoT and data gathering techniques as discussed in the previous round table discussion, data shall be streamed to the centralized data center owned by ICSRRA. Similarly, for any attack that is detected, a response is designed by ICSRRA and propogated back into the internet or respective data centers where the attack is in progress. The response in general is made of following elements – a) Warning b) Set of actions to mitigate the attack c) Set of actions to restore to old state.

To conclude, next decade is going to be driven by data. Data is the new mineral. Control of one nation by others will be primarily determined by who controls the cyber space. Thus we highly recommend for our nation to form ICSRRA as soon as possible.

Discussions Areas Imperative to Cybersecurity and India

Ms. Vaishali Patil

Entrepreneur in Skill Development Industry,

Director, Study Circle

1. Along with technology and ML and AI it is important to imbibe intuitive learning across levels of HR within and outside the government. Because resilience will come from being able to think and act intuitively and laterally in crisis situations. Ability to be able to live in an internet apocalypse will be crucial.
2. It then becomes important to consciously include intuitive learning besides the latest technology updates in all levels of syllabi.
3. Like the IAS, IPS, etc introduce a Specialised Indian Cyber Service, an all India service recruitment to which can be done through the UPSC with common prelims. But separate mains for this service.
4. Health and Fitness should be a part of critical infrastructure. During disaster management, the golden hour plays a crucial role in saving lives and integrated data related to health if linked with something like Aadhar and treated as critical can be vital.
5. Define the scope of cyber resilience separately from cybersecurity and make it part of the everyday

discussion of the common man because a single smartphone owned by a rural citizen can become a potent weapon to test our resilience at any level.

6. Make cybersecurity and resilience not only part of the mainstream education curriculum but also part of continued education in corporates and government departments for mid and sr managerial levels.
7. Like CSR makes it mandatory to make budgetary provisions for cyber resilience by organizations whether government or private.

We can talk of knowledge sovereignty but data nowadays is not sovereign at all and protecting the sovereignty of a nation like ours in such a scenario will need a multi-pronged approach. We are blessed to have strong democratic institutions in which people have faith. This should be leveraged to make data security and resilience part of everyday conscious awareness of the common man.

Intelligence Gathering and Social Media Sentiment Correlation

Ms Ihita Gangavarapau

Co-founder of Youth Internet Governance Forum India

Internet has a ubiquitous presence. Globally almost 3.5 billion are users of social media of more than 4 billion internet users. With a rapid increase in the penetration of the internet and its proliferation, tremendous amount of data is generated. The data generated is invaluable when analysed correctly and is now a new form of wealth for a nation.

Social media is a platform where various activities take place. It is where all the feelings and sentiments accentuate. Thus, this increase in velocity of spread of information has led to opinions getting hardened quickly. There is now a shorter time span for sentiments to turn into action. A small negativity would increase multifold leading to something detrimental. It is therefore crucial to determine the emotional tone behind words to gain understanding of the attitudes, opinions and emotions expressed within an online mention.

The companies and businesses have been doing social media sentiment analysis and correlation. They have been performing in-depth analysis to find sentiments and opinions of users over social media helping them with getting better audience insights to provide better customer service. It also helps them keep aware of brand perception.

It is therefore a no brainer that the government should be

involved in gathering intelligence and analysing sentiments of its citizens online. Pre-emptive action needs to be taken by the government for which they should be able to monitor its citizens to deescalate future tensions. It is essential for national security and stability purposes, public order and to ensure economic progress in the long run. However, the main question that arises is how do we make the surveillance legitimate?

Actions arising out of social media correlation can hinder various rights. There have been dialogues and debates from the public regarding invasion of privacy, which can be addressed through aggregation and anonymizations. Other most important concern that comes up with governments analysing social media is the suppression of free speech.

To cope with this challenge, the traditional intelligence gathering methods can establish areas of concern geographically, demographically and temporally. Social media can then be used as a tool for analysing sentiment for a targeted set. Approval can be taken from the appropriate authority for performing sentiment analysis for that set which intelligence gathering has said is an item of concern. The results of the analysis can be curated using correlation tools with a facility of logging to create logs for curation and oversight. We require an institutional mechanism in place that will use the insights appropriately so that rights such as free speech are not supressed.

Thus, social media can be used to supplement traditional intelligence gathering methods and this can help governments in making surveillance and monitoring more transparent for its citizens.

Cybersecurity and its Necessity for Land-Based Access Rights

Ms Shravishtha Ajaykumar
Associate Director - Centre for Knowledge Sovereignty

Through history, humans have associated ownership, with all that surrounds them, primarily the land that provides for them, forming a largely symbiotic relationship with the land owned.

It was, therefore, second nature for humans to allocate ownership of land to those who cared for it and thus could reap its benefits.

This form of ownership, though historically began with demarcating areas with right of way for hunting, to agriculture, has now evolved to homeownership in the modern-day Indian scenario.

The recording of land that is owned has been an important topic as this has determined, across time, to date the access that a person has to different facilities, ranging from social to commercial. However, the demands of such administration are evolving along with technologies.

Blockchain technology, though often confused with cryptocurrency, is merely inclusive of the same. Blockchain, as it consists of any data record, is the future of land records, and thus of all documents; financial, medical, familial, and all others that impact a person's day to day life.

Often, when certain social groups are found living in close quarters, the land that encompasses this area is categorised following the records of the few sample persons that utilise that land first. In case the original owners are successful. The records of future tenants are raised in quality, leading to risk, for example, for banks that might provide loans even if the new residents have a history of absconding payments. Currently, land records and the historical feature that these lacks are the cause of much discrimination and ghettoisation.

The ability to register land to own the need to use geospatial technologies like 3D scanning is becoming increasingly imperative. The complexity of these issues requires the introduction of ever-evolving technologies and the formalisation of these operations.

When technology is used to collect and maintain data, it becomes further susceptible to security issues. Without digital systems, there is a tremendous opportunity for the pipeline to become corrupted. The digital systems currently present are already an improved form from what preceded it. Blockchain technology can maintain records in one format across local borders. In case of disaster, data recovery is straightforward and efficient.

Using blockchain technology will also help the land administration avoid attacks. Not only are attacks more difficult, since the data is saved across different nodes, which are cryptographically connected, but each node requires unique authentication.

However, the viewing of this data is still possible by the

public using access codes, without the need for a notary. This feature thus helps both decrease susceptibility to attacks and theft but increase transparency.

The introduction of such a technology will thus ensure that all records are maintained for individuals, as compared to clusters, which is currently a drawback of different methods of land administration that are devoid of updated technology.

The issue of security with open records is one of the main ones that come to mind in such a scenario — specifically, cybersecurity. As land administration ICT systems and files are being digitised, cybersecurity becomes more and more critical concerning safeguarding people's ownership of their single most valuable asset. When digital systems come under attack, there is a threat that land and property records could be hacked and manipulated. Blockchain technology offers an added layer of security through its immutable nature and the advantage of limiting the tampering with of records generally. This feature of the blockchain is expected to become more prominent in land administration.

With the advent of geospatial technology and ensuring data is protected via legal cybersecurity policy frameworks, land administration, what is said to hold over 50% of the world's wealth, will be secured and retained.

Further, as mentioned in the prologue, the susceptibility of social implications negatively imposed on tenants and owners, upon the basis of land ownership will not impact them to the extent of the vicious cycle that is currently a symptom of land administration, nor will it affect future

generations and surrounding persons through the fault of generalisation.

One of the more clear applications of a combination of geospatial technology and cybersecurity is accuracy. Using such techniques will ensure that land disputes are limited because the distribution of land will be maintained via coordinates uncorrupted, as compared to the human description of dynamic features of the land.

Cybersecurity, will thus, impact not only the land administration of a city but by extension the planning of a city, allowing for greater access to top facilities to all citizens, as compared to those who live in more expensive areas vs ghettos.

Data localization and protection dimensions: A conversation

Mr Rajat Dhar
Managing Partner, Finogent

Today, we are entering a phase of increasing digital footprint. Be it businesses, government, citizens or academic institutions, the digital web of data that these bodies generate continues to grow and expand touching newer frontiers.

The journey so far

Internet came to India, in the year 1986.It was initially launched in the form of Educational Research Network (ERNET) that was orignallymeant for the exclusive use of educational and research agencies and institutions in the country. It was launched as a joint effort of the Department of Electronics (DOE), Government of India, and United Nation's United Nations Development Program that supports the development endavors of developing nations.

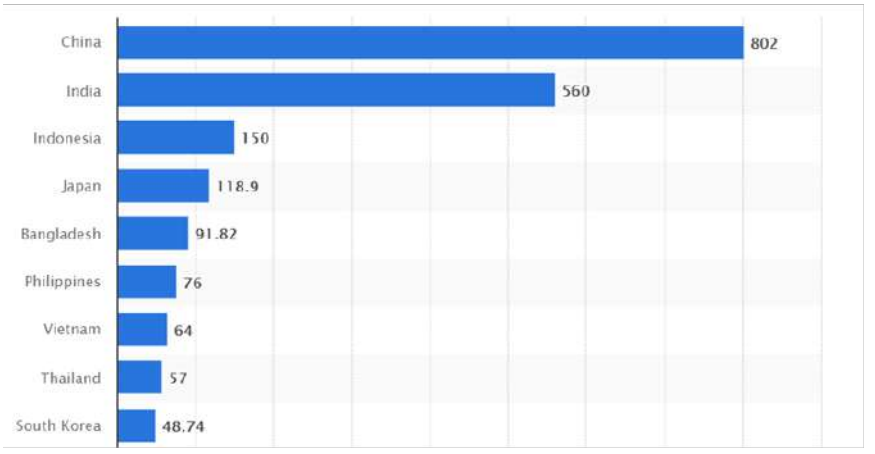
There was also the NICNet that began in 1988, the network was operated by the National Informatics Centre with the purpose of improving communications between government institutions.

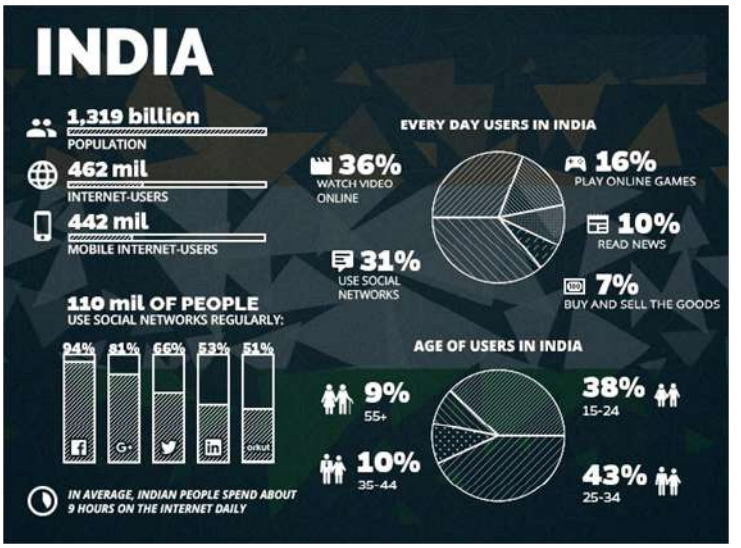
1995 was a historic year for the nation as it heralded the attainment of two big milestones. The first cellphone call in India was made in July 1995 and in August, the Internet

was thrown open to public.

Internet usage in India has grown to over half a billion people for the first timethis year (2019). This number is today pegged at approximately 566 million. This growth has been driven primarlyby rural internet growth and usage riding on an explosive growth in bandwidth availability and use of smartphones.In its ICUBE 2018 report that brings out numbers connected with digital adoption and usage in India,the market research firm and analysis firmKantar IMRBhas stated that the number of internet users in India jumped by a whopping 18 percent as of December 2018this represents nearly 40 percent internet penetration.

The total Number of internet users in a few countries in the Asia-Pacific region as of January 2019, by country (in millions)





Everyday internet users in India (source, DoT, Statista, Telco filings, and other sources)

India's digital success can be gauged by the following numbers. The country has the world's highest data usage per smartphone at an average of 9.8GB per month according to a report released in June 2019. Indian mobile data users consume more data than their Chinese and Korean counterparts who consume 5.5 GB per month and 8-8.5 GB respectively. Indians have 1.2 billion mobile phone subscriptions and downloaded more apps -- 12.3 billion in 2018 -- than residents of any other country except China.

India's data consumption numbers peaked in 2019, with almost every operator offering data at cheap rates. Also, the mobile data traffic is now growing exponentially as a significant number of Indians are now spending more

time accessing videos, infographics and other forms of contentthat is expected to account to account for as much as 75% of overall mobile traffic by the year 2024.

The report goes on to predict that the total monthly mobile data traffic numbers will grow at a CAGR of 23% growing from 4.6 exabytes in 2018 to as much as 16 exabytes in the year 2024. Smartphone user base in India will touch a high of 1.1 billion by this year (2024) as well. During the same period, the mobile broadband subscriptions will rise from 610 million in the year 2018 to touch 1.25 billion. These numbers will testify to the success of India's digital expansion drive with active assistance from telcos.

Increasing penetration of the internet while offering an opportunity also brings with it its own challenges. Content bearing hate speech, fake news, porn, and other reprehensible material is on the rise as well. An overwhelming proportion of data traffic emerging from the country is directed towards sites with questionable content. The use of VPN and other means to mask origin and IP address is also emerging as a source of concern for agencies in India.

Cyberattacks and related concerns

India has been the second most cyberattacks affected country between 2016 to 2018, according to a Data Security Council of India (DSCI) report released in 2019. It also states that the average cost associated with a data breach in India has gone up by as much as 7.9% since 2017. The average cost of a breach today costs INR 4,552 ($64) in the country.

Increasing cyber-attacks has also resulted in many

companies opting for cyber insurance policies to address the risks associated with cyberattacks. As many as 350 cyber insurance policies have been sold in the country till the end of 2018, which works out to a 40% increase from the year 2017.

The possible impact of a cyberattack

- The outflow of foreign exchange as ransom
- Data theft and espionage
- Capital leakage
- Loss of credibility for businesses
- In vital sectors like healthcare and critical infrastructure, it can lead to the loss of billions of Rupees
- Reduced attractiveness of the nation as an investment destination

DATA LOCALIZATION AND WHY IT MATTERS

Among reasons supporting data localization put out by the Justice Srikrishna Committee report last year, a few key ones are: Data localization is a critical aspect for all law enforcement agencies. Getting hold of data by Indian law agencies, post a data breach, a cyberattack or a threat, cannot be dependent on the mood of or the legal or any other process of a nation that hosts data generated in India.

Fact: countries such as India and Indonesia are among the most data rich nations in the world. But barely receive any data infrastructure related investments from companies based in the developed world

In a hypothetical case, if for instance, data generated in India is stored in the U.S., data consumers in India will have to rely on technology and channels including undersea fiber optic cable network to access the data. Such a reliance can prove to be a serious handicap in the case of a breakdown in technology or due to snapping of connection due to cable damage. The report recommends that to avoid such situations, at least a copy of the data generated in India must be stored within in the country itself.

THE ECONOMIC IMPACT

A 2018 study commissioned by Facebook claims that its data center activities in the US had created tens of thousands of jobs, supported investments in renewable energy and contributed nearlyUS$5.8 billion to the GDP of that country in just a tad over half-a-decade.

PRECEDENT

Canada and Australia protect their health data diligently. In South-East Asia, Vietnam mandates one copy of data to be stored locally. In addition, it also asks any company that collects user data to have a local office.The most comprehensive data sovereignty laws in existence today are in China and Russia, which mandate localization across multiple sectors for many kinds of personal data. Quite unlike the GDPR formulated by EU, citing national interests, China mandates strict data localization in servers located within its boundaries.

South Korea, requires the consent of the person associated with the data for it to be transmitted overseas. France is pursuing its own data center infrastructure, dubbed “le cloud

souverain", despite the closure of some of the businesses that had initially floated the idea. The most comprehensive data sovereignty laws in existence today are in China and Russia, which mandate localization across multiple sectors for many kinds of personal data.

Data colonialism

Social media giant Facebook counts India as its largest market in terms of users. Despite this, the only data center the company has in the whole of South Asia is situated in Singapore. Since then, India has boycotted a declaration on data flows, holding the view that large tech companies still harbour a colonialist mindset towards emerging economies, with an eye on stockpiling our data, rather than focusing on development.

If one looks at the last few years, India has emerged as a rallying point for nations that wish to localize data. India is in a strong position to do so given our large-scale digital industrialization and highly skilled manpower base not to mention the government championing the cause at all levels. India has also established a strong network of institutions to manage data related priorities.

Other emerging economies with large online populations that are facing similar challenges such as Indonesia have dragged their feet on data localization under pressure from certain Western countries. Many nations have been arm twisted by governments in developed nations who are

threatening to invoke specific preferential trade clauses for other goods and services if they go ahead and implement data localization regulations.

The way ahead

In addition to protecting the interests of the country and its citizens, data localization and protection offers India a chance to engage Indian companies in the endeavor. Companies that are formed here, have Indian promoters or are majorly owned by Indian companies can be relied upon to develop the expertise to establish and run large data centers in addition to protecting India's digital frontiers and infrastructure. This will lead to large scale investments in these areas as also the development of India's skill and talent pool in a critical domain.

India already has many companies that have taken the lead in various digital initiatives. Aadhar, for instance, has a basket of Indian tech companies working together to further various objectives. India is also home to many companies active in the cybersecurity space that can protect such initiatives.

India has to therefore:

- Bring out a whitepaper on digital data protection
- Shortlist and whitelist a set of Indian tech companies that can aid in establishing and protecting data centers and our digital infrastructure
- Take the lead: consult with other countries facing similar challenges to present a united front to nations and businesses that seek to curb data localization measures

- Promote and incentivize the creation of data protection zones that can house these data centers
- Keep citizens informed about the progress of these measures; engage them as stakeholders to put pressure on companies that resist data localization; the margins of many a social media giant will take an immediate hit even if our citizens stop using it for just a day
- Continue working towards evolving consensus with companies that resist data localization so that trade conflict is averted
- Cybersecurity should receive the highest priority; data can never be safe if the channels that host it or the infrastructure that enables its creation and distribution is not safe

Data localization is an opportunity and a challenge. If we rise up to the challenge the opportunity is ours to capitalize on – not just for the country and its citizens but also for generations to come.

Education & Skilling on Cyber Security must be an integral part of India's New Cyber Security Strategy

Mr Dinesh Vashishtha

Principal Consultant - Sector Skills

The Internet is becoming increasingly intertwined in the daily lives of all, particularly with the push for digital economy. The internet users base in rural India is expanding with access to mobile phones and ICT infrastructure. Simultaneously, the 4th Industrial Revolution technologies such as IoT's, Machine Learning, Artificial Intelligence, Cloud Computing provide data generation capabilities that were unimaginable ever before. With these positive developments, the incidents of data leakage, malware, phishing, ransomwares are also on the rise, several such threats being launched from international jurisdictions.

After land, air, water and space, Cyberspaceis becoming the 5th dimension for national security. To be able to prudently use these advancements in digital technology space for larger public good and nation's prosperity, cybersecurity is a priority for this decade in India. Cybersecurity is, therefore, a necessary part of the lives of individuals, organisations and nations. As such, many countries have developed and implemented cyber-security awareness and education measures to counter the perceived ignorance of Internet users, it is now India's turn to lead this sector with revolutionary cybersecurity education and skill-building.

The rationale behind pursuing cyber-security awareness and education varies from country to country. India, as a country, not only needs Cybersecurity to protect its population, like teaching youngsters to be sensitive and sensible in using social media, to IT departments of organisations, that cybersecurity engagement is necessary for the benefit of the company. The emerging cyberspace landscape necessitates incorporation of cyber security in not only the company policy and educational systems but also it is to be made part of the national cybersecurity policy to ensure that it is not missed out on by any institutions by the benefit of privilege.

Conventional classroom training is not ideal for acquiring skills and experience at a high level of competence. Instead, skills and experience are mostestablished in environments that mirror authentic scenarios where they will be applied. For a cybersecurity workforce, these environments include elements such as networks, software toolsets, and user-generated traffic. Such instruction is not optimal for rapidly modifying fields such as cybersecurity, where experts must stay abreast of the most current trends, technologies, and procedures to perform their job duties successfully. Quickly disseminating new and updated instruction courses is a task because of the additional time and costs associated with printing new material and having instructors learn it.

Thus, for proper indoctrination, an organisation must consider several factors when choosing a workforce development training program:

1. The training program needs to educate with the

knowledge that is relevant to their job duties.

2. Such a program needs to cultivate a high level of competence. This is targeted through the high development of knowledge, skills, and experience.
3. Education that utilises large portions of an individual's time hinders with their job duties and leads to lost productivity.
4. To ensure live experience. The goal is to maximise effective job performance by exposing individuals to authentic scenarios they will encounter in their jobs.

In the preceding phases, knowledge and skills are to be developed in controlled, focused environments. The objective of the skill-building phase is to develop applicable, technical skills, based on the foundational knowledge learned in the preceding phase, which will be used to perform job duties effectively.

Education on cybersecurity and even blue-collar training for the same can benefit in creating India as a leader in the sphere of cybersecurity, and further, reduce the risk of attacks by nipping it in the bud, and teaching the potential victims on how to protect themselves.

Articles Written in Absentia

India in the Era of Modern Technology

Mr Jaydeva Ranade

President, Centre for China Analysis and Strategy
Former Additional Secretary, Cabinet Secretariat (R&AW),
Government of India

The world is on the threshold of major technology advances that will translate what has so far been in the realm of science fiction to everyday reality. There is clear promise of transformational changes, with the next couple of decades being witness to technology driving almost every aspect of life.

1. Signs of this are already visible in robotics; artificial intelligence; telecommunications; Internet of Things; unmanned automobiles; biomedicine; etc. In the race not to be left behind in a world of advanced technologies, the US, Russia, some European countries and China have been working on different aspects of these technologies for a while. Taiwan, South Korea and Vietnam too are readying to compete globally in 5G communications. India needs to decide now whether it will be a leader or become a 'follower' -- the latter will mean we become susceptible to outside pressures and subservient to foreign powers. To aspire for a leadership role-- or even rank among the technologically advanced nations -- India needs to at

once take bold steps to encourage private technology small and big entrepreneurs. It needs to design policies to attract foreign technology companies to invest and set up their production and R&D centres in India. This will help train and skill our huge reserves of manpower. India simultaneously needs to take measures to protect data of national strategic significance and that of its citizens as well as deny foreign entities access to such data.

2. A preliminary, but overdue step, is to identify and prioritise areas where we need to rapidly build adequate capability. By harnessing available talent in our universities, private tech sector and from among our technology entrepreneurs, it will be possible to achieve this in a time-bound time-frame. India needs to craft programmes that fuse capabilities in all sectors so that research and its results whether in universities, hi-tech companies or industry and government can be pooled and optimised. The primary objectives should be to safeguard and secure India's critical cyber infrastructure -- which till today remains vulnerable -- and design and manufacture critical hardware components like routers, hi-tech chips etc. Here India can use the existing facilities which a few indigenous companies possess. India needs to encourage new and established companies to compete and grow globally while building a range of capabilities.
3. Data centres is one basic building block. Developing and producing hi-tech chips, routers etc are the other.

One ready example of how countries have begun the journey from ground zero is that of China -- it made huge capital investments in telecommunications technology, Artificial Intelligence (AI) etc., and its telecommunications companies like Huawei and ZTE are today rolling out fifth generation (5G) networks across the world – Huawei is present in fifty countries! ISRO is a standing example of what India can achieve!

4. The advent of Artificial Intelligence (AI) and its manifold applications accentuates the importance of data and securing that data more important. Technology-based public services usually have hidden, or invisible, data processing features and usually store client data in data centres normally in the country of their origin. This gives ready access to all stored data by other agencies either legally or through informal arrangements. Storage on Cloud, where only 3-4 companies of 2-3 countries have storage capacity, is equally risky. Important data includes economic data, stock exchange records, citizens data etc. With the development of AI and its predictive capabilities, the damage that can be done by access to such masses of data is immense. India has lagged in this area and needs to finalise a policy whereby it has full sovereignty over 'national' data including of its citizens.
5. India needs to be cognisant that advanced technology is the future and that work to secure itself must begin now. For a start India needs to establish a group of

experts drawn from the fields of cyber, computer hardware, hi-end software designers, specialised engineers, mathematicians, coders and security experts to formulate and publicise a: (i) national cyber policy; (ii) identify areas/sectors that India must first focus on; (iii) design programmes for educating school and college students and add the subject to school and college curricula; (iv) draft policies for encouraging and incentivising a 'cyber industry' etc. This effort will need to be insulated from the regular bureaucracy and structured akin to the scientific establishments like ISRO and DRDO.

Detecting Critical Cyber threats using native Technology

Mr Raman Bansal

Sr Additional General Manager, Centre For Railway Information Systems, Ministry of Railways

Timely detection and mitigation of cyber threats is of utmost importance especially for protection of critical infrastructure and for ensuring continuity of critical services. This requires putting in place an appropriate mix of People, Processes and Technology (PPT) in the organization. Since the type and nature of threats keep changing rapidly and so do the methods for their effective mitigation, the PPT aspect of the Security Architecture should be reviewed, refreshed and augmented at regular intervals.

The currently deployed threat detection systems are largely developed in other countries. However, most of this software requires a significant deal of customization/ scripting as effective co-relation rules have to be defined to detect threats and behavioural anomalies. There is potential for imaginative development/implementation in this area for user organizations. At the same time, while some efforts for indigenous development of cyber security solutions have fructified, this area requires more impetus both at the policy implementation level as well as by consuming organizations.

Another important aspect is guarding of our critical infrastructure and citizen services at the national level. To

draw an analogy, in the realm of physical security, despite every individual taking steps to ensure her/his security, there are measures taken at the colony, district, state and the country level for ensuring security. Similarly, in the cyber security domain too, we should attempt to implement a multi-tier security fabric with all levels coordinating closely. While some efforts appear to have been made in this direction, these need to be taken further to achieve a well orchestrated and resilient cyber security system having nation-wide coverage.

Intel Gathering and Social Media based Sentiment Correlation

Mr Pavithran Rajan,

Adjunct Faculty, Cyber Security Research Center, Punjab Engineering College and Advisor, Cyber Peace Foundation.

Intelligence in the form of collecting information in the interests of national decision-making is an activity that is as old as the practice of politics itself. The practice of early intelligence collection is found in all ancient societies. Intelligence is collected by public, covert or clandestine means and became an increasingly formalised aspect of military planning increasingly institutionalised within specialist units. The basic functions of intelligence agencies are divided into three steps: data collection, analysis and counterintelligence. Covert action, the more occasional fourth function for foreign intelligence agencies, aims to influence political, military or economic situations abroad while concealing the role of the state responsible in sponsoring such activities.

New age ICT has given intelligence agencies who have invested in creating MNCs unprecedented access both to the lives of citizens living within their national jurisdiction as well as to the global population of people, organisations and businesses. At the same time, the new threat environment has prompted changes to legal frameworks granting intelligence agencies increased powers of access and scope for action, sometimes with less oversight. The post-

Cold War era has seen these threats change as increased contact and cooperation among states and societies has blurred traditional distinctions between external and internal threats, and between state and non-state actors. The resulting changes include the development of international intelligence cooperation on a global scale.

The Snowden revelations of 2013 revealed an alarming picture, wherein Western nations under the leadership of the US had weaponised COTS IT products in partnership with iconic global brands under secret laws with built-in gag orders. Moreover, these revelations proved the extent to which there exists an international intelligence community, which, through its international cooperation networks, can escape both control and oversight. This lack of oversight erodes the national supervision of intelligence and can undermine democratic functioning. There are caste groups within these Intelligence agencies with some more equal than the rest. Certain Intelligence agencies have gone beyond constitutional mandates and today claim undue power through control of information. As a consequence of their role in regime maintenance, intelligence agencies frequently grow in size and power to gain high levels of political independence and control.

With these as a background, when you examine the sentiment analysis industry that has come up in India, one gets an alarming picture. In India, due to lack of strategic foresight, Western Big Tech companies and increasingly Chinese companies dominate the domestic social media market. The smartphone, IoT and the Mobile OS market that generates data from which sentiments are gleaned,

of both individuals and populations are also primarily of Western and Chinese origin. In an amazing display of strategic myopia, this vast trove of sensitive personal information of the whole citizenry goes mostly to the US and Chinese MNC farms located outside our national and legal jurisdiction. This results in a scenario wherein Indian intelligence agencies and police forces are dependent on the law enforcement apparatus and intelligence agencies of other nations to get information on matters of pressing national security matters and serious crimes.

In a domain like cyberspace, data sets can be altered, hidden or highlighted rapidly and selectively. Control of this data gives an inherent advantage to the MNC/ nation that controls the data of other countries. A continental-size country like India can ill afford to continue with this situation for two main reasons. Firstly, the strategic threat to India is the social cohesion of its varied population that can easily be manipulated by powers that control the MNCs who hold social media data. Secondly, unlike smaller countries, the rise of India will be carefully curated by other great-powers. Power finally is a zero-sum game and raising vast sections of its population economically (which today exists below the poverty line) will necessarily require a much larger GDP. Such a nation, under a single political authority, will impact the global power structures.

That these matters were allowed to fester, post the Snowden revelations when many other nations took corrective steps were primarily due to the following reasons:

Firstly, a generalist bureaucracy who are competent in

their particular specialities but have limited knowledge of matters of national security and strategic affairs has run the national security apparatus. While the political leaders have taken a back seat as they are too busy in pressing political engagements of a cacophonic democracy. This particular state of affairs has ensured that policymaking is in silos rather than in a holistic fashion keeping overall national interests in mind.

Secondly, a planned influencing of the above policymakers by people/ organisations owing allegiance to the 'Washington Consensus'. The methods used for influencing are innovative and subtle. They include but are not limited to scholarships and admissions in Ivy League universities to the children, high paid jobs to dependants and spouses, sponsored lectures on the international cocktail circuit, preferential green card/ citizenships to the children, employment opportunities for retired civil servants in foreign Think Tanks. Indian Think Tanks funded by MNCs whose members include retired civil servants and military officers who then influence their serving juniors, and a careful outreach programme to identify and curate key influencers of the nation. These loosely tied groups have then pushed globalisation policy dogmas, with limited context-setting irrespective of the government in power. Thirdly, elements of the Indian intelligence organisations and diplomats have developed cosy links with their Western counterparts who wooed them in a planned policy outreach. These individuals benefitted from the relationship; the career progression of many who rely on their personal-equations to get intelligence and diplomatic work done has blossomed. These people have

developed a vested interest in ensuring the continuation of the status quo as any disruption will affect the 'cosy' relations and their career interests.

In this backdrop, Western MNC attempts to market sentiment analytics platforms to our law enforcement and intelligence agencies is fraught with danger. This is to ensure the continuation of status-quo as they today control most of Indian social media and fear policy changes that can constrain their business. Fostering a sentiment analytics industry not only helps to monetise the data under their control but also gets the Indian agencies and the local industry more dependent and develop a vested interest to ensure their continuity. These expose the security agencies to the danger of curated information and also gives the MNCs and the security agencies of the parent nation an overview of Indian agency interests and an ability to blackmail security personnel by selective leaks about privacy violations about political intelligence gathering as can be discerned in the WhatsApp - Pegasus scandal.

The present situation has to change by bringing in legislation and localising the data. The violation of these laws should have not only financial penalties but also jail terms for corporate executives who are willfully violating the law. The data centres holding these data not only need to be controlled by Indigenous appliances but also have to have their logs to be collated in a central repository as part of the CII audit. India also needs to create a framework wherein Indian companies can create innovative social media platforms that are promoted right from primary schools. Today our education system encourages usage of Western social

media and platforms this needs to change. In conclusion, social media sentiment analytics for Intelligence gathering is an invaluable tool, but the present circumstances of their ownership and control require change. Not doing this will be complacent, and the disadvantages of the status quo vastly outweigh the advantages.

Intel Gathering and Social Media based Sentiment Correlation

Major General Neeraj Bali (Retd)
Founder CEO, LeadScape Advisors

It is hard to conceive today that the two main social media platforms that reflect the mood and sentiment of large swathes of the populace the world over are only a decade and a half old. Facebook was unveiled only for the alumni of Harvard in 2004 and made available to all in 2006. It now has 2.45 billion monthly users, a population larger than most countries. Twitter, the microblogging site that has made authorship and publishing accessible to anyone with a keyboard also came into being in the same year and now has 321 million active users. And these are only two of the many social media sites that are in currency today.

The humongous volume of the expression of joy and angst, likes and dislikes, views, opinions and preferences that is injected by these platforms into our lives are simultaneously exciting marketing specialists, making politicians wary and, above all, giving security apparatus anxiety, challenge and fresh opportunities. This new wave of collective expression has given rise to an entire industry aimed at sentiment monitoring and analysis. Though in a nascent stage, government agencies, especially in the developed world have joined this enterprise.

Thus, sentiment analysis is at the forefront of informing

public preferences and interests. It is used as a monitoring tool for social media content and can obviate an outburst or wrong decision making, as well as being blind-sided from a security standpoint.

Sentiment Correlation – Monitoring vs Analysis

There are no mid or large-sized companies that do not elicit social media reports. But reporting is only the first baby-step. The actionable 'intelligence' can only be derived with a deeper dive and analysing the sentiment emanating from the relevant social media. An example of social media monitoring would be to collect data and chart the troughs and crests of consumer reaction to a product, say a newly launched line of fashion accessories. This in itself is valuable but does not answer that one critical question that leads to valuable conclusions – "so what?" If, however, that data is studied closely and correlations drawn up between the trends and chronology, events, advertising etc, the company can understand the sentiment far more effectively.

The application for security purposes runs a similar course. Volumes of data, when simply bucketed or plotted, can give the government an inkling to the prevailing sentiment among the target population – say, response to an emotive religious issue or dissatisfaction with law and order situation. But by analysing this data, a more intimate correlation between the sentiment and actionable intelligence can be forged.

The Techniques for Sentiment Analysis

Several techniques are adopted for such an analysis. These use tools that can essentially be classified into two – search engines and web crawlers. Unlike the ubiquitous Google

search, these search engines are more niche and focused.

At the bottom of the food chain is the **Semantic Engine,** a tool aimed at in-depth analysis of the tone and tenor on the Social Media. This engine not only looks at the negative and positive words but establishes sentiment by examining related sentences throughout the text.

The **Machine Translation engine** plays an invaluable role as social media platforms allow and even encourage posting in multiple languages. This can easily be seen in the tweets posted on Twitter and even on Facebook. The automatic translation provided by this engine can then be easily analysed for establishing the prevailing sentiment.

Even more sophisticated is the **Geo-referentiation Engine**. This engine aims at searching for information on a geographic map. For example, security agencies, using a geographical interactive map, that is based the locations mentioned in a news article or post can understand how news and comments spread in a large country like India or the US. The resultant study of collective sentiment can lead to accurate perceptions about the original source of the information (or even 'fake news') and to conclude if a foreign or domestic entity is waging a deliberate and coordinated press campaign.

The Crawler or Web Crawler (sometimes referred to as 'spider') is a bot that downloads and indexes content from all over the Internet. The goal of such a bot is to learn from wide swathes of sites and create a virtual library so that the information can be retrieved when it's needed. These bots are almost always operated by search engines. A web crawler

bot has been described as "someone who goes through all the books in a disorganized library and puts together a card catalogue so that anyone who visits the library can quickly and easily find the information they need." It is obvious that the utility of such accessible information would be invaluable for security-related analysis.

While these and other search tools and techniques are invaluable, their efficacy has been enhanced manifold with the application of **Artificial Intelligence** (AI) and **Machine Learning** (ML). AI assists the process of sentiment analysis by handling large amounts of unwieldy data and then arrives not merely at analysis but proffers options for action. ML makes this process even smarter as machine continually go on refining their search and analysis ability, based on cumulative experience.

A Customised Approach

While the overall techniques and tools for establishing social media sentiment correlation are the same, the approach for each of the platforms needs to be customised for optimum results. Let us examine the four most popular sites, Facebook, Twitter, Instagram and YouTube.

Facebook is often considered as the perfect place to build and maintain a brand, and foster brand loyalty. It has been called "the starter kit for a brand's social media presence". It offers unlimited space to post text, pictures and videos and has its own messaging channel. It thus requires a deeper analysis to determine the prevailing sentiment. Also, since it transcends boundaries, it has an international character where people and groups from different parts of the world

can interact and collaborate. Facebook also has its own analytics platform that offers a multitude of insights into customer behaviour.

Twitter, the micro-blogging site that began offering space of 140-character tweets and has now doubled that quota, is the second natural home for sentiment analysts. From the analysis point of view, the strength of this platform lies in the immediacy with which the sentiment spreads through it. Relatively speaking, it works in geographical silos and its hashtag protocol often makes the initial data mining easy. Analyzing Twitter data has been described as "like having a finger on the pulse of your audience, as well as the larger conversation surrounding your brand."

Instagram, the digital picture and video site has, of late, captured the imagination of millennials and the post-millennial generation. It provides a visual representation of moods, reactions, responses and sentiment. With over 800 million monthly users, Instagram has arrived on the scene as a major source for sentiment analysis.

YouTube's popularity and potential as a source for sentiment analysis can be gauged from the statistic that over 300 hours of video are uploaded to YouTube every minute. With over a billion users and a myriad of advertising options, it is a powerful visual medium. The frequency with which a video is seen, the number of unique viewers that see it fro end to end and the geographical location of those who view the videos can offer many insights to the practitioner.

The conclusion from the above birds-eye-view is clear – those who are mining data from social media and are

mandated with sentiment analysis cannot adopt the one-technique-fits-all approach to such an analysis. This requires sophistication, persistence and, above all, customisation of the approach.

The Future is Here

Sentiment analysis is already happening, all over the world, using advanced AI techniques. It has recently been argued by the Forbes magazine though that its full potential remains to be seen. Forbes goes on to conclude "As with any new technology, the value is not in the information you mine, it's in what you do with it. The power of AI isn't in replacing our need to understand our customers, it's in using tools to understand them better and then act on those understandings, for the better."

Does this field of work require regulation? While on the face of it, that does not appear to make sense, but it is obvious that if the prevailing sentiment is used to negative ends, it can have disastrous security implications. If an anti-government entity arrives at the conclusion that the resentment in a part of the country or among a community is simmering, it can fan further fires by targeting that area or community with slanted or completely fake news. This scenario is not far-fetched. As with any technology, therefore, while security agencies must develop the highest competence to use every nuance on offer, it must also keep a watchful eye on misuse of analysis relating to sentiment by those who might stand to gain by fomenting trouble.

(The author is a retired Major General and currently Senior Advisor to Nfilade Security Solutions Pvt Ltd, a leading Cyber activities company.)

Cyber Warfare grips the World: Can there be Cyber Peace?

Major General Shashi Asthana (Retd)

The dimension of warfare keeps changing with technology, time and innovative minds of mankind. The conventional conflict since ages had well defined boundaries and invariably ended with some kind of peace negotiations/cease fire after the parties to the conflict exhausted themselves of fighting or one side gave up to the other one. The covert content in warfare also existed since the history of warfare as back as it can be traced, and will continue in future as well, although the modalities will change. As the conventional warfare started becoming cost prohibitive, the world shifted to cold wars with political, strategic and military posturing against adversaries, however the technological up gradation of military hardware as well as software continued. Some countries went nuclear, but the devastating effect displayed in Second World War, made it an instrument of mutually assured destruction, hence its utility got restricted to deterrence value. Amongst all the above-mentioned warfare, the possibility of peace negotiations exists. The Space warfare is a new dimension, although restricted to few powers, but formulating some rules should be possible by global bodies like UN. Innovative notorious minds started using terrorism, involving non state actors (who do not follow rule of law),

as a tool of warfare and the world continues to struggle with it to an extent that it has not been able to get consensus in defining it. The innovative technological minds saw the world overly dependent on electronic medium, information and computer/communication technology (ICT) in civil as well as military domain and came up with cyber warfare which has no boundaries, needs no declaration of war and is omni present. **The fact that cyber warfare can be combined with any/all kinds of warfare mentioned above makes it most dangerous and most easy to execute with maximum deniability.** It has players in civil as well as military domain. It is difficult to pinpoint as to who started it, as much as it is difficult to find a peaceful solution for it.

Why it is difficult to control Cyber Warfare?

The world is increasingly getting used to using cyber space in military and non-military domain and the attackers also utilize the same space. Cyberwarfare involves penetrating

computer network infrastructure of the adversary's government/business/ essential services of the target nation or population, utilizing techniques of defending and attacking information and computer networks that inhabit cyberspace through a prolonged cyber campaign and denying the opponent's ability to do the same. States and nonstate actors are carrying out increasingly sophisticated exploitations of vulnerabilities in ICT. Attribution to a specific perpetrator continues to be difficult, increasing the risk of "false flag" attacks—that is, attacks by a state, group, or individual under an assumed identity. The attacker need not be in the territory of the country/organization launching such attack; hence it enjoys the advantage of deniability.

It is a low cost option which can be used against a much stronger country. The fact that maximum cyber-attacks are being launched against countries, who are the leaders in the same technology like USA, indicates the asymmetric potential of this warfare. Global borderless connectivity, vulnerable technologies, and anonymity facilitate the spread of disruptive cyber activities that may cause considerable collateral damage, for example, by spreading malware into computer networks or digital control systems that were not the primary target of the original attack. Various UN reports highlight the specific risks stemming from the widespread use of ICTs in critical infrastructure, particularly through so-called ICT-enabled industrial control systems such as those used in nuclear power plants and essential services. Panic amongst the users of ICT is also a major side effect of such warfare. The difficulty in controlling cyber warfare is that cyber-space is, not owned by the governments and

attribution is difficult. No matter how laudable the norms to control may be, their implementation is a challenge.

The anonymity factor has contributed to increase in Cyber terrorism, which involves the use of computer network tools to shut down critical national infrastructures (such as energy, transportation, government operation of the target Government/population), recruiting, planning and executing strikes including lone wolf attacks adequately demonstrated by terror networking of ISIS. A new challenge has surfaced in the recent past with growing market of cyber security tools, which does not mind launching such attack using cover of anonymity on potential buyers to convince them to use their cyber security products. There is also a difference in perception globally with western countries batting for democratic, inclusive and transparent use of internet with full freedom and right to privacy thus increasing anonymity factor and some countries like China batting for encroachment into privacy on the excuse of cyber/national security.

WHAT HAS BEEN DONE SO FAR?

Taking note of such threats, the UN General Assembly (UNGA), in December 2018, adopted two resolutions: 73/27 on 'Developments in the Field of Information And Telecommunications in The Context of International Security'; and, 73/266 on 'Advancing Responsible State Behaviour in Cyber-space in the Context of International Security'. This was an attempt by the UNGA to address the problem of cyber-security, although the terminology used was 'Threats posed by the ICT to international security'.

UN did set up Groups of Governmental Experts (GGE) on many occasions to study the nature of threats in cyberspace and how to deal with them, which has made limited progress, although two of such groups are scheduled to submit their reports in 2020 and 2021. The inability to acknowledge cyber warfare in true sense and the fact that the non-state actors do not follow UN resolutions has affected the progress adversely at the global level, although at the national/organisational level countries/organisations are taking their own measures for enhancing cyber security, which is the defensive form of Cyber Warfare.

An analysis of earlier reports of UN on the subject reveals that fair amount of effort was made to increase transparency amongst Governments, sharing information and best practices and promoting confidence building measures. With the advancement of technology and prioritization of individual national interest over global interest, the effort neither produced any tangible results nor did it reduce the mistrust between various powers who are in strategic competition with each other. Most of the measures promoted by UN were in the cyber security/defensive domain, but nothing much has been done about the offensive content of Cyber warfare. **Today most of the countries are busy increasing their cyber warfare capabilities including offensive as well as defensive content and the force structuring pattern of every country proves this point adequately.** The other challenge is that ICT being common use facility, it is difficult to choke cyber-attacks by terrorists/ non state actors without undue restrictions on freedom of its use by innocent population. No legal framework/ UN

Convention can help in this regard as its difficult to enforce on them in the shadow of anonymity.

What More Needs to be done for peace in Cyber Warfare?

Ideally there needs to be a globally recognized legal framework amongst states to respect each other's sovereignty and independence in cyberspace. The states should comply with the prohibition on the offensive use of ICT against others, along with the principle of settling disputes by peaceful means in the same way as in the physical world. The right, specified in Article 51 of the UN Charter, to self-defense including the use of force should apply to a cyberattack as well. This expectation under the existing circumstances seems too good to be true. The danger of a cyber-attack by a non-state actor on another state being construed as a deliberate offensive action is another possibility, which prevents various states from binding themselves into a legal framework. The confidence-building measures and the exchange of information among states are essential to increasing predictability and reducing the risks of misperception and escalation through cyber threats were suggested by earlier UN reports and a number of countries went into such partnerships on bilateral, regional or multilateral basis. The aim being to increase transparency to reduce the possibility of an accidental/third party cyber-attack with potential to trigger international instability or a crisis leading to conflict.

Creating bilateral or multilateral consultative frameworks involving exchange of information regarding cybercrimes,

cyber terrorism, vulnerabilities and risks is doable, considering the magnitude of the threat. Additional organizations for sharing the best practices, regarding cybersecurity could be formed under the aegis of UN or on regional basis. These frameworks could include workshops and exercises on how to prevent and manage disruptive cybersecurity incidents. There is a need to enhancing mechanisms for law enforcement cooperation to reduce incidents that could be misunderstood as hostile state actions.

There is a need for global condemnation of state sponsored cyber-attacks or facilitation of terror network. Mechanisms need to be created for blacklisting such countries somewhat on the lines of Financial Action Task Force. There is a need to enhance technological solutions to such problems so that cybersecurity providers can stay ahead of the cyber spoilers and use advanced threat intelligence to develop effective counteractive systems. There is also a need for people to improve cyber hygiene so that they do not fall prey to cyber offenders. There is also a need for technologically empowered nations to share such technology with countries which do not possess it, because in borderless cyber space the weakness of such states can be exploited by cyber offenders to target those countries despite having best of technology.

The dangers of cyber warfare are well known to everyone, but the countries have started considering it as essential part of their comprehensive national power. The tendency to be one up in cyber warfare capability is steering the world to arm race, where the armament is in

cyber space and the targets are the users of ICT. With such tendency peace in cyber domain is nowhere in sight. To make situation worse the cyber terrorism, unethical cyber technological business is also growing to dangerous level and needs to be checked for common good. **There is a need forUN resolutions/treaties to call upon states to promote a "peaceful" ICT environment on the lines of other arms control treaties. Punitive actions against cyber terrorists** and their sponsors is inescapable and must be done before it is too late. Peace in cyber warfare is most desired, but remains a distant dream.

---

[i] *Wolter Detlov,(2013), The UN Takes a Big Step Forward on Cybersecurity, Arms Control Association, July 2013.https://www.armscontrol.org/act/2013-09/un-takes-big-step-forward-cybersecurity*

[ii] *Resolution adopted by the General Assembly, United Nations, December 05, 2018.https://undocs.org/A/RES/73/27*

[iii] *Resolution adopted by the General Assembly, United Nations, December 22, 2018.https://undocs.org/A/RES/73/266*

(The views expressed are personal views of the author, who retains the copy right). The author can be reached at Facebook, LinkedIn, and Google+ as Shashi Asthana, @asthana_shashi on twitter, and personnel sitehttps://asthanawrites.org/email shashiasthana29@gmail.com. LinkedIn Profilewww.linkedin.com/in/shashi-asthana-4b3801a6. Youtube linkhttps://www.youtube.com/channel/UCl50YRTBrOCVIxDtHfhvQDQ?view_as=subscriber

Why Critical Infrastructures are in target of cyber attackers

Mr Bharat Panchal

Chief Risk Officer- India, Middle-East & Africa, FIS global

As the digital world becomes increasingly connected, it is no longer possible for infrastructure owners and operators to remain agnostic in the face of evolving cyberthreats.. Nation's critical infrastructure is foundation for any nation to prosperous, to develop and more importantly act as a strong pillar for national security. Critical infrastructure has very vital importance to the running of the country as well as storage and transmission of the huge amounts of valuable personal data which are always on target of enemies and hackers.

CIs are our nation's backbone. Theyrefer to both physical and cyber systems vital to our nation's physical or economical security, health, and safety.

For every nation, national security and critical infrastructure sectors have become increasingly dependent on commercial information systems and technologies. These system architectures are fragile and already proven to be compromised when subjected to ever-increasingly advanced and adaptive cyber-attacks, resulting in failed, disrupted or compromised mission operations which can impact very adversely to the whole nation.

There are growing concerns and debates about the protection of these types of CI systems, especially, how to effectively protect them given their vital positions in social and economic developments. In the interconnected world, CIs are becoming more tightly coupled into a system of inter-dependent infrastructures, and converging with information and communications technology and the Internet.

Today financial sector, power and energy distribution, water dams, nuclear power plants, public utilities, trains, airports, defense and research establishment etc are always under the radar of cyber attackers for variety of motives. Without a strong resilient cybersecurity program, cybercriminals could completely destroy the ways in which our economies and nations operate, those that the critical infrastructure sectors have worked so hard to build the nation over decades..

National infrastructure is a prime target

Intensity and frequency of cyber-attacks continue to grow exponentially as the world becomes increasingly connected. According to Gartner, by 2020 there will be 20.4 billion internet-connected devices (IOTs), and approximately 37 percent of these will be used outside consumer settings including large numbers dedicated to infrastructure monitoring and control. While the spurt of such connected devices has created unprecedented productivity and efficiency gains, it has also exposed previously isolated or unreachable infrastructure systems to attackers due to interconnected IT world.

World has witnessed plenty of recent attacks to CIs. One

of the most famous is the WannaCry ransomware crypto-worm – a virus encrypting data and demanding money to re-access it – which, in May 2017, infected more than 2,00,000 computers over 150 countries. The National Health Services in England and Scotland, with over one third of the trusts being disrupted, was one of the largest organizations hit by the attack, together with the German national railway operator Deutsche Bahn and Spanish telecommunications company Telefonica.

After just a couple of weeks, the Petya ransomware spread globally, causing tremendous disruptions to big firms in the US and Europe (including food company Mondelez and shipping giant Maersk) and to dozens of key organizations in Ukraine (among those, state power plants, banks, airports and metro). India's most busiest port JNPT was forced to shut down one of the terminal which is managed by Maersk due to their systems got compromised which are located in Copenhagen.

Financial institutions are comparatively having stringent privacy and security protocols, aren't completely safe. One of the biggest breach in 2017 of Equifax saw hackers steal the personal data – including credit card details and social security numbers – of 143 million US citizens when they took advantage of a security vulnerability in the open source framework Apache Struts, which formed part of Equifax's IT infrastructure. This vulnerability had been discovered two months previously but Equifax had not installed the required patch that had been issued to close this vulnerability. Equifax is paying the price now

for its negligence, racking up a recent $700m fine from the Federal Trade Commission. In India, Hitachi payment services was impacted due to malware attack in May 2016 which resulted in 3.2 Million debit cards compromised. Customers of many banks lost more than 15 crores rupees in this attack. In August 2018, Cosmos Bank, Pune was attacked by cyber criminals and bank lost Rs. 94 Crores.

On 4th September, 2019, Kudankulam Nuclear Power Plant, one of the county's most advanced such station in India was under cyber-attack. Though it was contained immediately and no damage was cause, there were every change of massive damage had the attack got unnoticed.

Cyber Resilience for Critical Infrastructure

While continuous efforts are put into rigorous risk assessment and planning for mitigating any number of risks to an infrastructure asset, it is still not possible to envisage every potential cybersecurity incident accurately. There are many reasons for the lack of attention to cybersecurity.

Looking at the intensity of cyber-attacks on critical infrastructure and damage it can caused to the nation, it is now almost compulsory to continuously raise the bar to protect mission critical systems from these threats by implementing best security practices, best of the technology and highly skilled manpower. It may very pertinent to note that the current philosophy of restrain the adversaries out, or the assumption that they will be detected if they get through the first line of defence, is no longer valid.

Critical infrastructures for general utility are always accessible to many people. For example in any public

health services, hackers have multiple entry points, from patient management systems used for admission, highly sophisticated medical devices and electronic tablets used by doctors and their staff. Usage of so many systems and applications bring many vulnerabilities or gaps together, including legacy technology.

Building cyber defense for Critical Infrastructure

To build adequate defenses, infrastructure must assume that a cyberattack is imminent, rather in true sense its inevitable now. Therefore it is must to build a unified, integrated cyber defense that best protects all relevant critical infrastructure assets. Clearly, security risks for CIs are evolving day by day along new technology pathways where IoT devices and applications are finding their ways into CI systems. As a long term strategy to protect CIs effectively from cyber attack, newer or updated CIP cyber security resilience approaches should be developed at a national level. With emergence of IoT, scope of IoT in security risk management; from identification to effectiveness evaluations needs to be well defined. This can support appropriate alignments and responsiveness to the evolving trends introduced by new technologies such as IoT. Such approaches also need to adopt dynamic and real-time assessment processes to address the issues introduced by IoT in CIs, and the high impact security risks that evolves dynamically.

Further, A strong public-private sector partnership is important and should be vigorously pursued by both stakeholder groups to achieve better security and resilience in CIs. Such collaboration can empower the public sector

to monitor, in timely and efficiently ways, and to aggregate information about CI security threats, vulnerabilities, incidents and impacts as they emerge. The public sector can also provide the risk information to private sector operators to help them ensure an informed and well organised security management.

Implications And Significance Of Privacy For Citizens

Dr Roopak Vasishtha
CEO & Director General
Apparel Made Ups & Home Furnishing Sector Skill Council

The recent Chaayos controversy amply highlights the pitfalls of unregulated data collection that businesses often resort to collect information from customers discreetly. Chaayos, a beverage retail chain, recently introduced facial recognition technology at several of its outlets and started taking images of customers without their due consent. When this matter came to light in social media, Chaayos went on the defensive, claiming the data was encrypted. It also claimed the collected data was not used for any purpose other than to "speed up orders."

THESE ARE THE QUESTIONS THAT ARISE:

- If the data was indeed collected for customer experience, why weren't customers asked to grant their due permission?
- Why didn't Chaayos educate the customers about how this data would be utilized?
- Why did Chaayos not clear about its data-gathering techniques on its website and social media platforms before launching the program?
- Why weren't customers given a choice to opt-out?

Why were their pictures taken without their consent?

- What guarantee can Chaayos give that the data will be stored in a secure manner preventing loss either due to external hacking or internal leakage?

Greed for consumer data is growing

Chaayos is not the only brand to have undergone this disastrous turn of events. There was also a significant episode involving facial recognition failure wherein Amazon's software couldn't detect dark skin types and was therefore considered racial. There have been instances where facial recognition failed ultimately in classifying transgender and non-binary people accurately. This puts into question the core ethics that inspire data harvesting.

Google-owned Gmail was caught, giving data companies and app developers access to private emails in the recent past. Google also recently admitted that its employees were listening to the data collected by the Google Home, purportedly to help improve the AI engine. As this data is collected without the user's knowledge, it raises security and surveillance concerns in addition to ethics. Criminals can potentially hack security cameras and break into homes and offices.

Businesses have been collecting data from regular customers and even others who visit their sites. When you access a website, you are visible not only by the site but also by third-party trackers embedded in the website's code. We have no clue how and where our data is used by a third-party service provider residing in another country to whom this data is given for a monetary consideration.

Data stored by mobile phone manufacturing companies change hands often. Credit card, location, purchase information and other data has been released to hackers and other parties frequently.

Back home, a case was reported from Telangana in 2015 wherein a man hacked into a school's exam results in a database that was not securely stored and began targeting mostly non-meritorious students by acting as an education consultant and asking for favors from them.

Ramifications for the citizen

A recently conducted survey revealed that as many as 60 percent of users fear unauthorized data collection, and only 11 percent of users read privacy policies. This survey was done in early 2019 by CUTS International.

How do data breaches affect ordinary citizens? Experts opine that it may impact in different ways: exposed bank account information can trigger financial fraud, mark sheets can lead to cyber-bullying, and leaked private information can form the basis for blackmail or other criminal activities. Private data made available in the open can also spark psychological problems. In addition, being the target of focused advertising can be a menace. Companies and other entities can utilize a person's data, including search history, to learn more about the person, and thereby target her with customized advertisements and other commercial offers.

The Aadhar episode

The Supreme Court recently asked the Central government to respond to a petition challenging the legal validity of amendments allowing private entities to use the Aadhaar

data furnished voluntarily by customers for identity authentication. This instance represents the voluntary use of Aadhar for services such as phone, bank account, gas connection, etc. The petitioners alleged that the act created a backdoor to permit private parties to access the Aadhaar ecosystem, thus enabling State and secret surveillance of citizens.

The petitioners are, however, silent on the involuntary, discrete, and almost creepy collection of data by private entities. In cases such as Chaayos, the companies get away with some bad short term publicity and continue figuring out and implementing ways to collect more consumer data without their consent. It is such companies that never bother to inform and seek approval from customers that should be held responsible. They should also be made to extend basic moral and ethical courtesies to all stakeholders. It is such instances that need attention.

Unless the citizen is given an assurance on privacy in transactions and customer experience, the full potential of legitimately collected data will not be realized in various contexts. In the case of breaches of illegally obtained data, the same is monetized by third parties located in countries that may even harbor adversarial intent towards our country.

Thus the significance of data cannot be overlooked in any situation.

Annexure

CYBER SECURITY AND CITIZEN 2030

SERIES OF ROUNDTABLE CONFERENCES
NOVEMBER AND DECEMBER 2019

HOSTED BY:

IMC
Chamber of Commerce and Industry

Centre for Knowledge Sovereignty

CENJOWS

Mr Vipul Srivastava (IMC Chamber of Commerce and Industry)	*Lt Gen Vinod Bhatia (CENJOWS)*	*Ms. Uma Sudhindra (CKS)*	*Lt Gen Rajesh Pant (National Cyber Security Coordinator)*	*Mr Vinit Goenka (CKS)*	*Ms Sumitra Goenka (CKS)*

Submission of Brief Recommendations and Minutes of Roundtables on CyberSecurity 2030 to National Cyber Security Coordinator (NCSC) under National Security Council Secretariat (NSCS) Lt Gen Rajesh Pant (retd) by Representatives of CKS, CENJOWS and IMC at National Security Council Secretariat (NSCS) Headquarters New Delhi.

.

Disclaimer:

The following Minutes of the meeting are recorded and presented by the representatives of the Centre for Knowledge Sovereignty. The Chatham House Rule is followed for the following report as follows:

"When a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed."

However, if one has missed out any points as mentioned in this report, please do contact us in the details mentioned at the end of the report

Preface and History of the Advent of Cyber Technology in India

India is home to 17% of the world population.The accessibility to technology in India has been increasing exponentially, noticeably so since 2014. Concerning the inclusion of technology in recent years, demographic distribution has changed.

The demography that has access to the internet is as follows

Year	Population	Percentage
2000	5,557,455	0.5 %
2004	22,259,583	2 %
2009	62,166,128	5.1 %
2014	233,152,478	18 %
2019	627,000,000	79%*

Though there are no confirmed statistics in the public domain, the estimate for mobile device penetration was said to be over 18% post-2004 and is soon to reach approximately 30% in 2019.

- India in 2020 will have:
  - » 730 Million Internet Users
  - » 75% of all new users will be from rural areas
  - » 75% of new users will use vernacular language

[1] https://www.internetlivestats.com/internet-users/india/

  - » 50% Increase in travel transactions
  - » 70% increase in online purchase transactions
- India's venture into the cyber world began in
  - » On August 15, 1995, Videsh Sanchar Nigam Limited (VSNL) launched public Internet access in India.
  - » The first mobile phone in India came along with the internet in 1995

Need for Cybersecurity

Attacks in the country in the third quarter of 2019*:

- 14000 critical attacks detected very high sophistication and persistence
- 70300 High-grade attacks in the country
- 8300 malware variants identified.
- 3507 malware samples identified
- Main cities like Bangalore, Mumbai and New Delhi are the hubs of most attacks accounting for 38% of all attacks detected.
- Malware attacks have been:
  - » 3% on military-grade;
  - » 7% on research labs;
  - » 19% mixed;
  - » 21% produced via malware forums;
  - » 37% on Dark web; and
  - » 13% unknown.

- Major sectors that are attacked are:
  - » 5% Smart home devices;
  - » 7% Defence;
  - » 8% Smart cities;
  - » 10% Banking and Finance; and
  - » 11% Mixed.

Types of attacks:

According to a compilation of research from multiple Indian sources (Ranging from para-government like NitiAayog, to private organizations),one knows the types of attacks vary in the following ratio.

- 4% Simple reconnaissance
- 7% Privilege Abuse
- 10% Port Access Scan/ TCP Dump
- 11% Brute Force attacks
- 15% DoS and Variants
- 16% Firmware downgrade attempts (corrosion)
- 17% Integrity violation with malicious code injection
- 20% Persistent reconnaissance

*Source: Subex Ltd. State of IoT Security Report India (Jul-Sept 2019)

Cyber Attacks of note in India

2016 July – Union Bank of India Heist - Through a phishing email sent to an employee, hackers accessed the credentials to execute a fund transfer, swindling Union Bank of India of $171 million, Prompt action helped the bank recover almost the entire money

2017 May – Wannacry Ransomware - The global ransomware attack took its toll in India with several thousands of computers getting locked down by ransom-seeking hackers. The attack also impacted systems belonging to the Andhra Pradesh police and state utilities of Onest Bengal

2**017 May – Data Theft at Zomato-** The food tech company discovered that an 'ethical' hacker-who stole data, including names, email IDs and hashed passwords, of 17 million users demanded the company must acknowledge its security vulnerabilities-and put up for sale on the Dark Web

2017 June – Petya Ransomware- The ransomware attack made its impact felt across the world, including India, where container handling functions at a terminal operated by the Danish firm AP Moller-Maersk at Mumbai's Jawaharlal Nehru Port Trust got affected

The Need for Cybersecurity

For the first time in history, the majority of the population hold devices that are susceptible to attacks to an extend that allow it to become a weapon against its owner.

It is the era of Non- Kinetic Warfare, where the users are the most vulnerable to any strategic attack and must, thus, be protected through national strategies, policies, and frameworks.

Data is core to the use of any device, and the insurance that data is protected. The roundtable conferences must thus revolve around data protection, the importance of data sovereignty, a national policy and a core representation in the government.

List of Events Held under Cybersecurity Citizen

2030 Roundtables of 2019

Date	Topic
18-Nov-2019	Empowering Agencies with Comprehensive Data Gathering Technology Platform
26-Nov-2019	Intel Gathering and Social Media Based Sentiment Correlation
01-Dec-2019	Detecting Critical Cyber Threats using Native Technology
05-Dec-2019	Cyber Resilience for Critical Infrastructure

Delegates / Attendees of the Roundtables

(Not necessarily in a specific order)

- Hon'ble Member of Parliament, Lok Sabha,Shri Anantkumar Hegde, Former Union Minister of State for Skill Development and Entrepreneurship and currently on Standing Committee on Science & Technology, Environment & Forests of Parliament
- Dr S D Pradhan, Former Deputy National Security Advisor and Chairman, Joint Intelligence Committee, National Security Council Secretariat
- Lieutenant General Rajesh Pant, (Retd) Chief of National Cyber Coordination Centre (NCCC)
- Lieutenant General Vinod Bhatia,(Retd) PVSM,AVSM, SM Former Director General Military Operations, Currently Director Center for Joint Warfare Studies
- Lieutenant General Girish Kumar, VSM, Surveyor General of India
- Lieutenant General Dattatrey Shekatkar(Retd), PVSM,AVSM, VSM, Former Director General Military Operations, Currently Chancellor of Sikkim University, Chairman Centre for Knowledge Sovereignty
- Lieutenant General Venkatesh Patil(Retd) AVSM, PVSM, Former Director General Military Operations, Currently Vice Chairman Centre for Knowledge Sovereignty

- Lieutenant General Ajay Chandele(Retd) ,PVSM, AVSM , National Geospatial Think Tank Member
- Air Vice-Marshall Pranay Sinha, VSM (Retd) Advisor, Central Research Laboratory - Bharat Electronics Limited
- Mr Vinit Goenka, Secretary Centre for Knowledge Sovereignty, Governing council member Centre For Railway Information Systems, Ministry of Railways&Former Taskforce Member Ministries of Road, Transport, Highway & Shipping& Former Co-Convener National IT Cell, BJP.
- Major General Dhruv Katoch(Retd), SM, VSM, Former Director Centre for Land Warfare Studies
- Mr Amit Sharma, Additional Director in the Office of the Scientific Advisor of Defence Minister, Defence Research and Development Organization (D.R.D.O), Ministry of Defence
- IG Bhola Nath Sharma (Retd), Former Inspector General Border Security Force
- IPS, 1994 Brijesh Singh, Inspector General of Police, Cyber at Government of Maharashtra
- IPS, 1996 Ajay Yadav Inspector General, Communications and IT, Central Reserve Police Force
- IPS, 2005 Amresh Mishra Superintendent of Police, National Investigation Agency (NIA)
- Brigadier Manjeet Singh, PDS Cyber NSCS
- Brigadier Navdeep Brar, DDG RTG(UP & UK)

Indian Army

- Brigadier Pradeep Arora(Retd), Former Chairman Cyber Security Group DDP, DRDO
- Brigadier Rajeev Bhutani,CENJOWS
- Commander PrakashL R (Retd), Senior Director-Centre for Development of Advanced Computing
- Group Captain Guruhari, IAF (after Infowar)
- Colonel Aman Anand, Spokesperson, Ministry of Defence
- Lieutenant Colonel,Jigyasu Bagai Defence Intelligence Agency (DIA), JIG Indian Army
- Lieutenant Colonel,Jaimandeep Singh, Defence Intelligence Agency
- Mr R Chandrashekhar, Senior Fellow, CENJOWS
- Dr Vipin Tyagi, Director General, Centre for Development of Telematics, CDot
- Dr Haresh Bhatt, Chairman, Information and Cyber Security Board & Mission Director, Information and Cyber Security, Space Applications Centre, ISRO.
- Dr K J Ramesh, Former Director General, India Meteorological Department, National Geospatial Think Tank Member
- IAS, 1996 Navin Mittal, Commissioner, Collegiate Education & Technical Education, Government of Telangana
- Dr Sunil Gupta, Economic Research Unit, Joint Plant Committee, Ministry of Steel

- Shri Mukesh Nigam Managing Director, Centre For Railway Information Systems, Ministry of Railway
- Dr Sanjaya Das, Former Managing Director, Centre For Railway Information Systems, Ministry of Railway, Government of India.
- Mrs Vandana Nanda, Former Managing Director, Centre For Railway Information Systems, Ministry of Railway,Government of India.
- Mr VijayDebnath, General Manager (Infrastructure & Security), Chief Information Security Officer - Centre For Railway Information Systems,Government of India.
- Mr Ashutosh Vasant, Director (Project Operation and Maintenance) of RailTel,Government of India.
- Shri A K Agarwal, Chief Administrative Officer, Central Organization for Modernization of Workshops, COFMOW,Ministry of Railway,Government of India.
- Dr Unnat Pandit, Programme Director, Atal Innovation Mission, Niti Ayog
- ITS Shubha Bhambhani, Principal General Manager (C&M) at Bharat Sanchar Nigam Limited
- Dr JanmejayThakur Scientist, Intellectual Property and Know-How Informatics, National Informatics Centre
- Dr Rita Srivastava Sr DGM, Cyber Security- Bharat Electronics Limited

- Dr Hemavathy Muthusamy, Sr DGM, Network & Cyber Security, Central Research Laboratory-BG
- Dr Santulan Chaubey, Department of Information Technology, Government of Delhi.
- Mr K K Minocha, Former Deputy Director-General Broadband USOF at Department of Telecommunications (DOT)
- Mrs Veni Thapar, Sr Partner, V K Thapar & Co.
- Mr Shivkumar Pandey, Group Chief Information Security Officer, Bombay Stock Exchange Ltd
- Mr Shankar Jadhav, Managing Director, BSE Investments Ltd, Head Strategy BSE (Bombay Stock Exchange)
- Dr DeepaPrakash, Food Scientist, Formerly with Council for Scientific Industrial Research, Central Food Technological Research Institute
- MrVijay Karia, Managing Director, Ravin Group
- MrVinod Kumar, Managing Director, Subex
- Mr Ajit Mangrulkar, Director General, IMC Chamber of Commerce and Industry .
- Mr Vipul Srivastava, Director, IMC Chamber of Commerce and Industry.
- Mr Ashok Narayanaswamy, Partner, Price Waterhouse Coopers
- Mrs LakshmiMadhusudan, Head of Talent Acquisition, Guardian Life
- Mrs Sumitra Goenka, Managing Director, Ratein

- MrRajat Dhar, Managing Partner FINOGENT
- MrRishabh Gulati, Managing Editor, NewsX
- Mrs Uma Sudhindra Member- Board of Governors, Indian Institute of Management - Vizag
- Dr SanjaySharma, Dean -School of ICT, Gautam Buddha University
- Dr Faruk Kazi, Dean- Research, Development and Consultancy at Veermata Jijabai Technological Institute, Core Advisory Committee Directorate of Technical Education, Maharashtra State
- Dr Vijay Kumar Kaul, Professor, Department of Business Economics, Delhi University
- Dr Munesh Trivedi, Professor, Department of CSE, National Institute of Technology
- Dr PradeepTomar, Professor, School of Information & Communication Technology, Gautam Buddha University
- Dr SandhyaTarar, Professor, School of Information & Communication Technology, Gautam Buddha University
- Dr DeepakUpadhyay. Professor, Cyber Expert, Gujarat Technological University
- Dr Aroon Sharma Professor, Rural Development, Industrial Eco./Econometrics. Jammu University
- MrKartikVaidyanathan, MD Apco Digicon
- MrAjay Kashikar, Consultant, E-zest Solutions Ltd.
- Dr DeepakDeshpande, Chief Human Resource

Officer- Netmagicsolutions

- MrRahul Seth – Head Government Public Policy and Government partnerships, ValuePitch ETechnologies Pvt Ltd.
- Mr RajkumarMohanraj, Director, IT, Apco Digicon
- Mr Alok Oak, Deputy General Manager, Godrej and Boyce Mfg
- Mrs Vaishali Patil, Director Study Circle.
- Shri Anand Patil,CMD Study Circle & IIFW
- Ms Ihita Gangavarapau, Co-founder of Internet Governance Forum India
- Mr Dinesh Vashishtha, Principal Consultant - Sector Skills

List of Authors for Compendium

Across the four roundtable conferences, theOrganising committees were able to assemble a veritable cast of decision-makers, functionaries, dignitaries and lawmakers drawn from the armed forces, intelligence, media, advocacy groups, public sector undertakings, industry, private sectors, industry bodies, financial institutions and academia.

Through focused and in-depth discussions, these experts were able to chart a course to navigate India and our digital dreams to a secure future. We were also able to set a roadmap and agenda for Cybersecurity 2030 and data protection for the country.

We had also requested all our invitees to submit articles for publication in a compendium. The list of authors is as follows:

- Hon'ble MP of LokSabha Shri Anantkumar Hegde, Former Union Minister of State for Skill Development and Entrepreneurship, Currently on Standing Committee on Science & Technology, Environment & Forests of Parliament
- Dr S D Pradhan, Former Deputy National Security Advisor and Chairman, Joint Intelligence Committee, National Security Council Secretariat
- Lieutenant General Vinod Bhatia (Retd),PVSM, AVSM, SM , Former Director General Military Operations, Currently Director Center for Joint

Warfare Studies

- Lieutenant General Dattatrey Shekatkar (Retd),PVSM, AVSM, VSM , Former Director General Military Operations, Currently Chancellor of Sikkim University, Chairman Centre for Knowledge Sovereignty
- Lieutenant General Venkatesh Patil (Retd),AVSM, PVSM , Former Director General Military Operations, Currently Vice Chairman Centre for Knowledge Sovereignty
- Air Vice-Marshal Pranay Sinha VSM (Retd) Advisor, Central Research Laboratory - Bharat Electronics Limited
- Shri Vinit Goenka, Secretary Centre for Knowledge Sovereignty, Governing council member Centre For Railway Information Systems, Ministry of Railways, Former Taskforce Member Ministries of Road, Transport, Highway & Shipping
- Shri Bhola Nath Sharma (Retd), Former Inspector General Border Security Force
- IPS, 1996 Ajay Yadav ,Inspector General, Communications and IT, Central Reserve Police Force
- Brigadier Navdeep Brar, DDG RTG(UP & UK) Indian Army
- Brigadier Pradeep Arora ,Former Chairman Cyber Security Group DDP, DRDO
- Brigadier Rajeev Bhutani ,CENJOWS

- Lieutenant Colonel Jaimandeep Singh, Defence Intelligence Agency
- Dr Vipin Tyagi , Director General Centre for Development of Telematics
- Dr K J Ramesh Former ,Director General, India Meteorological Department, National Geospatial Think Tank Member
- Mr. Mukesh Nigam , Managing Director Centre For Railway Information Systems, Ministry of Railway
- Mr Ashutosh Vasant, Director (Project Operation and Maintenance) of RailTel
- Dr Unnat Pandit, Programme Director, Atal Innovation Mission, Niti Ayog
- ITS Shubha Bhambhani, Principal General Manager (C&M) at Bharat Sanchar Nigam Limited
- Dr Rita Srivastava Sr DGM, Cyber Security- Bharat Electronics Limited
- Mr K K Minocha, Deputy Director-General Broadband USOF at Department of Telecommunications (DOT)
- Mr Shivkumar Pandey Group Chief Information Security Officer, Bombay Stock Exchange Ltd
- Mr Shankar Jadhav, Managing Director, BSE Investments Ltd, Head Strategy BSE (Bombay Stock Exchange)
- Dr Deepa Prakash , Food Scientist, Council for Scientific Industrial Research, Central Food Technological Research Institute
- Mr. Ajit Mangrulkar Director General, Indian

Merchants' Chamber

- Mrs Sumitra Goenka, Managing Director, Ratein
- Mrs Uma Sudhindra Member- Board of Governors, Indian Insititute of Management - Vizag
- Mr Padmanabhan Vinod Kumar, CEO and MD, Subex Ltd.
- Dr Sanjay Sharma Dean -School of ICT, Gautam Buddha University
- Dr Faruk Kazi, Dean- Research, Development and Consultancy at Veermata Jijabai Technological Institute, Core Advisory Committee Directorate of Technical Education, Maharashtra State
- Dr Vijay Kumar Kaul, Professor, Department of Business Economics, Delhi University
- Dr Munesh Chandra Trivedi Professor, Department of CSE, National Institute of Technology
- Dr Sandhya Tarar, Professor, School of Information & Communication Technology, Gautam Buddha University
- Mr Kartik Vaidyanathan , Apco Digicon
- Ms Ihita Gangavarapau Co-founder of Youth Internet Governance Forum India
- Mr Ajay Kashikar, Consultant, E-zest
- Mr Rajkumar Mohanraj , Director, IT, Apco Digicon
- Mrs Vaishali Patil,Director Study Circle
- Ms Shravishtha Ajaykumar, Associate Director - Centre for Knowledge Sovereignty
- Mr Raman Bansal, Sr Additional General Manager,

Centre For Railway Information Systems, Ministry of Railways

- Mr Pavitran Rajan - Defence Analyst and Cyber expert.
- Major General Neeraj Bali (Retd) Head of Corporate Affairs at Rodic Consultants
- Major General Shashi Asthana (Retd)

Minutes of the Meeting

Roundtable: 1/4

Topic: Empowering Agencies and Comprehensive Data Gathering And Technology Platforms

Venue: Constitution Club of India, Sansad Marg, New Delhi

Date: 18th November 1000hrs

Key points of discussion

- Armed forces have always been preparing anticipatory threat analysis (predictable threat analysis). If we fail in prediction,then we must be prepared for the consequences. The new threat is developing around the world. **Data is energy. Data is power.** In the 21st century, knowledge is power, and we need to ensure the use of data to do something good.
- **Perception management** is also an industry – international diplomacy as an exercise is also about perception management. Today is the era of rogue nations who are more dangerous than the nations having nuclear bombs. Because nuclear bombs can be seen, but cyber threats cannot be seen. They don't want you to progress the way you want you to.
- **Social media has become an active conduit to pass on fake news.** This has led to the creation of news out of nothing. A well-spoken lie spoken through a credible source can attain a life of its own. Our intelligence system is being impacted. Our adversaries are using young minds against our own

country.

- Someone can use the data against us. Data will represent the convergence of thoughts and ideas. Let everyone be connected and be prosperous. To protect your national interest, you need a hard shield which is the armed forces.
- Nations go to war because you want to impose your will on others. Now you don't need to go anywhere; are we going to be subservient to people who own our data? We want to change Pakistan's behaviour. Are there other means to do it? Are we looking at offensive deterrence?
- Image of a new India as a modern and secure society. There are almost 5000 data points for every citizen on social media. India is a resurgent and responsible power. We have the brains, but do we have the structure**? Data is on the central, state or concurrent list what the status of data is? Who is going to handle digital India?** Constitutionally it must be given to someone either centre or state.
- **Battling an invisible enemy:** AI has complicated the system and our ability to detect threats
- Make in India dream. We should become self-reliant; why don't we have an "Indypedia" on the lines of Wikipedia?
- When IC 814 was hijacked, we couldn't do much today; retribution is swift and violent as demonstrated by Uri and Pulwama. We need to invest in developing pre-emptive intelligence at all levels. We have the

people and the knowledge to make it happen

- **Data is a raw uncut diamond.** Plenty of data is being generated so this must be managed via a data centre that should be under the government – named central data warehouse which is in turn supported by regional data warehouses empowered to gather and collect data. Here the data needs to be gathered in a format to reduce latency (EDGE) and cloud for central warehouse we can have in-memory computing.
- Even if data is available, the user could be another entity. But veracity and validation by a government agency is the need of the hour with regional data marts giving data to various agencies including armed forces and business houses and educational institutions. Now data can be sold and bought provided they are made available and verified.
- **A national analytical agency or a laboratory** is needed to manage this common data and gather insights. Data in the hands of non-native agencies has led to other business entities gathering data in an unauthorized manner while gaining influence. Data of Indians should be analyzed and put in the public domain. Many firms are taking up this data like pharma, agriculture etc. And this data can be used for many purposes as per various use cases.
- **There is a jump in cyberattacks to 26 per cent**.We roughly have 10-12 billion devices globally. These devices are connected to the Internet. We are still not very secure as far as the transport and communication

layer of data is concerned. The solution can be to have a proper cybersecurity framework and the transfer and management protocols to be secure. Empanelled data service providers are undergoing a major overhaul; everyone is working together to retain data in India. But gathering analysis and keeping safe as far as data is concerned is essential (whether inside or outside).

- We need to create a platform for the collection of data (primary, secondary or tertiary) to assess its veracity and security before it is put into the platform. This is where a lot of effort and knowledge tools are required. Data authentication needs more effort, and that is not the case so far. In this GPS era, all data should have a knowledge attribute that feeds into its authenticity. **Once data becomes available, there should be a way of segregating whether it is for civilian or strategic use.**
- We have to ponder if **data be used for the future strategic application, and** that goal should be at the core of this activity so that our national data is not vulnerable.**Needs assessment survey** should be done, anddata capturing should be made on this premise from time to time across sectors. We need to have a **digital information analysis platform** – for example, in the healthcare sector, incidents of communicable devices are not available at a national level, and practitioners are not connected. So we don't know the scale of action required.
- There will be 30-40 indicators for sectors, and then

there are other sub-sectors, and we need to **look at and adopt international best practices** at the earliest possible instance. With the existing tools, we need to have the wherewithal to use that data to risk proof the data once it becomes available (they must be identified and implemented).

- This is the era of sensors (multilayered information will be there). We need to put algorithms and to filter data, and pre-processing happens before data goes into the cloud. We should use a **national knowledge network (NKN)** with controls in place in terms of who is using it and give privilege based access. It can have an international link as well. Best use of this would be in offering weather information being shared for weather prediction using the high bandwidth available. **We must have live access data servers which do analytics and issues of concern should come on an immediate basis based on differential access**.
- **Between 2017 and 2018, 600 bn dollars were spent to protect organizations from cyberattacks.** That is a considerable amount.
- **Cyberattacks are linked heavily to intelligence activities.** All kinds of intelligence activities across data centres and telecom for instances. Misinformation is fueled through these cyberattacks.
- In the startup ecosystem, every company roughly less than 5 years old spends almost 10 per cent of its revenue on protecting from cyberattacks. Imagine

how much they are spending. They are barely surviving. And they are spending so much of their money. So, what is important is to enhance the cyber intelligence capacities pull our actionable insights from the data we gather.

- We still work in silos, and we don't work in collaboration. **21 agencies under 11 ministries work on cyber and data in India. The left-hand doesn't know what the right hand is doing.** We have a common objective which is to protect data. Coordination is needed at the highest level, to get real-time information. A massive attack can happen if there is a lack of coordination between Ministries and Agencies.The extremist groups are using the episodes to spread fake news and misinformation. This should be dealt with a high degree of automation and a shared umbrella under which these agencies can function.
- Railway data protection and sharing are essential. Data should not go anywhere in an unauthorized manner as it could be hacked. A lot of customer data is there, which needs to be protected.
- **There is a platform being built by law enforcement agencies. (NATGRID)**. The queries coming from national agencies are very specific related to specific people who can behave in any way. The data alone cannot help. They need some domain expertise as well that will come from the transport operator to make sense out of that data. Transport Service

providers like Railways need legal protection as well who is asking is not known and for what reason. There may be rivals who would want to use this data for commercial purposes. Authentication of the law enforcement agency is critical and needs to be guarded against privacy lawsuits as the customer may not want it that way, and many times, in the long run, this can prove detrimental to the provider who shares confidential data.

- Another threat we face daily is people (**employee or contractors**) and their intentions. Controlling the motivations of employees is a tough proposition, and there are various motivations, grudges and harassment levels at play. Due diligence needs to be exercised at the law enforcement level so that the employees don't stop sharing data out of fear.
- **National critical infrastructure is a perennial target.** We require common minimum national standards on cybersecurity and then sector-wise standards as well.
- Another aspect is **intra-agency collaboration** which needs to be enhanced. Data should be retained within the country with an SLA for action in case of a cyberattack. How quick you can get the data informs how quickly you can capture the crook, so need to work towards cyber resilience.
- Dealing with **deep fakes** is an ongoing challenge. Detection is the biggest challenge.
- Data ministry and sector-wise data ministry is what

is being proposed. This will be a primary goal that we need to work towards. Other than this, some sectors are not organized. Organize them and have owners who are responsible for data. And have architects who can answer questions around whom what when and the legal aspects in terms of what framework needs to be put together and at what level.

- **Our procurement policy needs to be realigned** to make the incorporation of technology faster and smoother.
- Technology, when created, is morally neutral. It's the environment that converts it into good or bad. Now data monetization seems to be an overarching concern. Intended misuse of data and security issues around the breach. Earlier it was targeted against institutions and businesses who had the wherewithal to defend. It is effortless to get malware today. Earlier it was difficult to get money as a ransom now it is easy thanks to cryptocurrency so now citizens and SMBs are getting targeted. Everybody is rushing to connect everything. Digital is very enabling but very vulnerable. The scale of digital risk is enormous.
- Honeypots: Nothing available as localized and global IoT threat intelligence. As of today, an Indian company Subex, an Indian company, has deployed 4000 devices in 60 plus locations ensuring maximum threat coverage and preparation of digital signatures. Modular malware that comes in small packages which have less footprint than emails and we are

reporting that.

- WhatsApp information spreads faster. Leading MSPs have a tech to get all kinds of information. They are gathering all kinds of data, and this needs to be regulated.
- Make in India is the way ahead. Encourage indigenous technology so data can remain in India.
- Threat from the non-conventional adversaries. India is sitting on a cyber volcano, and we are dealing with it using fire extinguishers. What is the stage we are at? We need to test our systems against a possible threat. Our focus should be on big and small enemies. We are more vulnerable as we are using foreign tech.
- Women and child safety, privacy, industrial cyberattacks are all essential aspects. We have 1/6th of the data so we can use that as a bargaining chip.

Roundtable: 2/4

Topic: Intelligence gathering and social media-based sentiment correlation

Venue: Jodhpur Hostel Mess, New Delhi

Date: 26th November 1000 hrs

- Social media is influencing people and their behaviour.
- Railways (IR) carries about 25 million passengers each day. For each passenger, we answer queries as well. So, when social media came, a Twitter cell was set up in 2016. Initially, there was some resistance, but then IR started responding, and it was the vision of the leadership that drove the change. All divisions and zones were told to react immediately to it. Since then, the number of queries has grown so AI and Machine Learning were used to respond on a one on one basis on the complaint resolution platform to protect anonymity. Redressal on twitter is done in a matter of 6 hours on an average. So, the resolution is now quicker and faster.
- **Privacy: central to the core of our being.** We have nothing to hide, so why should we curb this sharing is what people often ask. Our voice samples, our iris data, location information, fingerprint. So, can we hide our data?
- This information can be taken out if you become a person of interest. If you are not, then it is irrelevant. Companies are hoarding this data until the quantum computer arrives to crunch this data is a challenge.

- If you search for any product, then you will be targeted. Any product you buy is not your choice- you are targeted through gratification.
- We **have the surface web, deep web and the dark web**. Maybe there is a case in point for a neutral search engine that protects your privacy
- **Your cellphone is a Kryptonite, according to Snowden**. These devices are always on and transmitting information. So, he is putting together a Faradays cage which will protect your phone and data
- **23 attacks on Indian Army websites**. Every day we are fighting so many attacks in the cyberattack faster than the human mind can comprehend
- Human beings are being kept in the kill loop. How long will this be is the question? You need a warrior mindset to target these agents. War games are events that help us refine our strategy. There is no respite its always on.
- **Cyberattacks are happening more often in an organized manner.** AI - Watson is a fusion of man and machine which identifies the threats and mitigation measures in real-time. Machine learning – preparing machines to use the power of AI and knowledge and both are dangerous, and have we crossed this threshold? Are robots fighting in tunnels in Afghanistan? We don't know. Cybercriminals can use AI itself. Only science where passion is beyond the college level. All warfare doctrines of the US

Army are coming to a grind.

- Cyberwarfare skills are an applied mindset.
- China is planning to be an AI leader by 2030 which has significant implications
- Fear of AI escaping human control is a real threat today
- **Deep Fake** – is hard to detect and counter. Is used as a means of spreading fake news
- We need to have basic **cyber-hygiene** and more. We need to be cautious, which is the first step. Second **is protecting critical data. If data is on our physical domain,within Indian geographical boundaries, it is safe else it could be compromised**.
- We need to get our brains and skills together to take this to the next level. This is a question of dynamic defence. We need to evolve continuously.
- Cybercrime is a crime against everyone. There are no boundaries and norms, and therefore it is asymmetric and combative. How easy it is to compromise infrastructure today. It starts with a simple, phishing email. Cosmos Bank lost 100 crores in just over 2 and a half hours.
- **Social media can be used for intelligence, investigation, law enforcement and operations**. There are different products – area monitoring, profiling and more. UK Person object location event (POLE used by the UK) if you feed it social media feeds, it can segregate it by POLO. Even connected

persons can be exposed. So, a lot of data insights can be crunched.

- We have missed the bus. During the Maharashtra polls, Aarey Protest, Pakistanis IPs were tweeting in Marathi. Pakis and Chinese, have created so many avatars and they are running a well-oiled machine. Our intelligence goes around procuring some workaround for this. We do not have any long term outlook towards procurement of tech. China has a complete pipeline. They have people studying Marathi, Malayalam, Sanskrit, Hindi etc.
- We have 42 APTs (advanced persistent threats). Unit 61398 PLAs 3rd bureau is an elite cyberwarfare company of PLA. After PDPR comes into play, we lose access to intelligence.
- Metadata that is important. But do we have mechanisms to scan metadata in realtime and profile people? Like for instance, I take 5 samples of your writing and then locate you on social media all this is needed for protection. Start establishing social media labs wherever possible – army, intel, railways. Start with open source tools. If taken as a license it will cost 10-100 crores. Simultaneous start developing indigenous tools as backend APIs keep changing so that people work on this tool daily.
- **Procurement process needs to change**. The government needs to get out of tech. as there are a capability and timeline mismatch
- **Hunt for talent.** Actively hunt for and poach for

talent. Make a directory of people who have worked on critical projects aboard and bring them back to work in India. We need the right talent.

- **Crowdsource intelligence**. China has an active intelligence and cybercrime. We should have an army like that
- **Work on regional languages to derive sentiments.** APIs for modelling and understanding topics. Quality of academic scholarships is not good
- Reverse engineer commercial products like China
- Localize data in India, that's must for LEA investigation.
- Develop your own platforms; you cannot investigate China. Pakistan blocks all pings from India.
- We must have a staging infrastructure – to stage attacks into adversaries
- Think about VPN and honeypots
- KYC must be linked to social mediaaccounts.
- Need more language and subject experts/domain experts who can help in investigations into cyberattacks from foreign entities.
- Align university courses and piped into an innovation system. Make and sell these tools to the rest of the world
- Food security and cybersecurity are of the highest importance. If someone hacks into a food library and adds more of a micro ingredient, death may result.25 million people are travelling by train, and each

person drinks at least tea. If someone hacks into a central kitchen and modifies some culinary data, then what could happen? If an adversary mixes a nano ingredient in a wrong proportion and sells it in India? Bypassing various norms and mixed with various other items which can cause a long- term genetic problem, then what could be an outcome?

- Food supplied to the troops in the front, but what about people who are in peace posting and training who consume food procured from outside.
- 85 billion robocalls are made each year.US companies don't need our workforce, they just need your data, and then AI takes over to push you into making buy decisions. In the silicon chip market, our share is 0 %. We don't have products. The first route to data security is to produce hardware. If adversaries embed something in the hardware, what can be done? Everything from now is about data. Chinese have sold crap to the world, made money and converted it into AI. We don't have centres of excellence, so we are losing people. Google and Youtube decide on what is to be consumed. The algorithm decides everything, and we are under pressure. How many of us can survive without an instant social messenger?
- To create 5G systems it takes 10 years and 40 billion dollars, and we have missed the bus.
- If you push companies to firewall Indian data here, they will do it. If WhatsApp is blocked or YouTube is blocked, we don't know whom to talk to? No office in

India. Firewalling social media systems can be done in a few months if we decide. Sentiment correlation is an old game.Social opinions are hardened. Use traditional intelligence and supplement information from social media.

- Data colonization is a problem. Next-generation is getting influenced by social media LEAs are not geared to target social crime in India. Content monitoring is very critical, and there is absolutely no policy on this. When it comes to hiring people, we do not have the right skill sets in the country as we are not providing the right infra. We don't have labs, for instance.The government needs to wake up.Data localization and using indigenous tech is what we need is to take this issue seriously. Enable our citizens to be more vigilant. Parliament needs to frame a policy mechanism. Content carriers and content creators must come under the policy and guidelines.
- Bitdance (tiktok and hello) has aligned content from across the different sections of the society. All data is residing on a CDN built by china.IP assignment we don't have any control
- 5G and IoT are adding way more data to the web. The encrypted pipe between two endpoints can be misused, and we don't have a control on the endpoints. Data can be pushed via VPN tunnels outside. Android set-top boxes can be hacked, and they have entered our living room and bedroom

- The significant threat in cybersecurity is related to Pharma Sector.40 per cent of our formulations are sold in highly regulated markets. In the next 10 years, all such pharma cos will need managing this data. Need to have a prevention regime in place. What happens when IP gets lost? Illustrated through the case study of a diagnosis start-up whose IP was stolen
- Gaming Industry is affecting youth in a big way. Who certifies gaming standards? No mechanism is available in India to regulate them our culture is being threatened. What about the content that gets pushed to children. Is there any guideline or policy in place? The answer is no.
- The financial sector is not away from the fear of cybersecurity threat. Dow Jones crash engineered by a set of hackers taking control of an AP news handle to push fake news.Targeted social engineering to attack financial services
- Our digital economy should contribute 1 trillion in 5 years, but the threat landscape is growing exponentially. National Cybersecurity Task Force is working on the policy aspects. Vision: to ensure safe, secure and resilient cyberspace for the prosperity of the country. India is the largest producer, and consumer of data and India has the right to protect and secure its data and its citizens.We have to be self-reliant in terms of tech – indigenous solutions and safety of our IPRs is going away. India should

rely on indigenous vendors, and we should become a destination for making secure software and hardware. China created an infrastructure to store data; 30 per cent of data was going to China at one point in time. IPRs are pinching us because of data hoarding and theft, and China is using data against us. Data supply chain infection should be guarded against. We need to provide a safe working space/environment to employees

- Procurement policies need change. Technology gets obsolete before the procurement process gets completed.
- The biggest threat of cybersecurity is the manipulation of elections and constitution.

Roundtable 3/4

Topic: Detecting critical cyber threats using native technology

Venue: India Habitat Center, New Delhi

Date: 1st December 1000 hrs

Native technology is an essential factor in increasing the likelihood of sovereign data, that is managed in an indigenous fashion. Significant challenges are not only to have better cyber hygiene and security but also how one can improve user experience and ensure better use of resources.

- **DIA's specific challenge** – integration at the agency and tri-services level. The second major challenge is lack of a superior uniformity in terms of devices, networking devices and infra. We lack OEMs; different parameters are being used to categories devices and all. Lack of training infrastructure and trained manpower are both challenges we are trying to address by courses and campaigns
- **Lack of national-level policy on cybersecurity** – a systematic form that gives all the dos and don'ts for all digital platforms including social media ones should be brought into the public domain
- Can we fight with Google? Or even the US or Israel in cybersecurity? Cybersecurity should be in the perspective of significant lacunae in end devices – IoT devices, computers and data
- What is critical data, and what is not? Information and communication security is a significant challenge;

are people bypassing rules and procedures?

- NIA faces challenges when sensitization becomes a key issue, along with coordinated work.
- NIC is spread across all levels of governance. Thus we face many problems and have come up with some solutions such as e-office. Earlier when NIC email facility was not availed, private email was used, and government secrets would go out
- WhatsApp hacking: we cannot do away with WhatsApp; foreign firms own most of these platforms. So, we have come with Gives – government instant messenger which has been rolled out for group messaging securely even where we don't have access to secure communication channel. Such alternate infrastructure is placed so that government data and Infrastructure are secure.
- We have neglected the hardware part and the software part. We are not willing to work as we have become complacent as others have given us everything; So, we need to invest in developing our IP. Even in Israel, we find a lot of work going on in eastern European countries on cybersecurity then why not us? What stops us?
- Delhi Govt is providing 560 services to citizens so large citizen interface is there, and thus more is the threat, and anyone can enter from anywhere. A cybersecurity company has been empaneled, but major problem is end-point security. For instance, Aadhar came; first, they said use Aadhar for everything then

they said to remove all data and don't put anything on public services or data centres

- A significant difference between software product and services. Products are bought for at least a decade; DNA of product and services companies are different
- The government lays down an environment that matters; the environment has to be conducive.
- Subex has clients who are 220 companies across the world when we started; we couldn't bid for BSNL due to some lacunas in the procurement system, bidding criteria. We are now focusing on digital trust; we are looking at attacks on critical infrastructure; we give reports on cyberattacks a 26 per cent increase in attacks. Lots more weaponized malware made by research institutions with an intention to create harm. We have seen persistent harm being done through malware. Mumbai, New Delhi and Bangalore are most attacked, smart cities, transportation is most attacked along with financial services. We generate a lot of threat intelligence we are handing over to threat intelligence to others as well. There are 4 phases of persistent attacks – snooping, pre-attack phase, attack and post-attack. Hackers are using machine learning to develop malware. If we have a machine learning trained model listening to all indicators in the system, an attack can be detected in the pre-phase, and machine learning is essential on this front. A lot of data is needed, and the data must be sanitized and

checked for patterns.Cybersecurity has come a long way. Hackers are not just a nuisance but are a well-fundedthreat.Most institutions have cybersecurity teams that focus on response rather than prevention

- In cybersecurity, when you get to the investigative part when it comes to being attacked. What kind of data is shown to us when we see YouTube or other social channels? Smartphones are everywhere. We are heading towards digital slavery and data colonization, both of which require attention. We are moving towards SAAS and IAAS and how competent are we to develop a solution for this? Training LEAs is another issue of concern; resources available are not up to the mark as training is lacking, and we need to address these issues. Is my personal data critical data? It is critical for me as it is essential. Are we making our children's life secure? Active security mechanisms are needed to protect our citizens
- Data is so critical, but we take it so lightly like a coal mine. Data is coal and information is diamond.
- Cybersecurity policy is a must like GDPR in Europe. Let'sformalize the cybersecurity policy, which can be held in a court of law. Data protection is a problem – people moved from physical to digital files. Empower the relevant people and youth who are aspiring to get into these domains
- MoS Development has IT/ITES is a sector skill council. NSDC is working on this
- In the 1962 war; troops are moving on land. Warfare

today is different, and you don't see the enemy. Two aspects of warfare – space-based and physical ops. Now focus is on how can satellites be targeted? Cyber part of the war will be the most important one; the battle will be fought on the airspace over the oceans or the skies, so a strong air force is needed, space technology needs cyber resilience.A competent force has to be developed that can protect our cyber-assets, then we will be able to defend and win.

- Awareness and education at the topmost level at Government and Academician is not there; since most of the people holding senior positions are above 50 years of age and SMEs are below 35 years of age. Coordination must be built for the same.
- Data protection is essential – rest will follow.The moment you launch any govt. website. The website is attacked immediately. We need to have a national cyber strategy, invest in capacity building. Geospatial technologies must be indigenously developed like maps.

Roundtable 4/4

Topic: Cyber resilience for critical infrastructure

Venue: Constitution Club of India, Sansad Marg, New Delhi

Date: 5th December 1000 hrs

- We need a forum or platform that brings all the cybersecurity professionals from the govt. Sector so that they can interact and exchange knowledge and best practices as they find it difficult to reach out. This can look at training requirements and skilling needs. Various departments can then connect and interact to determine risks and then figure out the funds needed. A portal can then be hosted to support this initiative backed by an industry body
- Reports published by various organizations should be studied and then used to give inputs to the government agencies to improve awareness and action.
- Update on vulnerabilities and the link to organizational wellbeing. Including breaches and attacks outside.
- Cyber Resilience is essential, not enough to just protect data; unless data is pure and trustworthy and protects the privacy of individuals, Resilience is the central part as to how you mitigate, contain and resurrect rapidly
- Multi-functionality is here. It is essential to protect our data from cyberattacks and natural disasters as well that can affect service delivery. This is a challenge to handle all the forms of disasters that can

happen

- **5.2 trillion dollars of impact can be caused by cyberattacks alone. With mistakes, it could go up to 10 trillion USD**
- Kundamkulam nuclear plant attack, WhatsApp snooping and the recent withdrawal of support for Windows 7 are all important events. Most breaches are attributed to human intervention and error is wrong and not in order. It is not the human error but the human nature that creates problems.
- **We secure infra through isolation in the real world. In the virtual world also, we must isolate these virtual assets.**
- In open-source libraries, back doors are there in the libraries, and thus all interdependencies get installed leading to breaches. So, we need a system and a tech approach; tech solutions are a part, but processes also need to be understood to offer a complete solution.
- Ransomware may or may not be detected why? Because it emulates human behaviour. So, understanding the complete aspects of human behaviour is essential after this system should be designed to detect whether it is a human or not
- Russian aircraft have back-up manual systems that work;
- China has active hackers and manpower; do we have the manpower?
- Do we have a unified command? And leadership?

- Media management and public confidence management are essential in a war situation like Balakot. Are we ready?
- Definition of cyber resilience is different for different agencies; for some, it is the SOC, malware protection systems etc.
- **Reclassification and recategorization of critical and information infrastructure**
- **Mock drills for living without the internet should be conducted. If India is cut off from the rest of the world, can our infra (maybe banking?) work without the internet? Not just for a day but 1-30 days.**
- AI, IoT and ML are most dangerous for cybersecurity. A smartphone could be used to attack critical infra and become a significant threat
- In armed forces even today, we are dependent on weapons from abroad; with the rapid increase in ICT devices and the equipment, we import pose a significant threat in terms of what gets embedded. (supply chain poisoning). This issue needs to be addressed so that our operations are not disrupted
- Chip design should be indigenized and need to strategies
- Each system should have a plan – like a graceful degradation; how do we have back-up redundancies built in so that the system doesn't collapse when a part of it is stressed

- Definition of critical infrastructure; Sec 70 talks about critical communication infra; It is very generic and brings enough flexibility to change with time; we have rules based on that. Should include cyberattacks, damage due to natural calamities and damage due to obsolesce of IT assets because of mismatch of funds;
- Promote cybersecurity professionals in India to develop solutions to deal with those problems; upgrading skills and skillsets
- High time that we do BTech in the fields in cybersecurity to get specialized manpower
- Most of the threats are coming from the interface of human and systems;
- **NCCC** is finalizing cyber strategy next year. 3 common strategies – cybersecurity strategy is part of national security strategy; to respond use all means military and nonmilitary to impose a cost on the actor; deterrent is a crucial element. US has clearly said the DOD has to formulate and implement strategies to prevent hacks.We should also build infrastructure here itself
- Balkanization of internet taking place. Of all the 13 internet services, 11 are in US 1 in Europe 1 in Japan; so, if the net pipe is cut, what happens? We should have a UN-led solution; so, the UN group of experts in meeting next week; India will play a significant role in UNJG; we will work towards making nations work together.
- Govt. has issued instructions about 6 sectors (health

is not part of it) NCIPC was raise in 2014 – they have the mandate to identify critical IS infrastructure. Within that, they need a protected system defined by the concerned ministry. Problem is once they come under a protect system, there are severe penalties in case of mistakes, including imprisonment up to 7 years, so no ministry has declared a protected system.

- There is a need for SOC at the sectoral level, then SOC at the unit level and then IT employees should be separated from CS employees; IT guys are monitoring 800 endpoints.
- NCCC will change and go for a 3-tier structure. A different certification mechanism needs to in place for each part of the critical infra that is recognized by all. NCCC is meeting CAG next week to see how financial and cyber audit can be combined and meeting CBSE chairman to incorporate cybersecurity in the curriculum. MEITY made the earlier policy; Now NCCC has a consultative approach to create a cybersecurity strategy where representations are heard every Friday.
- **NCSS2020.nic.in is the site to submit your comments**
- Techsagar.in is the repository for tech companies connected with cybersecurity.
- NCCC has opened a national malware lab. We are planning to have a national-level threat intel and how to distribute it.

Take Away and Way Forward

- The risk faced by India on the platform of cybersecurity is unique. Being a subcontinent as diverse as India, and one with a history of invasion, colonization and freedom impacting its participation in the global growth in the technology sector needs to be overcome soon.
- Data sovereignty is of the utmost importance; it is necessary to ensure that the world does not control India, but the home to 1/6th of the population of the world has a strategic right over its data, and this data is not used commercially.
- Data and Technology go hand in hand, and thus, hardware and innovation in this area are as necessary as ownership of data. Indigenous technology will directly impact data sovereignty.
- A central agency for data storage and mandates needs to be established; this agency will be core to the central government and be supported by its regional counterparts. This will not only be a warehouse for data storage but an agency that regulates data usage, access and collection.
- A well-versed policy document and framework need to be immediately rolled out to ensure that the lack of power India has within its borders concerning Data Privacy in nullified and data is an empowering factor for the population, commercial organizations and strategic establishments of the nation-state.

- As with information technology itself, the circumstances surrounding cybersecurity legislation are changing so rapidly that an accurate prediction is difficult to make. The door remains open for cybersecurity policy to flow not down from the federal government but up from the information technology industry.
- It is no longer realistic to expect an IT department to mitigate every IT security risk. The mitigation should be converted into prevention at a much broader level. Many new cybersecurity dangers originate from social engineering, user error, exploits to web browsers, and others that are not entirely protective.
- The marketplace for cybersecurity protection has boomed, and it is now something that companies should ponder. Cybersecurity insurance is not only about protecting against financial risk. If a data breach hits one's company, there is much damage to contain, and one may need help with that from the kind of experts and damage-limitation specialists one's insurer could provide.
- Cybersecurity is not merely a technology issue is how easy it is for a member of staff in any department to cause a data breach.
- Essential to building capacity right from school level to engineering-specific courses to handle cybersecurity, it is an applied science so needs more practical exposure for academics and an environment under the supervision of LEAs to need to be built for

the same.

- Decide if Data is in the concurrent list or Central list or State list.

About Hosting Organisations

The Roundtable conferences on Cybersecurity Citizen 2030 are being hosted by:

Centre for Knowledge Sovereignty (CKS) has been working on various aspects of cybersecurity in conjunction with state enterprises and individuals at large. Due to financial losses, conflict or disharmony, state or non-state actors may have to face such challenges of cybersecurity. CKS has been discussing and proposing measures to address such threats through a series of roundtables, whitepapers and books conducted in the recent past.

Centre for Joint Warfare Studies (CENJOWS) was raised at the initiative of Ministry of Defence, that has worked to rise above sectoral and departmental legacies and, to examine joint warfare and synergy issues in their entirety.

The IMC Chamber of Commerce and Industry, popularly known as The IMC, is a legendary organization which has relentlessly pursued the agenda of identifying opportunities, addressing critical issues and driving Indian businesses with the single minded focus of sustainable growth.

Shreya Sharma
Secretariat
Mob: +91 9821240543
Email: secretariat@cksindia.in
www.cksindia.in

ATTENDEES OF CYBER SECURITY 2030 ROUNDTABLE IN 2017)

1	Shekhar Dutt SM	Former Governor Chattisgarh
2	Lt Gen Vinod Khandare AVSM, SM	Defence Intellegence Agency
3	Lt Gen Vinod Bhatia, PVSM, AVSM, SM (Retd)	Centre For Joint Warfare Studies (CENJOWS)
4	Lt Gen Dr. D. B. Shekatkar PVSM, AVSM, VSM (Retd)	Center For Knowlege Sovereignty
5	Lt Gen V. M. Patil AVSM, PVSM (Retd)	Center For Knowlege Sovereignty
6	Rear Admiral S Y Shrikhande AVSM (Retd)	Indian Navy
7	Dr S D Pradhan	National Security Council Secretariat
8	Avadhesh Mathur	R &AW
9	Jayadeva Ranade	R &AW
10	Amitabh Mathur	R &AW
11	Vinit Goenka	Secretary, Centre for Knowledge Sovereignty
12	Brig Pradeep Arora	Joint Intelligence Committee
13	Brig Manjeet Singh	DACIDS/DIARA
14	Brig Jai Singh Yadav VSM	CENJOWS
15	Brig Deepak Malhotra	CENJOWS
16	Brig H S Cheema	CENJOWS
17	Brig R K Bhutani(retd)	CENJOWS
18	Dr Vipin Tyagi	Centre For Development Of Telematics (C-DOT)
19	Dr B V L Narayana	Centre For Railway Information Systems (CRIS)

20	Group Captain G D Sharma VSM (Retd)	CENJOWS
21	Commander L R Prakash (Retd)	C-DAC
22	R Chandrashekar	CENJOWS
23	Air Commodor T Chand(Retd)	CENJOWS
24	Capt Ranjeet Seth (IN)	CENJOWS
25	Uma Sudhindra	IIM Vizag
26	Professor Dr Sharad Sinha	National Council of Education Research and Training (NCERT),
27	Bharat Panchal	NPCI
28	Dr Arunima Chakravorty	DPS Bhagalpur & DPS Greater Ranchi
29	Dr. Vatsala Joshi Pande	Lok Sabha
30	Pavitran Rajan	Cyber Security Reaserach Center
31	Sanjukta Mookherji Sahani	JaagoTeens , an NGO
32	Sumitra Goenka	Ratein Infotech India Pvt Ltd
33	Savita Kakar	DRDO
34	Rita Shrivastava	Central Research Laboratory , Bharat Electronics Limited
35	Ambika Khurana	IBM
36	Ajay Ranjan Mishra	Ericsson
37	Tulsidas Bhoite	Lokmat Digital
38	Krishna Kumar Thevar	Economic Times
39	Nitin Gokhale	Journalist, Bharat Shakti
40	Rahul Aggarwal	Partner, PWC
41	Col Y S Pathania	CENJOWS

42	Col Harpreet	CENJOWS
43	Professor Chandan Chowdhury	Indian School of Business (ISB)
44	Rohit Bhambri	PWC

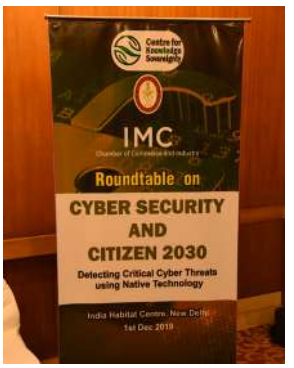
PHOTOGRAPHS FROM THE 4 ROUNDTABLES: CYBERSECURITY AND CITIZEN 2030

CONDUCTED IN NOV-DEC 2019


IMC
CYBER SECURITY AND CITIZEN 2030


IMC
CYBER SECURITY AND CITIZEN 2030


IMC
CYBER SECURITY AND CITIZEN 2030


IMC
Roundtable on
CYBER SECURITY AND CITIZEN 2030
Detecting Critical Cyber Threats using Native Technology
India Habitat Centre, New Delhi
1st Dec 2019


IMC
Roundtable on
CYBER SECURITY AND CITIZEN 2030
Detecting Critical Cyber Threats using Native Technology
India Habitat Centre, New Delhi
1st Dec 2019


IMC
Roundtable on
CYBER SECURITY
AND
CITIZEN 2030


IMC
CYBER SECURITY AND CITIZEN 2030
Cyber Resilience for Critical Infrastructure


HITA GANGADHARAPU


LT. COL. JOYASU BAGAI


ND CITIZEN 2030
tical Infrastructure
019
dia, New Delhi


Roundtable on
CYBER SECURITY AND CITIZEN 2030
India Habitat Centre, New Delhi
1st Dec 2019


MUNEESA NIGAM


MUNEESA NIGAM


CYBER S
AN
CITIZEN


SUMITRA GOENKA


VIJAY KUMAR KAUL


VINIT GOENKA


CYBER SECURITY
Empowering Agencies with Comprehens
Constitution Club


Roundtable on
YBER SECURITY AND CITIZEN
Cyber Resilience for Critical Infrastructure
5th Dec 2019
Constitution Club of India, New Delhi

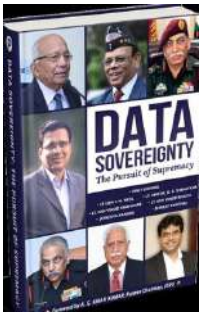

VINEET KUMAR
SANTOSH CHAUBEY

CKS Publications


New Generation Port Community System – The digital future of Indian Maritime Industry

Table of Contents

Contents



CYBER SECURITY & CITIZEN 2030

Since the launch of the National Cyber Security Policy in 2013, India has needed a futuristic Strategy that will not only mandate the need for cybersecurity across all sectors but will help the entire economic and political pipeline identify and strategise for growth and success appropriately. With new concepts like data sovereignty, and the 4th generation Industrial revolution like AI, IoT, 5th Generation technologies, geospatial and other technologies the possibility of citizens being individually targeted and scope for non-kinetic warfare, make a cybersecurity strategy most imperative. A policy framework is the need of the hour.

Centre for Knowledge Sovereignty (CKS) in association with **Centre for Joint Warfare Studies (CENJOWS)** and **IMC Chamber of Commerce and Industry, formerly Indian Merchants' Chamber** (IMC) thus, hosted series of roundtables that focused on deliberating challenges the nation will face if we remain oblivious to cybersecurity and the need for the same, alongside the solutions that each sector can provide.

The discussions were compiled into a set of recommendations that were then submitted to Lieutenant General Dr. Rajesh Pant (Retd), PVSM, AVSM, VSM, PhD, Chief of National Cyber Coordination Centre (NCCC) and have been published in this book.

Post the roundtables, the attendees and few relevant stakeholders who were unable to attend were requested to submit their views in the form of articles. This book is a compilation of all articles and discussions concerning the roundtables conducted under the title of Cybersecurity& Citizen 2030.

Also available as an **e-book**

ISBN 978-81-944894-5-0

978-81-944894-5-0

₹ 599/- | $9.99

authorvine.com