Vivekananda International Foundation

Research and Development in Cyber Domain and Indian Perspective

Maj Gen P K Mallick, VSM (Retd)

VIF Paper | September 2019

Published in September 2019 by
Vivekananda International Foundation
3, San Martin Marg | Chanakyapuri | New Delhi - 110021
Tel: 011-24121764 | Fax: 011-66173415
E-mail: info@vifindia.org
Website: www.vifindia.org
Follow us on
Twitter | @vifindia | Facebook | /vifindia

About the Author

One of the foremost experts on electronics and communication, Maj Gen PK Mallick, VSM (Retd) is a graduate of Defence Services Staff College and M Tech from IIT, Kharagpur. He has wide experience in command, staff and instructional appointments in Indian Army. He has also been a Senior Directing Staff (SDS) at National Defence College, New Delhi. Presently, he is a Consultant with the Vivekananda International Foundation, New Delhi.

Research and Development in Cyber Domain and Indian Perspective

The quest for an open and accessible internet often leads to vulnerability. Stories of hacking and defacement of websites are the tip of an iceberg. They suggest that cyber attacks are a significant threat, especially in the democratic world. We need to ensure that vulnerable sections of our society do not fall prey to the evil designs of cyber criminals. Alertness towards cyber-security concerns, should become a way of life.

Nations must also take responsibility to ensure that the digital space does not become a playground for the dark forces of terrorism and radicalization. Information sharing and coordination among security agencies is essential to counter the ever-changing threat landscape.

- Prime Minister Narendra Modi at Global Conference on Cyber Space in New Delhi, Nov 23, 2017

Introduction

With the convergence of computer and communications technology a vast, interdependent physical and electronic network has emerged which connected government, commercial, scientific and educational infrastructures including critical infrastructures. This rapid increases in interconnectivity have facilitated enhanced communications, economic growth and the delivery of services critical to the public welfare.

Professional criminals and state sponsored saboteurs pose a serious threat in cyber space. Large number of countries are developing increasingly complex digital attack capabilities. Digital infrastructures of countries are getting numerous attacks daily from non state actors. Economic interests and national security of countries are threatened. Cyber attackers are technically advanced, highly motivated and well funded. Their attacks pose a threat to national initiatives such as Smart Cities, E-Governance and digital public identity management. Government and military organisations and other businesses are susceptible to cyber threats. The potential damages put national security at risk if critical information infrastructure is targeted.[1] Over the past few years, India has witnessed massive adoption of cyber technologies in all the facets of life. This adoption is raising concerns and

challenges from cyber security and privacy view point. India being a preferred outsourcing destination for IT and Business Process Management (BPM) services requires a focused and continued attention on security and privacy. There is a demand for investment in cyber security capability building and Research and Development (R&D) activities.

To define a cyber security R&D roadmap for the country all the stakeholders - government, industry and academia have to come together. To develop a securer cyber ecosystem Public Private Partnership (PPP) would help in combining best of both worlds and complement capabilities. Talent in this field has to be retained in the country. Appropriate protection to the Intellectual Property Rights (IPRs) developed by the indigenous cyber security research organisations has to be arranged. Increased government funded research and public private coordination is needed in the expanding fields of new secure networking and computing architectures, high-performance computing, encryption, data integrity, artificial intelligence, big data, privacy and risk management strategies. Governments have to provide legal protections for legitimate and beneficial computing privacy and security research.

Post Snowden disclosures it is very clear that we must develop our own indigenous capabilities in the cyber domain if we have to secure our networks, systems and critical infrastructure.

Learning from Other Countries

Cyber Security Research Areas for Governments.

Governments around the world are eyeing continuous research in the field of cyber security to safeguard against the emerging and future threats. It is always good to learn from others and not waste resources in reinventing the wheels. Some of the cyber security research areas that are in focus by various countries are briefly mentioned below.

USA

Federal cyber security R&D strategic plan implementation roadmap for the financial year 2019 issued by Committee on Science & Technology Enterprise of the National Science & Technology Council, lays down the framework for cyber security research in USA.[2] Federal R&D in high-capability computing is advancing state-of-the-art, dual-use technologies and tools to defeat emerging threats on the physical and cyber battlefields, including applications ranging from military platform analysis to artificial intelligence; supporting quantum computing and including leading-edge supercomputing facilities.

U.S. Government Federal Cyber security R&D Strategic Plan Implementation Roadmap, August 2016 has identified following six areas critical to successful cyber security R&D[3]:-

- Scientific foundations.
- Enhancements in risk management.
- Human aspects.
- Transitioning successful research into pervasive use.
- Workforce development.
- Enhancing the infrastructure for research.

Guiding Principles. A set of guiding principles are formulated to ensure the cyber security program addresses the desired improvements, outcomes and guidance stated in policy document. The following are guiding principles specific to the cyber security domain[4]:-

- Coordinate research activities to systematically progress towards achieving the attributes and desired end state of a healthy cyber ecosystem.
- Engage social science research labs to understand social science dimensions of cyber security, augmenting "hard computer science" research.
- Focus research on promising scientific approaches which comprehensively and rigorously underpin required security policy.
- Focus research on promising scientific approaches which comprehensively and rigorously underpin the quantitative cyber security risk assessment of complex systems especially critical infrastructure.
- Focus research on promising scientific approaches to automate collective action amongst distributed systems to defend individual

computers and networks.

- Focus research that recognises the presence of adversaries in cyberspace, with potential emphasis on the Manichean sciences.

- Engage research labs to investigate cyber security related research gaps and to de-risk scientific approaches and emerging technological solutions.

- Leverage and influence cyber security related maturity models and standards when investigating hard problems.

- Build upon existing knowledge that is relevant to cyber security.

- Leverage research that addresses big data challenges that also addresses cyber challenges.

- Leverage existing knowledge regarding ways of working and carefully address the numerous considerations (such as those pertaining to ethics) that influence and are influenced by cyber security.

Agencies. The following agencies in USA carry out R&D on cyber security[5]:-

- Air Force Research Laboratory & Air Force Office of Scientific Research.

- Army Research Laboratory and Army Communications-Electronics Research, Development and Engineering Center.

- Defense Advanced Research Projects Agency.

- Department of Defense High-Performance Computing Modernisation Program (HPCMP).

- Department of Homeland Security.

- Department of Energy Office of Cyber security, Energy Security and Emergency Response.

- National Institute of Standards and Technology.

- National Science Foundation.
- National Security Agency.
- Office of Naval Research.
- Office of the Secretary of Defense.

European Union (EU)

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and EU citizens. It has identified the threats and the strategic priorities in research and development. The themes for research, the challenges of education and emerging threats have been given out in Analysis of the European R&D priorities in cyber security, European Union Agency for Network and Information Security, December 2018.[6]

Themes. The following themes were suggested where future research should be focused on:-

- **Awareness Building – Societal Challenge**. Addressing the need, across society, to build awareness of the impact of technological change on social evolution and hence on societal risk.
- **Capacity Building – Educational Challenge**. This recognises the shortage of cyber security experts and considers means to refresh education at secondary and tertiary levels to bridge the gap
- **Existential threats**. It is those threats that if enacted have potential to destroy the directly impacted part of society, industry or business. The threats are:-
    - **Artificial Intelligence**. Due to the pervasiveness of data collection by the Internet of Everything (IoE), the processing power and storage capacity offered by the cloud,

pattern recognition and automatic decision will develop at great speed bringing new opportunities and risks.

- **Quantum Technologies**. Uncertainty may be used in both attack against current cryptographic protection methods and in the development of new computational models for further acceleration of change.

- **Complexity of Interconnectedness**. It may lead to cascade fail of multiple systems across the supply chain.

- **Cybercrime**. Because of digital transformation, digital identities and valuable assets may become prey during a cyber attack. Detection and mitigation of cyber attacks becomes extremely important.

- **The Threat to Privacy.** It is increasing with "big data" collection and unexpected inference.

Singapore

Singapore has an National Cyber security R&D Programme (NCR) to develop R&D expertise and capabilities in cyber security. The aim of the programme is to improve the trustworthiness of cyber infrastructures with an emphasis on security, reliability, resiliency and usability. NCR is coordinated by various Government agencies like Ministry of Defence, Ministry of Home Affairs, Cyber Security Agency of Singapore, National Research Foundation Singapore (NRF), National Security Coordination Centre, Government Technology Agency, Info-communications Media Development Authority (IMDA) and Economic Development Board. It promotes collaboration among government agencies, academia, research institutes and private sector organisations.

Cyber security research spans six themes, which are designed to provide an element of operational context, while not restricting "game-changing" ideas from the community. The six themes are[7]:-

- **Scalable Trustworthy Systems**. Research into technologies to make computing systems' hardware, firmware and software function dependability despite the presence of untrustworthy components or insiders.

- **Resilient Systems**. Research for improving resiliency, robustness, adaptability and capacity in systems will provide technologies to rapidly respond & recover cyber-physical systems and supporting infrastructure (e.g. power, water, communication).

- **Effective Situation Awareness and Attack Attribution**. Focus on research to enhance understanding of cyber situations, deliver new cyber forensics techniques and tools to fast-track investigation and attack attribution.

- **Combatting Insider Threats.** Research to combat insider threats will enable us to create, analyse, evaluate and deploy mechanisms and strategies that can provide detection, prevention and identification of insiders and their activities.

- **Threats Detection, Analysis and Defence.** Research to combat threats like malware and botnets will enable us to create, analyse, evaluate and deploy mechanisms and strategies that can provide detection, analysis, prevention and immunisation capabilities against malware and botnets.

- **Efficient and Effective Digital Forensics.** Applied research for digital evidence acquisition and forensics to reduce the analysis time required to comprehensively locate and evaluate digital evidence in diverse, disperse and multi-tenanted systems.

R & D Agenda. The Government of Singapore has identified the following research areas. These are[8]:-

- Authentication, cryptography and other secure data communications technology; computer forensics and intrusion detection.

- Reliability of computer and network applications, middleware, operating systems, control systems and communications infrastructure.

- Privacy and confidentiality.
- Network security architecture, including tools for security administration and analysis.
- Emerging threats.
- Vulnerability assessments and techniques for quantifying risk.
- Remote access and wireless security.
- Enhancement of law enforcement ability to detect, investigate and prosecute cyber-crimes, including those that involve piracy of intellectual property.
- Secure fundamental protocols that are integral to inter-network communications and data exchange.
- Secure software engineering and software assurance including:-
    - Programming languages and systems that include fundamental security features.
    - Portable or reusable code that remains secure when deployed in various environments.
    - Verification and validation technologies to ensure that requirements and specifications have been implemented and
    - Models for comparison and metrics to assure that required standards have been met.
- Holistic system security that:-
    - Addresses the building of secure systems from trusted and untrusted components.
    - Proactively reduces vulnerabilities.
    - Addresses insider threats and

    - Supports privacy in conjunction with improved security.
- Monitoring and detection.
- Mitigation and rapid recovery methods.
- Security of wireless networks and mobile devices.
- Security of cloud infrastructure and services.
- Security of election-dedicated voting system software and hardware.
- Role of the human factor in cyber security and the interplay.

China

China has been declaring its policies on cyber security from time to time through different government policies and plans. The 2015 Ministry of National Defense paper entitled "China's Military Strategy" defined cyberspace as a "new pillar of economic and social development, and a new domain of national security." It declared that "China is confronted with grave security threats to its cyber infrastructure as international strategic competition in cyberspace has been turning increasingly fiercer, quite a few countries are developing their cyber military forces."[9]

State Network and Information Security Coordination Small Group (SNISCSG) is working on the development of China in the fields of information technologies. The Chinese authorities declared in the 2016 Outline of National Information Development Strategy that the building of a strong cyber nation is an urgent matter and no time should be wasted. The strategy points out that key weaknesses in China's cyber capabilities including lack of 'core technologies', underdeveloped information technology infrastructure, seriously challenged internet security and a poorly developed legal and governance regime.

The 2006-2020 Medium and Long-Term Science and Technology Development Plan (MLP) argues that the only way that China can advance against international competition is to "improve its independent innovative capabilities and master a number of core technologies, own a number of proprietary intellectual property rights and groom internationally competitive enterprises in important fields." This can only be achieved through indigenous innovation.[10]

Internet Plus. On July 4, 2015 China unveiled its Internet Plus roadmap. The road map aims to integrate the Internet with traditional industries to fuel economic growth.This five-year plan intends to integrate the Internet of Things, cloud computing and big data with a variety of industries from manufacturing to commerce, internet banking, agriculture. The Internet plus road map consists of several different initiatives:-

- Additional funds for research and development, reaching 2.5 percent of GDP through 2020.
- More funds for promoting business development and innovation.
- Reduced dependency on non domestic technology innovation.
- Access to 100 MB/s internet connections for people in large cities.
- Broadband connectivity to reach 98 percent of population.

Premier Li Keqiang's in the annual report on the work of the government. stated: "We will increase support for basic research and application oriented basic research, step up original innovation and work harder to achieve breakthroughs in core technologies in key fields."

In April 2018 Speech at a second Cyber Security and Informatisation Work Conference President Xi Jinping focused on core technologies, a thriving digital economy and strong controls and political work by Chinese

Communist Party (CCP) and government authorities online. He stressed on comprehensive network governance capabilities, core technologies as important instruments of the state, strengthening civil-military integration in the cyber security and informatisation domain, move forward the construction of China as a cyber superpower through indigenous innovation. He said, "Without cyber security, there is no national security, the economy and society will not operate in a stable manner, and the broad popular masses' interests will be difficult to guarantee."

Xi described core technologies as falling into three categories. The first is basic technology, commonly used technology; the second is asymmetric technology, or 'trump card' technology; the third is advanced technology, or disruptive technology. Core technology would include cryptography, certain types of advanced semi-conductors, advanced memory circuits, server technology, a growing list of software, including operating systems, enterprise-level database software, cyber security software, cloud systems and lately, both hardware and algorithms that power advanced artificial intelligence systems.[11]

R&D Through Cyber Security Clusters. Several countries across the globe have established cyber security 'clusters' to foster innovation and promote research and development in the field. These clusters are areas with a high concentration of cyber security companies with special incentives and growth accelerators. We can also develop our cluster around Bangalore/ Hyderabad/Gurugram/Chennai/Pune.

From the above it can be seen that most of the leading countries in the world are taking keen interest in research and development of cyber security issues. They have formulated clear cut processes to achieve their aims.

Cyber Defence Plan

Cyber defence is a computer network defence mechanism which focuses on preventing, detecting and providing timely responses to attacks or threats so that no infrastructure or information is tampered with. All responsible nation states have their strategic plan to provide priorities for cyber security R&D in alignment with their national framework for Improving Critical Infrastructure. The four strategic defensive elements of the strategic plan consist of Deter, Protect, Detect and Adapt, as defined below[12]:-

- **Deter**. The ability to efficiently discourage malicious cyber activities by: measuring and increasing costs to adversaries carrying out such activities; diminishing the spoils; and increasing risks and uncertainty for potential adversaries.

- **Protect**. The ability of components, systems, users and critical infrastructure to efficiently resist malicious cyber activities and to ensure confidentiality, integrity, availability and accountability.

- **Detect**. The ability to efficiently detect and even anticipate adversary decisions and activities, given that perfect security is not possible and systems should be assumed to be vulnerable to malicious cyber activities.

- **Adapt**. The ability of defenders, defenses and infrastructure to

dynamically adapt to malicious cyber activities by efficiently reacting to disruption, recovering from damage, maintaining operations while completing restoration and adjusting to thwart similar future activity.

Figure 1 shows how these four defensive elements thwart malicious cyber activities and the value of continuous outcome-driven improvements in efficacy and efficiency.

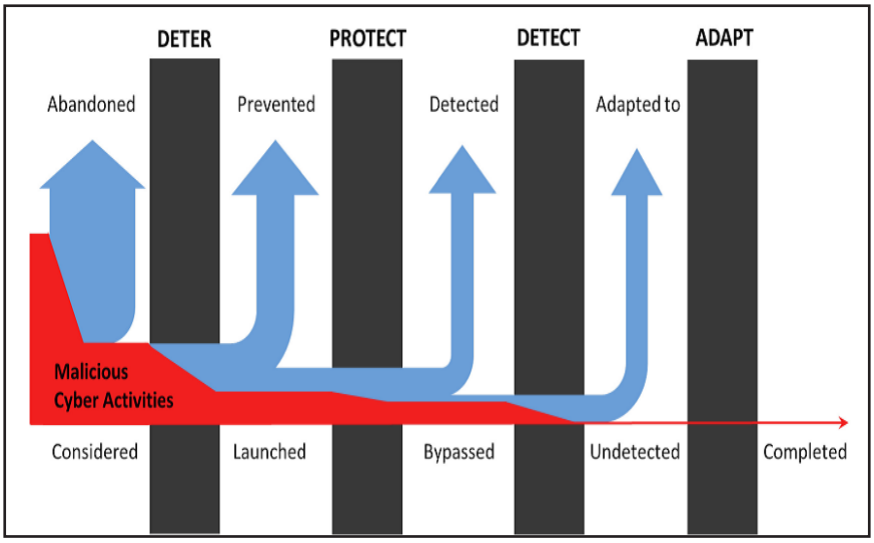

Figure1. Continuously strengthening defensive elements improves success in thwarting malicious cyber activities.[13]

Some of the Critical Issues which drive cyber security R&D efforts are given below.

Emerging Technologies

The following emerging technologies may have a considerable impact (negative, positive or both) on cyber security are discussed below[14].

Autonomous Technologies. Emerging technologies, such as AI-based

robotics and deep learning, enable more and more applications where human decision-making is no longer required. Such networked applications may be vulnerable to hackers in areas such as communications channels, controls and sensors.

Internet of Things (IoT). We are moving toward the connection of "things" made available to people through much-improved interfaces. This trend includes Industrial Control Systems for operating critical infrastructures and also wearable/implanted medical devices. The Internet of Things (IoT) pervades daily life, blurring the physical and virtual worlds. This entanglement leads to online risks becoming increasingly intangible, contributing to further cyber-threats.

Artificial Intelligence (AI). Artificial intelligence (AI) has at its core the promise of huge benefit with similarly huge risk. Enabled by the massive amount of collected data by the evolving Internet of Everything (IoE), the ubiquitous fast connectivity and cloud infrastructure, new applications using artificial intelligence are proposed every day. We increasingly rely on AI for decision-making, creating new vulnerabilities to cyber attacks. AI systems can definitely help in mitigating cyber threats, but may suffer from various deceptive tactics that are difficult to anticipate or understand. It can not only lead to more automated social engineering attacks but also help in predicting and preventing such attacks. More specific research actions on AI are summarized below:-

- Research in developing AI techniques that produce more explainable models while maintaining prediction accuracy.
- Research in verification, validation, security and control of the machine learning algorithms for preventing safety issues.

- Research in adversarial machine learning in order to avoid wrong results due to the introduction of false data in the machine.

- In applications where machine learning is unsupervised and there is an interaction with people, AI experiments have shown bias and unfair results. Research is needed how to build inclusive and no discriminatory AI.

Quantum Computing. Quantum computers have potential to break current cryptographic tools, thus posing a serious threat to all systems that use "classic" cryptography. Quantum cryptography and quantum communication have the potential to offer "perfectly safe" networks. Quantum computers might be able to undermine the security that underpins e-commerce, e government.

Supply Chain Threats. The digital transformation has engendered a subtle transformation that has made all sectors increasingly dependent on digital infrastructures. Cloud providers offer many services now and any unavailability, loss of integrity or violation of confidentiality, may have serious consequences for businesses or governments who use their services. The unavailability of financial operations has the potential to affect the operations and economy of most countries and businesses. Unfortunately, the security of systems cannot be guaranteed to 100 percent. But efforts must be done to secure the systems in order to reduce the risk at an acceptable level and guarantee resilience and business continuity. Specific research actions are:-

- New approaches for dependency and interdependency impact assessment.

- Research on the cyber security measurements (by catching meaningful parameters from empirical data analytics) might be extremely important to determine trends to better utilize security resources and judge the success or failure of implemented security solutions.

- Convergence of safety, security and quality elements that might be used to assess the maturity mode land the resilience of the system.
- Define secure, interoperable interfaces among different critical infrastructures to prevent from cascading effects.
- New approaches to mitigate against the increasing value of attacks as a result of data centralisation.

Blockchain. It is a peer-to-peer network with open distributed ledger facilitating secure online transactions for applications such as financial services, smart contracts, healthcare and IoT. Blockchain enables protecting identities and preventing data manipulation and fraud, as well as preventing distributed denial-of-service attacks.

Cyber Resilience. Cyber resilience is the ability to absorb attacks, as well as to recover from them and rapidly restore business operations back to normalcy. This technology includes several techniques, such as adaptive response, diversity, redundancy, deception and proactive resilience.

Homomorphic Encryption. It is an encryption technology that enables performing calculations on encrypted information without decrypting it first. This technology can change how data are protected when using remote systems, such as cloud services.

Bio-hacking and Human-Machine Interface. Development of neuro-technology and robotics enables new opportunities for human–machine interaction. However, such devices can be used to maliciously extract private information from users, or even tamper with the device's functionality.

New Technologies. The report on Credible Cyber Deterrence in Armed Forces of India by Vivekananda International Foundation Task Force, March 2019, identified the hard problems of cyber security that require

R&D efforts[15]. The following emerging advances in technology would help deliver a step change in cyber security[16]:-

- Extending encryption to allow computation to be performed directly on encrypted data, to enable full end-to-end data security.
- Quantum-safe cryptography including implementation-efficient algorithms that are resistant to advances in Quantum Computing, should this be necessary.
- Verified trustworthy systems, including through security by design.
- The application of formal methods to safety critical applications such as Critical National Infrastructure, industrial process control and medical applications.
- New data anonymisation methods for enhancing the protection of user identity, privacy and confidentiality.
- Strengthening the chain of custody of data or transactions using distributed ledger technologies such as blockchain.
- Technologies for intrusion, malware and distributed denial of service detection including new methods for the real-time application of network traffic analysis based on advanced machine learning algorithms.
- Malware-based defences to 'live with the threat', analogous to biological defences in living species.
- New technologies and models for Internet of Things network security, reflecting their highly distributed nature and the intrinsic need for security by design.
- New resource-constrained crypto and multi-factor authentication technologies for the Internet of Things and other low cost, low energy systems.

- New security architectures for hyper scale cloud infrastructures and highly virtualized computing and communications systems.
- Physical layer security for securing communications when cryptography is not possible due to limitations on computational capability, or to the network architectures involved.

Emerging technologies are changing many industries drastically. Protecting emerging technologies is difficult. It requires an in-depth basic defence approach that combines people, processes and technologies. The war between security experts charged with the responsibility of protecting cyber infrastructure and adversaries who threaten to compromise the integrity of data for different entities has become a cat and mouse game. We should be leveraging these new technologies with the existing fundamentals that are in place.

Recent Trends

Possibilities

Symantec Corporation in its latest report has highlighted some of the trends and activities that would most likely to affect organisations, governments, and individuals in 2019 and beyond.[17] These are listed below.

Attackers will exploit artificial intelligence (AI) systems and use AI to aid assaults. AI systems automate manual tasks and enhance decision making and other human activities. AI could :-

- Probe networks and systems searching for undiscovered vulnerabilities.
- Make phishing and other social engineering attacks even more sophisticated by creating extremely realistic video and audio or well-crafted emails designed to fool targeted individuals.
- Used to launch realistic disinformation campaigns.

Defenders will depend increasingly on AI to counter attacks and identify vulnerabilities. Defenders can use AI to better harden their environments from attacks and protect their own digital security and privacy. AI could

be embedded into mobile phones to help warn users if certain actions are risky.

Proliferation of offensive tools. Offensive cyber capabilities of the government and proliferation of simple attack tools both contribute to frequent incidents. Nation state cyber tools escape onto the black market and the same are reused by cybercriminals to steal from organisations. Intelligence agencies stockpile zero day vulnerabilities rather than informing affected parties, resulting in a deluge of data breaches.

Attackers will become bolder, more commercial less traceable. Hackers are becoming more organised and commercialized as seen with fraudulent dating sites, having their own call centres. They will look to base themselves in countries where cybercrime is barely regarded as a crime and thereby placing themselves outside their victims' police jurisdictions.

Attackers will get smarter. Attackers capability to write targeted code will always remain ahead of the defenders ability to counter. They will continue to exploit the Dark Web, to successfully hide and to communicate with other criminals.

Growing 5G deployment and adoption will begin to expand the attack surface area. There will be rapid growth in 5G networks. More 5G IoT devices will connect directly to the 5G network rather than via a Wi-Fi router. This will make them more vulnerable to direct attack. The ability to back up or transmit massive volumes of data easily to cloud based storage will give attackers rich new targets to breach.

IoT-Based events will move beyond massive DDoS assaults to new, more dangerous forms of attack. Massive botnet-powered Distributed Denial of Service (DDoS) attacks have exploited tens of thousands of infected IoT devices to send crippling volumes of traffic to victims' websites.

Among the most troubling will be attacks against IoT devices that bridge the digital and physical worlds. Growing numbers of attacks against IoT devices that control critical infrastructure such as power distribution and communications networks are expected.

Attackers will Increasingly Capture Data in Transit. Attackers will exploit home based Wi-Fi routers and other poorly secured consumer IoT devices in new ways like capture of some of the data passing through them or launch of massive crypto jacking efforts to mine crypto currencies. Malware inserted into such a router could steal banking credentials, capture credit card numbers, or display spoofed, malicious web pages to the user to compromise confidential information.

Attacks that exploit the supply chain will grow in frequency and impact. An attacker can target the software supply chain implanting malware into legitimate software packages at its usual distribution location. Attempts to infect the hardware supply chain will be made in the future. An attacker could compromise or alter a chip or add source code to the firmware of the UEFI/BIOS before such components are shipped out to millions of computers. Such threats would be very difficult to remove even after an impacted computer is rebooted or the hard disk is reformatted.

Privacy becomes reinterpreted. The concept of privacy will be reinterpreted by people who have been raised in an age of social networking and ubiquitous Internet access. Lives are lived 'online' and reputational damage is frequent as citizens display intimate histories through digital portals

Growing security and privacy concerns will drive increased legislative and regulatory activity. The European Union's mid-2018 implementation of the General Data Protection Regulation (GDPR) will likely prove to be just a precursor to various security and privacy initiatives in countries outside the European Union. In the U.S., soon after GDPR arrived,

California passed a privacy law considered to be the toughest in the United States to date. There is a potential for some requirements to prove more counterproductive than helpful. Overly broad regulations might prohibit security companies from sharing even generic information in their efforts to identify and counter attacks. If poorly conceived, security and privacy regulations could create new vulnerabilities even as they close others.[18]

The forthcoming Regulation on Privacy and Electronic Communications may reinforce the legal basis for the protection of privacy in electronic communications. The research challenge are:-

- New anonymisation privacy models and methods are required.
- New Analytics tools where the principle of data minimisation is applied.
- New Model of safeguarding mechanisms following the privacy by design and by default requirements.

Repressive enforcement of online order. While many states take liberal risk-based approaches, several favour repressive means to enforce order online. This leads to blanket censorship and surveillance, an order stronger than in current regimes, damaging cross-border trade and placing global commerce under pressure.

Heterogeneity of state postures. The heterogeneity of state technology postures suppress international agreement and cooperation over cyber norms. Attacks increasingly originate from 'safe havens' who refuse to prosecute their cyber criminals. The challenge of digital attribution leads to a fragmentation of shared understandings, with nations treating their allies with suspicion.

Traditional business models under pressure. Traditional business

models are placed under increasing pressure from both pirates and new competitors. Established market leaders fall and sell their data assets to innovative firms better equipped to operate in these novel environments.

Big data enables greater control. Big data and machine learning supports the manipulation of individuals' behaviour by corporations and governments. While these developments benefit commerce and law enforcement, deviations from the norm are increasingly viewed with suspicion.

Growth of public-private partnerships. Organisations continue to know more about their customers than national governments, contributing to the growth of public private data sharing partnerships. These arrangements though beneficial to national security, but large parts of critical infrastructure remain owned by foreign corporations. This reliance on private industry shifts considerable power from elected Government officials to unaccountable executives, resulting in damage to the democratic process and national security becomes critically undermined.

Citizens demand greater control. Some citizens demand greater transparency and agency over their online data. Technologically literate individuals store information remotely, occasionally selling details for a range of benefits. Corporations offer paid alternatives to data hungry social networks, creating new markets for online communities and Privacy-Enhancing Technologies.

Organisations value cyber resilience. Cyber resilience is increasingly important for informing business decisions, with issues such as insider threats high on the agenda. The infeasibility of absolute security drives a market for cyber insurance, as corporations adopt prescribed measures to reduce their premiums. Board rooms quickly learn the reputational costs of cyber-attacks, resulting in greater private investment in the actuarial and

mathematical sciences. [19]

Kill Switch. In digital devices, a digitally implemented kill switch is used to protect data by either erasing it or permanently or temporarily disabling the device, rendering it unusable by the thief without unlock credentials from the owner. As cell phones become more technologically advanced and expensive, they have become the target of an increasing number of thefts. A kill switch built into the OS of the phone or as third-party apps discourage theft by rendering the devices unusable and ultimately worthless. [20] There also is a debate about implementing kill switches in robots and advanced artificial intelligence systems. French and Israeli electronic warfare units use kill switches to disable opponents' military systems. R&D efforts are required to be made in India both for offensive and defensive aspects of Kill Switch.

Public-Private Partnership (PPP) in Cyber Security Research

Guiding Principles and Objectives that Would Underpin the PPP in cyber security are:-

- Given the diverse stakeholders in cyber security, institutional mechanisms should be set up to promote convergence of efforts both in public and private domains.
- Use existing institutions and organisations to the extent possible in both private sector and government and create new institutions where required to enhance cyber security.
- Set up a permanent mechanism for private public partnership.
- Identify bodies that can play a wider role in funding and implementation in the public and private sector.
- Identify areas where both private and public sector can build capacities for cyber security research.

- Put in place appropriate policy and legal frameworks to ensure compliance with cyber security efforts.
- Promote active PPP cooperation in international forums and in formulating India's position on global cyber security policies.
- Establish India as a global hub of development of cyber security products, services and manpower.
- Promote indigenisation and work on joint R&D projects to meet the cyber security needs of the country.[21]

From the above it is clear that the attackers in cyber domain would increasingly use more and more latest technologies. For the cyber security defenders it will be a very challenging task to thwart these new attack vectors. There will be requirement of rapid co-operation between nation states and public and private partnership.

Cyber Range Based Security Laboratory

Cyber Range. A cyber range is a controlled virtual environment that is used for cyber security and cyber warfare capacity building and technology development. It is a platform that help strengthen the stability, security and performance of cyber infrastructures and IT systems used by public and private organisations. Cyber Ranges creates near real virtual environment with Internet-scale network traffic and a credible threat intelligence to test network resiliency against modern day cyber-attacks without disturbing the production environment in any way. The cyber ranges can be custom made to suit an organisation's requirements.

Cyber range use cases. A brief list and an overview of some cutting-edge usages are as under:-

- Red-Blue Team Exercises.

- Cyber Offensive Services.
- Securing the Operational Technology (OT) Landscape.
- Research and Development.

Red-Blue Team based cyber drills. Cyber Range is used for conducting RED – BLUE Team exercises for developing a battery of cyber warriors who would be trained to safeguard the critical IT infrastructure of the country. The WHITE Team continually monitors the progress of the members of the RED Team who attacks the simulated networks, servers and applications while the BLUE Team defends them**.**

Cyber Offensive Services. Cyber Ranges are used to set up test beds to conduct hardware and software based research and testing of the malware before being launched**.**

Research and Development. Cyber Ranges can be an extremely useful tool for conduct of R&D in various fields. It can present different cyber infrastructure environments which researchers utilize to conduct their experiments. Testing of cryptographic algorithms, Network security appliances, security applications etc. are various use cases where cyber ranges are utilized effectively.

Securing the IOT and OT Landscape. Large scale power grids, oil and gas refineries, transport systems, manufacturing plants etc. which are Cyber Physical Systems (CPS) heavily depend upon Operational Technology (OT) components like Supervisory Control and Data Acquisition (SCADA), Industrial Control Systems (ICS) or Distributed Control Systems (DCS) systems to monitor, control and operate their vast infrastructure. IoT devices are any smart device which can use the TCP IP protocol to connect to the network. OT and IoT devices are exceptionally OEM dependent with little information of their code and applications. Cyber Ranges can be

utilized to scan for vulnerabilities and threats in these devices. OT and IoT devices are connected directly to the range and a series of attack simulations are run past them to discover their attack surfaces and threat vectors.

Deter Lab. Deter Lab is a security test bed located at USC/ISI and UC Berkeley which is funded by National Science Foundation (NSF) and Dept. of Homeland Security (DHS) and was started in 2004. It is focused purely on cyber security experimentation and gives researchers exclusive access to multiple PCs and specialized hardware, running Operating Systems of their choice, with an array of security tools for conduct of various experimentation. A Cyber security lab based on the cyber range can also aid and fund researchers in various Indian Universities and provide a dynamic platform for conduct of critical research in the area of cyber security.

Availability of Data and Experiments. To perform suitable experiments we need both data and laboratory facilities that representatively scale to the complexity and vastness of cyber space. These are ongoing challenges. Access to data often is impeded by legal, policy and security concerns. However, there are examples of: Deter Lab (hosted by ISI, Marina del Rey, California) and the botnet laboratory at **École** Polytechnique de Montréal. There is also research into the generation of representative synthetic data since often at times data is not available due to proprietary or classification reasons.

Programming and Computing Resources. Significant programming and computing resources are required to effectively perform research and experimental development. Examples of required programming capability and computing resources include:-

- Shared state-of-the art computation systems.
- Highly capable systems with high performance I/O and extensive and high performance memory.

- Advances in embedded, distributed and parallel computing, including the ability to distribute analytics.
- The ability to scale up and to scale down capacity in support of experimentation.
- New architectures that respond to new programming and analysis techniques.
- Novel uses of Graphical Processing Units (GPUs) and Special Purpose Devices (SPDs).
- Near real time programming and computational methods that are responsive to the rapidly evolving threat space.

Critical Dependencies

Factors

US Federal Cyber security Research and Development Strategic Plan, National Science and Technology Council of February 2016 has identified that R& D on cyber security has to depend on the following factors**.**

Scientific Foundations. Cyber security involves hardware, software, networks, data, people and integration with the physical world in today's increasingly networked, distributed and asynchronous world. Cyber security needs sound mathematical and scientific foundations with clear objectives, comprehensive theories of defense, systems and adversaries, principled design methodologies, models of complex and dynamic systems at multiple scales and metrics for evaluating success or failure.

Risk Management. Risk management is the ongoing process of identifying, assessing and responding to risk. Advances in risk management are needed to achieve the R&D objectives. Integrated cost modeling techniques are needed that incorporate human factors and risk models that incorporate information about the known and projected vulnerabilities. [22]

Human Aspects. Experts estimate that 80-90 percent of current cyber security failures are due to human and organisational shortcomings. Research in this area is needed.

Transition to Practice. A gap exists between the research community and the operations community. Bridging this gap requires synergistic efforts and investments by both the R&D and operations communities. Government should allocate R&D funding to transition-to-practice activities, such as System Integrator Forums, Small Business Innovation Research (SBIR) activities and consortium ventures.

Workforce Development. Good research requires a good understanding of scientific inquiry and scientific methods. Knowledge of disciplines such as computing science, mathematics, engineering, psychology, sociology, economics is essential. Openness to multidisciplinary thinking would be beneficial.

Cyber security is a science which requires knowledge of operations research, cybernetics and game theory. Further areas of importance include trust, cryptography, model checking, obfuscation, machine learning and composition. Cyber security workforce development depends on cyber security researchers, cyber security professionals and product developers. The cyber security profession must attract and retain talent.

Research Infrastructure. Cyber security test beds are essential for the researchers for using actual operational data to model and conduct experiments on real world system vulnerabilities and exploitation scenarios. Researchers lack access to realistic social media and insider threat data to conduct human behaviour analyses to refine technical solutions and policies. The Government should promote the creation and uptake of world class test facilities, including data sets to allow the robust evaluation of new cyber security research and products. The Government, with industry

participation, should expand the scope of cyber security test beds in cloud computing, manufacturing, electrical power, transportation, information and networking systems, healthcare and telecommunications.

Roles and Responsibilities

Research and development funding is a scarce resource. Government is the primary source of funding for long term, high risk research initiatives. It also funds near term developmental work to meet department or agency specific requirements or important public goods that industry is not interested. Depending upon the agency, the research may be executed in house, at national laboratories, in academia, cooperative agreements or on contract basis. The challenge is: identifying and funding the most promising and important R&D initiatives and transitioning this research into practice. Near term, broadly applicable R&D is best done within private industry, as it is better positioned to shape and respond to market demands.

Cyber security is not just a problem of IT and telecommunications. Companies producing medical equipment, automotive systems and avionics sectors, banking, manufacturing, power and agriculture are equally affected.

Government Research Agencies. To perform long term high risk research government scientists, national laboratories and government funded Research and Development Centers are in a better position. These organisations perform research that is too sensitive or too risky for the private sector and are capable of doing this across multiple disciplines.

Academia and Research Organisations. Academia is the leading R&D performer of basic research and longer term, higher risk initiatives. It is the source for new ideas in cyber security. They produce research strategies, organize conferences and publish journals. Universities and their

technology transfer offices should focus on the volume of commercialisation opportunities, recognising the difficulty of predicting the success of cyber security initiatives and taking in to account broader benefits beyond the expected financial return.[23]

Private Sector. Even the largest IT companies the budgets for cyber security research is usually low. Private sector R&D funding typically is internal and focused on product development goals based on the specific needs of the company as well as on profitability and turnaround time. The R&D activities of the private and public sectors should be synergistic and complementary. Private and public sector R&D should mutually benefit from each other.

International Partners. India should leverage other countries' cyber security R&D investments and vice versa since cyber security is a global concern The government R&D community should have relationships with the private sector in areas such as cognitive systems, big data, social networking, privacy, cryptography, predictive analytics, search, cloud computing and software.

Coordination and Collaboration. Coordination and collaboration across sectors is essential to avoiding redundant research initiatives. This coordination should occur at several levels: among departments and agencies, government, private industry, academia and international partners.[24]

Ways of Working. The Government must respond to complex interdisciplinary cyber security research challenges. We must leverage external research capacity to address these challenges. Partnering is often a prerequisite for success. The Government should expand the engagement of SMEs and academic researchers with industrial partners through procurement mechanisms, including the Small Business Research Initiative

Academic, Private and Public Engagement. There are many models for successful partnering. The varying forms of partnership respond to varying objectives. While by no means exhaustive and somewhat overlapping, the following forms of partnership are used:-

- Centres of excellence.
- Meeting grounds.
- Virtual organisations.
- Consortia.
- Strategic networks.
- Incubators.
- For Profit.
- Not for Profit.

Implementation Roadmap

Developing Senior Leaders. It is inappropriate to leave the task up to experts and operational level staff because cyber security is not simply a technical issue. Senior leaders must:-

- Understand the cyber security related risks that must be assumed in conducting operations and the risks that an organisation must manage.
- Utilize and operational level staff experts to execute countermeasures and responses to incidents in the role of providing the support for risk management.

This would help the leaders to direct R&D efforts to most important areas.

Time. The acquisition process requires many time consuming tasks and

processes. The normal process of acquisition of technology would not suffice in the fast moving technical field like cyber. A fast track method must be made for R&D technology. It should not be difficult as other democratic countries face the same problem and are now overcoming the problem by some ingenuity and trust

Funding. Funding is critical for the development of indigenous cyber capabilities both defensive and deterrence/ offensive capabilities. This should be assured and the process must be different and fast for developing this niche technology.

Indian Perspective

India is one of the largest and fastest growing markets for digital consumers having 560 million internet subscribers in 2018. Indian mobile data users consume 8.3 gigabits (GB) of data each month on average. Indians have 1.2 billion mobile phone subscriptions and downloaded more than 12 billion apps in 2018. India has the second largest number of instant messaging service users worldwide. India is the most social media users. Aadhaar, India's unique digital identity programme, covers more than 1.2 billion people, the largest system of its type globally. The above figures are enough to justify huge investment in R&D efforts by India to indigenise and protect our cyber infrastructure and data.

Indian government's spending on R&D in terms of percentage of GDP has been stagnant at 0.6 to 0.7 per cent in the last two decades. This is much lower than the major nations such as the US (2.8), China (2.1), Israel (4.3) and Korea (4.2). R&D expenditure on cyber security is even lower. The present Government has taken some remarkable initiatives for R&D in the cyber domain. The major proposals are given below.

National Digital Communications Policy 2018.[25] National Digital

Communications Policy 2018 lays down the following for Research and Development:-

- Promoting research & development in Digital Communication Technologies by:-
- Restructuring Centre for Development of Telematics (C-DOT) as a premier Telecom Research and Development Centre for identification, customization and development of digital products and services in the country as per indigenous needs.
- Simplifying approvals/ processes for R&D procurements/ imports.
- Creating a framework for testing and certification of new products and services.
- Creating a Fund for R&D in new technologies for start-ups and entrepreneurs to enable innovation in cutting edge communications, 5G, software, content, security and related technologies and applications and commercialization of products and services through grants, scholarships, venture capital, etc.
- Establishing Centres of Excellence including in Spectrum Management, Telecom Security and Next Generation Access Technologies.
- Fostering an Intellectual Property Rights regime that promotes innovation by:-
- Implementing key recommendations in the National IPR Policy pertaining to Digital Communications, including a review of the legal regime around copyright, patents and trade marks.
- Assisting start-ups and other innovators in filing copyright, patent and trademarks applications.
- Providing financial incentives for the development of Standard Essential Patents (SEPs) in the field of digital communications technologies.

- Promoting Indian IPR through international collaborations and active participation in standard development processes and IPR related events.

- Simplifying the process of obtaining Experimental Licenses and establishing regulatory sandboxes like:-

- Enabling creation of suitable infrastructure for testing of new products and services with due regard to safety and security concerns.

- Facilitating allocation of spectrum for R&D and experimentation at affordable prices.

- Simplifying and fast-track approvals for products and services for experimental purposes through de-licensing and other mechanisms; and promoting establishment of test beds, incubators, innovation centres, etc. in collaboration with industry and academia.

Ministry of Electronics & Information Technology (MeitY). Ministry of Electronics & Information Technology, Cyber Security R&D Division had called for proposals under Cyber Security R&D Division. Research & development activities are promoted under this programme through grant-in-aid support to recognized autonomous R&D organisations and academic institutions proposing to undertake time bound projects in the thrust areas identified. The grants are given to autonomous R&D and academic organisations. Funds are provided for capital equipment, software, manpower recruited specifically for the project and reasonable institute overheads, consumables, travel and contingencies.[26]

List of Ongoing Projects are also given at https://meity.gov.in/content/list-ongoing-projects. There are number of projects which are of training in nature but have been funded under R&D. IT Minister Ravi Shankar Prasad at a cyber security event organised by industry chamber ASSOCHAM on August 30, 2017 announced that the government will fund research

and development costs of up to Rs 5 crore incurred by any company on developing an original cyber security product in the country.[27]

Department of Science and Technology: Government of India.[28] Department of Science and Technology, Government of India has identified the cyber security technologies for R&D. The details are available at http://dst.gov.in/basic-research-cyber-security.

Department of Science and Technology (DST), Government of India. The department has set aside a budget of Rs 3,660 crore to set up 20 physical cyber centers called hubs for research in future technologies. Each hub will have a distinct focus in areas of machine learning, sensors, internet of things. Some will be sector specific such as in agriculture, geo spatial technology and in technologies such as 5G, supercomputing, quantum sciences etc. This is a new model of doing research, where everything will be in one place. It will be overseen by same set of wise people who know what is worth researching. It will be like a mini-ministry that will be responsible for everything that happens in the country in that particular area. It will be an aggregator and custodian of the knowledge and activities in that area. The first hub is expected to be set up by the next financial year. Most of these will be located in R&D and academic institutes to leverage the knowledge and infrastructure that exists there.[29]

National Security Council Secretariat (NSCS)[30]. As per Hindu Business Line Report of January 16, 2018 it was announced that the central government is setting up a cyber security research and development fund of 1,000 crore to be spent over five years. It was decided that such an R&D programme can be operationalised and implemented by the National Security Council Secretariat (NSCS). The fund will be sourced from the annual budgets of the Department of Science and Technology (DST) under a separate head. The activities proposed to be covered under the programme

will include support for R&D projects, setting up centres of excellence, an inter-operability laboratory to test the developed hardware and software products, indigenisation of products and human resource development.[31]

State Government. In a welcome development the Government of Madhya Pradesh in its Cyber Security Policy 2017 has announced that it will facilitate to provide specific R&D grants to IT companies who are in cyber security domain in tune of 10% of overall R&D expenses of the company's Madhya Pradesh operations or INR 500,000 whichever is lesser. Other state governments may follow suit.

Problems of Indian ICT Industry for Promoting R&D

The Indian IT industry is doing very well and going up in the value chain. The Indian telecom industry is also growing rapidly. But excepting for a few banking and insurance products, India has not developed any great software solution. There is very little success in developing indigenous telecom products excepting the efforts made by companies like Tejas. Most designs have stayed as prototype and there is limited success in their commercialization. Thus India has made limited impact in Research and Development and continues to import all its Hardware.

Challenges

India faces number of challenges before becoming a hub for research and development and innovation. Some of these are enumerated below.

Inadequate Expenditure on R&D. Investments by Private industry in R&D have been far below public investments in India. The government is both the primary source of R&D funding as well as primary user of these funds. The Government should spend more in application oriented R&D aimed at problems specific to their needs.

Inadequate spending on R&D by industry and lack of long term strategy and high risk taking attitude by the Industry. The ratio of R&D funding by Government to that by private sector industry is approximately 70:30. R&D expenditure by ICT industry in cyber security needs to be increased drastically. In February 2018, Reuters reported that the Chinese telecom group of companies Huawei increased its annual spending on Research and Development (R&D) to between $15 billion and $20 billion as it races to be a global leader in 5G technology. About 80,000 of Huawei's employees or 45 per cent of its total workforce are engaged in R&D. The world's top R&D spenders, Amazon and Alphabet, spent $22.6 billion and $16.6 billion in 2017.The big Indian business houses simply prefer to remain in the 'service' field. China and Western companies will remain the leaders while India will have to buy their technologies, with all the risks involved. When the Indian behemoths post such healthy profit margins in their quarterly balance sheets, their lack of interest in investing in R&D defies logic. For national security purposes they may have to be goaded into investing in R&D for indigenization. Expenditure like Corporate Social Responsibility may be made compulsory for R&D in cyber security also.

Inadequate skilled manpower for R&D. Lack of quality in the engineering graduates is of a major concern. Though availability of them has increased manifold. The number of graduates going into M.Tech/ Ph.D programmes is quite low. There is a dearth of talent when it comes to specific niches, such as Cyber Security. R&D engineers to a large extent, do not find it a remunerating career because of great differential between their career prospects vis-à-vis the managers in the industry. R&D scientists and engineers have to be paid at par with the best paid in the industry.

The Riddle. India must reconcile the dichotomies in utilisation of the skilled manpower available within the country. R&D Centres of most of the high tech global companies are located in India because of India's

extremely talented human resources. There are over 1,250 MNCs with Global Capability Centres (GCC) in India now. India has by far the biggest presence of GCCs in the world. The market size in India for the MNC tech centres (GCC) touched $28.3 billion in 2018-19. More than 1 million people are now employed by the GCCs. They account for a quarter of the total workforce in the country's technical sector. Their average salaries are among the best in the sector. GCCs are now value creators. Most of the new GCCs in India and increasingly the older ones work in cutting edge areas like data analytics, AI, IoT, cloud and mobile technologies. Engineering, Research and Development (ER&D) centres do core engineering in areas like software, aerospace, telecom and automobiles. The technologies being developed in India are used for creating generic malware signatures, machine learning based security solutions, customer analytics, disease detection and connectivity platforms. In finance, they are leveraged for fraud detection, data analytics in cash management, chatbots, loan processing automation, insurance claims processing automation, payment analytics and treasury management.[32]

When so many of our own people are doing research and development work for MNCs in India, the some talent pool must be utilised for developing India solutions in Cyber domain in both hardware and software. The Bhava Atomic Research Centre (BARC) and Indian Space Research Organisation (ISRO) are shining examples what even in government sector can be achieved in development of niche technology completely indigenously. IIT graduates do not join them. It is the other Government engineering college graduates or students from ISRO's own colleges who do these research and developments. IIT students may become head of Microsoft or Google, but they become US citizens and look after US interests. They are not of any use to India. Bright young researchers from China join the best of educational and research labs in USA and after attaining prominence go back to China to boost up Chinese R&D efforts.

The talent is there. How do we utilise them in cyber security research and development efforts is the crux of the issue.

Inadequate infrastructure for incubation of technology. Unless R&D infrastructure is created for incubation of technologies, its deployment and pilot demonstration its commercialisation and mass deployment will not take place.

Collaboration between R&D, academic institutions and industry. There is no institutional mechanism available for taking up collaborative R&D projects by the R&D, academic institutions and industry. However, some beginning has been made.

IPR and TOT Issues. There is need to bring in changes in Intellectual Property Rights (IPR) policy defining the IPR and royalty sharing mechanism between developing institutions, inventors and the industry. The Transfer of Technology (TOT) policy should be put in place defining clearly the terms of TOT so that technology developed through government funding is transferred to interested industry well in time avoiding obsolescence.

R&D Fund Management change required in Rules for private funding. The private sector industry needs to be part and parcel of the entire R&D environment. In the existing system R&D funding by the government goes to government organisations. This should include private sector industry also. R&D is a risky job needs to be suitably factored in the relevant rules and regulations while drawing out safety checks for public funding. The relevant financial rules and audit mechanism may have to be re-looked by the Government.

Development and establishment of standards for emerging technologies. Deployment of technologies in field or its commercial exploitation very much depends on creation of standards.

Lack of mandatory standards for import of electronics and IT products. There is a need for bringing in mandatory standards and establish adequate test houses as per these standards. These mandatory standards are to be evolved in consultation with industry. For enforcement of these standards new testing centres will be required to be created or enhancement in the capabilities of existing testing centres would have to be done.

Incentives for using indigenously developed technology. Government should give incentives for deployment of solutions created using domestic technology. Most of the large-scale technology consumers of India including Indian defence, tend to procure technology from outside India through technology transfers. There are instances when genuine technologies produced in the country are made to face undue competition as the tenders are drafted demanding products tested as per some non-Indian standards.

Lack of national level architecture for Cyber Security. Critical infrastructure is owned by both public sector and private sector in India. However, there is no national security architecture that is able to assess the nature of any threat and tackle them effectively in a coordinated fashion unifying the efforts of the public and the private sector. [33]

Implementation Plan and Institutional Framework[34]

Recommendation for implementing plans and institutional frameworkare as discussed in succeeding paragraphs.

Strengthen/Create Schemes. The collaborative research involving academic/R&D institutions, industry and end users should be further strengthened. The support to incubating start-ups and SMEs is required to be further augmented.

Capacity Building. There is a need for creation of enabling R&D environment in Tier-II and Tier-III institutions and setting up of centres of excellence in identified areas in the country. New R&D infrastructure at Tier-II and III institutions needs to be created. Wider utilization of already existing centres and setting up of design studios is to be taken up.

Strengthen Linkages. Government support for pre-competitive research with academics-industry, enhancement of commercialisation of technologies, specific linkages of government with academics and industries is to be strengthened.

Testing and Certification. To address the growing concerns relating to Supply-Chain Vulnerability the following is recommended:-

- Establishment of National Testing and Certification Schemes, under the supervision and oversight of appropriate empowered entities.

- While action is underway for establishment of Telecom Testing and Certification Centre in telecom sector, there is a need for establishment of an independent government certification body for IT products under the MeitY. The certification body should be separate from the testing facilities. In the interim, Standardisation Testing and Quality Certification (STQC) may be authorized as certificate issuing body for IT products.

- Development of skills and competence of evaluators, validators and certification body personnel for successfully running the National Testing and Certification Scheme.

- Establishment of private owned testing labs, duly accredited by the certification body; Government may provide the necessary incentives for the private sector for opening testing labs.

- Encourage active participation in the communities of interest for defining protection profiles for addressing the security requirements of specific sector.

- Take necessary steps to transition from a 'Common Criteria Certificate Consuming Nation' to a 'Common Criteria Certificate Authorising Nation'.[35]

Centres of Excellence. Government should strengthen and support R&D Centres of Excellence with IPR and translational R&D focus. Government should provide funds for global patenting.

Support Entrepreneurship. Beginning has been made. It is required to set up focused program to provide seed and startup capital for ventures undertaking product development. Also setting up of Venture funds to fund start-ups beyond seed stage is required.

Encourage Made in India Goods. There is need to encourage use of Made in India goods in the country against the imported products.

Coordination. R&D activities have to be coordinated between various stakeholders. Initiatives have been taken by different ministries. These efforts need to be coordinated as meager resources of R&D fund has to be optimally utilised and there should be no overlap. Department of science and tech can support academic research. Similarly other stakeholders like MEITY, communication, commerce and banking services, respective ministries like power, aviation, transportation etc. can drive R&D in their respective sectors. This arrangement assures that the full spectrum of R&D approaches is represented and engaged. Since ministries operate in stove piped vertical systems without any horizontal overlap the best option is that the cyber security R&D should be overall coordinated by NSCS under National Cyber Security Coordinator. As a query it will be interesting to note, before funding the R&D efforts whether some coordination was carried out amongst the ministries by say Ministry of Science and Technology.

National Security Domain. In the national security domain the stakeholders are: armed forces, Defence Research and Development Organisation (DRDO), National Technical Research Organisation (NTRO), Research and Analysis Wing (R&AW), Ministry of Home Affairs (MHA) etc. Armed forces research organisations focus on their respective mission requirements. NTRO, intelligence agencies and MHA support applied research in the context of internal security and securing the Nation's critical infrastructures. DRDO can focus on high risk efforts that both prevent and create technical surprise. Cyber capabilities developed by armed forces/ cyber command must be integrated into a whole-of-government approach and integrated with private sector and coalition efforts to most effectively defend our collective interests. In earlier days military used to drive R&D, today it is other way round.

Organisations. Organisations within the cyber community offer the capabilities, resources and expertise to pursue and achieve cyber capabilities. Those critical to accomplishing the cyber end state are: Armed forces and defence laboratories, academia and commercial vendors in the defence industrial base. We should leverage commercial research whenever possible to reduce costs and increase capabilities. Collaborative innovation venues and processes will continue to evolve providing routine and frequent opportunities for the government, the armed forces and industry to work together to develop cyber capabilities. The armed forces facilitates adjustments in their Science and Technology community to keep pace with rapid evolution in the cyber domain. The armed forces must collaborate with the other stake holders.

R&D for Product Development and Cyber Weapons. India must concentrate in capability building for electronic combat as part of Information Warfare. Indian Armed Forces and intelligence agencies must have the latest means and capabilities for cyber defence, exploitation,

offence, technical intelligence, cyber deception and launching of probing attacks. They must develop cyber weapons both for causing disruption and destruction. India needs focused R&D in the development of safe products; discovery and analysis of vulnerabilities, fixing attribution, design of 'kill switches' and security patches; and creation and analysis of malware, production and delivery of cyber weapons.

The R&D activities are carried out by a number of agencies with varying missions but complementary roles. Among the agencies in India, for example, Department of Science and Technology supports academic research, DRDO under Ministry of Defence (MoD) focuses on high risk efforts that both prevent and create technical surprise, MoD Service research organisations focus on their respective mission requirements and Ministry of Home Affairs (MHA), MeitY and NTRO supports applied research in the context of internal security and securing the Nation's critical infrastructures. This arrangement assures that the full spectrum of R&D approaches is represented and engaged. The agencies should engage industry and academics through their respective departmental channels.

Development of Deterrence Capability. Though this is a highly classified domain, armed forces and intelligences agencies in close cooperation must develop these capabilities. These should be tested in peace time so that they can be employed during War. Some of the R& D projects as part of capability development may be:-

- How do you penetrate advisory's classified military networks.
- How to you isolate a built-up areas electronically and in cyber domain before carrying out any kinetic operation.
- What type of tasking be given to Special Forces operating deep inside enemy territory. Can they puncture enemy's optical fiber cable network and obtain data.

- Develop malware in pen drives to be inserted in enemy's classified network with the help of intelligence agencies so that information is sent back at appropriate time and in a way which is not detectable.

- Develop cyber exploits to be planted in enemy's key military infrastructure like telephone exchanges, main servers of classified networks, radar installations etc. This would explode electronically as per our timings to make them nonfunctional.

- How do we influence the mind of opposing operational and strategic commanders and leaders, specially for our Northern neighbours.

- What is the security of data link of our extremely costly airborne early warning and control system (AWAC) to the other flying aircrafts or to the bases. Getting a solution from Israel would not do. We must develop our own solutions for these highly classified links.

- Already there are Chinese network equipments in our highly classified network like the Air Force Net (AFNET). How do we mitigate this danger.

- How do we overcome electronic and cyber attacks by swarm of drones. Our Northern neighbours are adept at it.

- How to develop a malware which flown by a drone or UAV can fly into adversary's dense radar coverage, home onto the radar beam and insert the malware to make the Air Defence Command and Control Systems to malfunction, like in Operation ORCHARD.

There are many such applications that need to be developed during peace time. The military leaders must ask the right questions. Then only the technical experts will start thinking and come out with innovative solutions.

Summary of Recommendations

Funding

There has to be an assured funding for R&D in the cyber domain. Arrangements may be made to carry forward the budgetary allotment for the next year to maintain continuity and save time. The acquisition process for R&D efforts has to be streamlined and be different from normal procedures as time is at a premium and technology is niche. There has to be more trust between different stake holders. Not all R&D efforts will fructify and be successful. This has to be understood by the government funding and auditing agencies. Requirement of auditors cannot drive R&D programs.

Initially a lot of funds will be required for establishment of state of the art Labs, for example, detection of embedded hardware and software, micro electronic laboratories for development of own technology can be fabricated outside the country after due clearance till our own chip manufacturing facilities are developed. The concerned Labs of DRDO, CSIR, IITs, IISc and other academic institutions may be coopted for this effort. Defence Public Sector Undertakings (DPSU) also can play a part here. Armed Forces must establish their own Labs in niche technology fields to cater for their specific requirements.

Regrettably the private sector hardly funds any R&D efforts in cyber domain. We have large behemoths like TCS, InfoSys, Wipro and many others who are big players in IT field in the country and generate huge revenues. All the R&D efforts cannot be done by the government. Private sector has to contribute to this effort. Similarly DPSUs in their respective areas must spend on R&D efforts.

We have some wonderful talent for R&D in small and medium level enterprises. They must be brought into R&D ecosystem and should not be left behind under various elaborate processes and capital requirements.

Out of Box Thinking

There are two shining examples of our scientists and technologists developing completely indigenous solutions in niche technology arena: Bhabha Atomic Research Centre (BARC) and Indian Space Research Organisation (ISRO). In both the cases there was no bureaucratic control and the head of these organisations were given complete freedom. In cyber security research arena we can identify acknowledged specialists like, say, Prof Manindra Agrawal of IIT Kanpur and make him in charge of the development of cyber security technology development. There is no reason to believe that only bureaucrats understand national security. We may think of Cyber Commission on the lines of Atomic Energy Commission and Space Commission.

Talent Management

All the developed countries of the world are grappling with the problem of retaining skilled manpower in this field, specially in R&D, as the supply is far less than the demand. Government remunerations cannot match those of private industry. We can look at the various innovative actions taken by Western governments to attract and retain talent. We can make a program of catch them young, show them the laboratories, give them offer of continuity, motivate them with national feeling etc. These cyber professionals look forward to the working environment that are agile, multi-functional, dynamic, flexible and informal. These working conditions can easily be created. Most importantly, given the work requirements, these organisations must have leaders who not only share a competitive nature

and passion for technology, but also have a proven track record of thriving in dynamic, multi-functional settings.

Armed forces must identify talents who are very good in cyber field. Their talent should be nurtured and their career progression assured vis-à-vis their peers in the general field. There should be continuity of tenure, training and up skilling. Till such time a formal arrangement is in place selected personnel may be sent to countries like Israel, Japan, South Korea, Singapore, Estonia to learn from the best practices in the field for about six months to a year. These people then can utilise this knowledge in developing cyber power in our country. In the extremely sensitive technology areas only uniformed personnel would be allowed to operate. Their skill sets have to be continuously updated.

Israel the leading player in cyber field, utilizses the talent pool from their intelligence and military agencies to start cyber franchises that are world class. We must utilise similar talent pool from our security agencies for indigenous effects and start ups. The following must be considered:-

- Recruiting programs to ensure that the right human capital for the future is taken.
- Training and education programs to ensure that the human capital is ready for tomorrow's challenges.
- Talent management programs so that the right person in the right job at the right time is placed.
- Necessary incentives to ensure retention of the right talent.
- Learn from industry to address this challenge.

Development of indigenous Operating System, Search Engines, Network/ System Analysis Tools

For working in the classified network of armed forces some of the services is utilising indigenously developed operating system like Bharat Operating System Solutions (BOSS). China had started using Baidu as search engine and Kylin/Neo Kylin/UbantuKylin as the operating system. Seeing the market Microsoft has made Baidu as default browser for Windows 10 in China.[36]

While making an operating system is no big deal, maintaining them like issue of patches thwarting cyber attack etc. are difficult. Orgnisations like The Centre for Development of Advanced Computing (C-DAC) has developed operating system like Linux open source Bharat Operating System Solutions BOSS. Though the Linux based BOSS in more secure than Windows it has the disadvantage of user friendliness, non-availability of drivers, application and support system. Most computer malware are designed to attack Windows, the odds are considerably less for Linux to be infected with virus, spyware, Trojans and worms. Linux malware are few in member.

However, a huge support system in terms of resources and manpower are required to maintain the system 24 x 7. In present form C-DAC is in no position to do it. Even if it is outsourced to Indian Silicon Valley, it cannot match the might of Microsoft. If somebody finds a vulnerability to Windows and reports to Microsoft, they are handsomely paid. Zero day vulnerability has to be constantly sought and researched and patches updated immediately.

In the highly classified secured networks of Armed Forces, sophisticated technical attacks will be specific with difficult to detect processes. Idea of air gapped network is passé. It would boil down to how much effort and

adversary is willing to put to breach the gap. It is difficult to believe we have that sort of expertise and resources. How do you find out you are compromised if you don't open your system to public scrutiny. What is the time lag between reporting of a vulnerability and issue of a patch.

Before adapting the home grown operating system like Boss the various concerns of users have to be taken into account.

Supervisory Control and Data Acquisition (SCADA), Industrial Control Systems (ICS) or Distributed Control Systems (DCS) Systems

We do not have much of indigenous SCADA, ICS or DCS Systems. For securing critical infrastructure these must be made in India. Our industry should be able to develop these technologies.

Deter Laboratories. Specific Labs on the lines of Deter Labs in Collaboration with leading universities like Berkley must be established to carry out cyber security researches in near term. Research infrastructure in terms of test beds and other facilities should be created so that talented people from small and medium sectors can avail these facilities.

Forum for Discussion. Cyber security research community should have their own discussion forum like The Institution of Electronics and Telecommunication Engineers (IETE), Computer Society of India (CSI) etc. It can be a Society of Information Assurance where new ideas can be discussed and validated. A technical journal can be a part of this society where peer reviewed papers can be published.

Information Assurance College. MIT recently created A College of Artificial Intelligence. On similar lines a College of Information Assurance can be opened. This can be a part of National Defence University as and when it comes up.

Organisation. R&D in cyber domain would have two components. One in the civil domain looking into R&D requirements of cyber security in government and private sector arena. The other would be responsible for R&D specifically for the requirements of armed forces, their deterrence and offensive capabilities. There will be some overlaps which could be resolved through cooperation between the two agencies as well as intelligence agencies like NTRO.

Due to the sensitive and classified nature of operations some R&D efforts have to be strictly under government control. Organisations like DRDO have to take the lead into these efforts. Armed Forces may develop their own research organisations like US Army's Army Research Lab for the specific requirements of respective services. Developing organisations like Weapons and Electronics Systems Engineering Establishment (WESEE) by army and air force may be looked into.

It is for consideration if an "Inspector General Cyber Security" should be appointed with small team of experts like DASSI of the air force, to oversee cyber security of Platforms, and weapon systems during peace and field exercises.

Development of Crypt Analysis Capability. We do not have any capability to decrypt high grade crypts worth the name. It is becoming more difficult by the day. We must start the process of developing this capability. Cryptographers, mathematicians, analysts with the power of super computers must get together to get this capability. Collaboration with countries like Ukraine, Belarus, South Africa, Iran and Russia can be explored.

Use of Cyber Range. Cyber Range is a very potent system to impart high grade training as well as carry out deterrence activities. The cyber exercises that are carried out by NATO at Tallinn, Computer Emergency Readiness

Team (CERT) of USA and armed forces of USA should be looked into. Similar exercises should be carried out regularly. Professional expertise of existing Cyber Ranges must be utilized.

Forensic Labs for Embedded Hardware and Software. We are the biggest importer of military equipment of the world. All these have lot of electronics hardware and software components. There is always a chance of embedded hardware and software in these weapon platforms. While procuring, some legal and business clauses can be incorporated, but there is no getting away from having own testing facilities. This is extremely niche technology and costly, but needs to be developed.

Disaster Management. Armed forces must develop tactics, techniques and procedures to work under extreme adverse situations of non-availability of cyber and electromagnetic domain. The cyber resilience of their networks must be continuously improved. There should be no single point of failure. Same applies at national level specially for the critical infrastructures.

Kill Switch. Research should be conducted for both offensive and defensive aspects of Kill Switch.

De-anonymisation of Dark Net. Three leading universities of the world from USA, Israel and Russia through their research have been able to de-anonymise the Dark Net. Given the expertise available within the country we should also be able to do this provided focused efforts are put in place.

System Integration. We have a definite deficiency of good system integrators in the country. This capability should be developed.

Acquisition Process. Normal acquisition process should not apply for R & D related activities. The time required to acquire a particular technology must be short and processes less cumbersome.

Centralised Audit. There should be regular audit of platforms, weapons, systems and software to find vulnerabilities and how to close those. Self-certification will not suffice. Presently organisations under MoD and Intelligence agencies do not get audited. Similarly defence industrial base units must be audited as they will also be dealing with sensitive technology. Manufacturer must be made equal partner through well drawn contract and be responsible for availability of systems, regular inspection to look for malware and release of patches to nullify any vulnerability or accommodate change in technology.

Conclusion

India has no other choice but to develop and harness indigenous technologies in cyber domain. India has the capability but needs political support, enabling policies, financial backing and less bureaucratic control. India is a lead country in designing semi-conductor chips but lacks a foundry for in-house production.

India has to develop its own technologies, an electronic manufacturing base, R&D infrastructure and a highly skilled human resource. Being late has an advantage of 'leap ahead', but delays can have catastrophic consequences. There is a need to encourage our industry, provide at least a level playing field, encourage start-ups and Mico, Small and Medium Enterprises (MSME) and create a vibrant eco-system. The young extremely talented professionals available in the cyber eco system have to be brought in for research on indigenization of cyber technologies. The rules of the game, if needed to be changed, must be done. We cannot hide behind bureaucratic procedures.

A way has to be found to provide data to researchers specially in defence related domains. Without required data sets meaningful research in niche

technology areas will not be possible.

Though a little late, but given the required priority, funding and impetus India has the capability to develop indigenous technology in cyber domain. The Government of India has taken certain initiatives in the right direction.

Endnotes

1. Cyber Security in India, Opportunities for Dutch companies, Netherlands Business Support Office, Hyderabad, India, available at www.rvo.n
2. The Networking & Information technology Research & development program, Committee on Science & Technology Enterprise of the National Science & Technology Council, August 2018, Available at : https://www.nitrd.gov/pubs/FY2019-Cybersecurity-RD-Roadmap.pdf
3. Federal Cyber security Research and Development Strategic Plan, National Science and Technology Council, February 2016, available at : https://www.nitrd.gov/cybersecurity/publications/2016_Federal_Cybersecurity_Research_and_Development_Strategic_Plan.pdf
4. Cyber Security Research and Experimental Development Program, Issued by the Communications Security Establishment Canada (CSEC), 30 May 2013, available at : https://timreview.ca/sites/default/files/CraigenWalsh-Whyte2013_Cyber_Security_Research_and_Experimental_Development_Program.pdf
5. National Science & Technology Council Committee on Science & Technology Enterprise Subcommittee On Networking & Information Technology Research & Development,(NITRD), Supplement to the President's FY2019 Budget, August 2018, available at : https://www.nitrd.gov/pubs/FY2019-NITRD-Supplement.pdf
6. Analysis of the European R&D priorities in cyber security, European Union Agency For Network and Information Security, December 2018, available at :www.enisa.europa.eu
7. National Cyber security R&D Programme, The National Research Foundation (NRF), Singapore, available at : https://www.nrf.gov.sg/programmes/national-cybersecurity-r-d-programme

8. Federal Plan for Cyber Security and Information Assurance Research and Development, April 2006, available at :https://www.nitrd.gov/pubs/csia/csia_federal_plan.pdf

9. Lyu Jinghua, What Are China's Cyber Capabilities and Intentions? April 01, 2019, available at : https://carnegieendowment.org/2019/04/01/what-are-china-s-cyber-capabilities-and-intentions-pub-78734

10. Tai Ming Cheung, The Rise of China as a Cybersecurity Industrial Power: Principles, Drivers, Policies, and International Implications, September 2018, available at : https://basc.berkeley.edu/wp-content/uploads/2018/09/BWP18-03.pdf

11. Paul Triolo, Lorand Laskai, Graham Webster, and Katharin Tai, Xi Jinping Puts 'Indigenous Innovation' and 'Core Technologies' at the Center of Development Priorities May 1, 2018, available at : https://www.newamerica.org/cybersecurity-initiative/digichina/blog/xi-jinping-puts-indigenous-innovation-and-core-technologies-center-development-priorities/

12. The Networking & Information technology Research & development program, Committee on Science & Technology Enterprise of the National Science & Technology Council, August 2018, Available at : https://www.nitrd.gov/pubs/FY2019-Cybersecurity-RD-Roadmap.pdf

13. Source Roadmap for Photovoltaic Cyber Security - Scientific Figure on Research Gate. Available at : https://www.researchgate.net/figure/Thwarting-malicious-cyber-activities-by-strengthening-defensive-elements-through-R-D_fig6_322568290

14. https://www.researchgate.net/publication/327188download709_Foresight_of_cyber_security_threat _drivers_and_affecting_technologies/

15. Credible Cyber Deterrence in Armed Forces of India, Vivekananda International Foundation Task Force Report, March 2019, available at : https://www.vifindia.org/sites/default/files/Credible-Cyber-Deterrence-in-Armed-Forces-of-India_0.pdf

16. Progress and research in cybersecurity, Supporting a resilient and trustworthy system for the UK, The Royal Society, July 2016, available at : https://royalsociety.org/~/media/policy/projects/cybersecurity-research/cybersecurity-research-report.pdf

17. Dr. Hugh Thompson and Steve Trilling, Cyber Security Predictions: 2019 and Beyond, 28 November 2018, available at : https://www.symantec.com/blogs/feature-stories/cyber-security-predictions-2019-and-beyond

18. CIO&Leader, Key Cybersecurity Activities That Are Most Likely To Affect Organisations In 2019, Nov 30, 2018, available at : https://www.cioandleader.com/article/2018/11/30/key-cybersecurity-activities-are-most-likely-affect-organisations-2019

19. Meredydd Williams, Louise Axon, Jason R. C. Nurse and Sadie Creese, Future Scenarios and Challenges for Security and Privacy, Available at :https://arxiv.org/pdf/1807.05746.pdf

20. Kill switch, Available at : https://www.techopedia.com/definition/4001/kill-switch

21. Recommendations of Joint Working Group on Engagement with Private Sector on Cyber Security, National Security Council Secretariat, available at : https://cii.in/WebCMS/Upload/JWG%20report.pdf

22. Federal Cyber security Research and Development Strategic Plan, National Science and Technology Council, February 2016, available at : https://www.nitrd.gov/cybersecurity/publications/2016_Federal_Cybersecurity_Research_and_Development_Strategic_Plan.pdf

23. Ibid.

24. Ibid.

25. National Digital Communications Policy 2018, available at : http://dot.gov.in/sites/default/files/EnglishPolicy-NDCP.pdf

26. MEITY Ministry of Electronics & Information Technology, Government of India, available at : https://meity.gov.in/content/overview

27. Govt to fund R&D cost of up to Rs5 crore for original cyber security products, Livemint, 31 Aug 2017, Available at : https://www.livemint.com/Politics/iwcaInqqfYM5c7oEKc6llN/Govt-to-fund-RD-cost-of-up-to-Rs5-crore-for-original-cyber.html

28. Basic Research in Cyber Security, Department of Science and Technology, Available at : http://www.dst.gov.in/basic-research-cyber-security

29. SonalKhetarpal, Govt sets aside Rs 3,660 crore to set up 20 cyber centres, Business Today, January 22, 2019, available at : https://www.businesstoday.in/current/economy-politics/govt-sets-aside-rs-3660-crore-to-set-up-20-cyber-centers/story/312409.html

30. S Ronendra Singh, Govt to set up 1,000-cr cyber security R&D fund, available at : https://www.thehindubusinessline.com/money-and-banking/govt-to-set-up-1000cr-cyber-security-rampd-fund/article9258781.ece

31. India's R&D spend stagnant for 20 years at 0.7% of GDP, The Economic Times, JAN 29, 2018, Available at : https://economictimes.indiatimes.com/news/economy/finance/indias-rd-spend-stagnant-for-20-years-at-0-7-of-gdp/printarticle/62697271.cms

32. Shilpa Phadnis, Sujit John, MNC tech hubs' business in India grows to $28 billion: Report, The Times of India, 16 May 2019, available at : http://timesofindia.indiatimes.com/articleshow/69350843.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst

33. Cyber Security in India, Opportunities for Dutch companies, Netherlands Business Support Office, Hyderabad, India available at www.rvo.n

34. Report of the Working Group on Information Technology Sector Twelfth Five Year Plan (2012 – 17), Government of India, Ministry of Communications & Information Technology, Department of Information Technology, available at : http://planningcommission.gov.in/aboutus/committee/wrkgrp12/cit/wgrep_dit.pdf

35. Recommendations of Joint Working Group on Engagement with Private Sector on Cyber Security, National Security Council Secretariat, available at : https://cii.in/WebCMS/Upload/JWG%20report.pdf

36. BOSS Linux and variants, Centre for Development of Advanced Computing (C-DAC), available at : https://www.cdac.in/index.aspx?id=st_pr_Boss_gnu_linuxb

37. Credible Cyber Deterrence in Armed Forces of India, Vivekananda International Foundation Task Force Report, March 2019, available at : https://www.vifindia.org/sites/default/files/Credible-Cyber-Deterrence-in-Armed-Forces-of-India_0.pdf

About the VIVEKANANDA INTERNATIONAL FOUNDATION

The Vivekananda International Foundation is an independent non-partisan institution that conducts research and analysis on domestic and international issues, and offers a platform for dialogue and conflict resolution. Some of India's leading practitioners from the fields of security, military, diplomacy, government, academia and media have come together to generate ideas and stimulate action on national security issues.

The defining feature of VIF lies in its provision of core institutional support which enables the organisation to be flexible in its approach and proactive in changing circumstances, with a long-term focus on India's strategic, developmental and civilisational interests. The VIF aims to channelise fresh insights and decades of experience harnessed from its faculty into fostering actionable ideas for the nation's stakeholders.

Since its inception, VIF has pursued quality research and scholarship and made efforts to highlight issues in governance, and strengthen national security. This is being actualised through numerous activities like seminars, round tables, interactive dialogues, Vimarsh (public discourse), conferences and briefings. The publications of VIF form lasting deliverables of VIF's aspiration to impact on the prevailing discourse on issues concerning India's national interest.

VIVEKANANDA INTERNATIONAL FOUNDATION
3, San Martin Marg, Chanakyapuri, New Delhi – 110021
Phone: +91-11-24121764, 24106698
Email: info@vifindia.org,
Website: https://www.vifindia.org
Follow us on twitter@vifindia