Vivekananda International Foundation

Cyber Security

Fundamental to India's Sovereignty

Lt General Davinder Kumar, PVSM, VSM Bar, ADC

VIF Brief - October 2018

About the Author

Lieutenant General Davinder Kumar retired as the Signal Officer-in-Chief of Indian Army after distinguished service of 41 years. An expert in telecommunication networks, Information Warfare and Space systems, he was the CEO and MD of Tata Advanced Systems and was on the Board of Directors of both Public sector and Private companies. He has published more than 400 papers and spoken at various fora in India and abroad.

Cyber Security:
Fundamental to India's Sovereignty

Cyber security is the single largest concern for nations and societies today as they move from agro-industrial age to the Information Age. It is paradoxical that while information and communication technologies (ICT) are at the heart of all facets of human life and are central to national, economic and human security, the level of their penetration creates certain vulnerabilities. These are then exploited by individuals, industry, state and non-state actors who pose direct threat to nations and societies that are transiting to digitisation and digital economies and those that are digitised already.

The threats are present 24/7 across the full spectrum, from: Cyber-crime to cyber espionage to cyber terrorism; social engineering; and even cyber warfare. The threat landscape is dynamic, evolving rapidly in consonance with, and sometimes, even ahead of technological developments. These threats get accentuated by the unique characteristics of cyber space which is expanding constantly, becoming increasingly vulnerable, and hosting ever growing vast amounts of data. Ironically, with easy access to technology, the low costs and threshold of the expertise required, the number of bad actors seeking to exploit cyber space for criminal or malicious purposes is growing too. Training for malicious hacking can be acquired easily, and for free, on line on sites like YouTube that one probably visits a few times a week. In fact, today the tools for bad actors in cyberspace are, quite literally, "commodities" and are being bought and sold accordingly. For example, cyber criminals sold the login credentials for Facebook in bulk, quite recently[1].

The threat landscape must be analysed carefully –- we now have everything from individual hackers, to hacktivists, to basic cyber criminals to organised crime groups, non-state actors, all the way up to state sponsored attacks. Experts agree that the coming years will see more activity in the so-called 'dark nets' and greater use of crypto-currencies; that the ability to stage cyberattacks will continue to outpace the ability to defend against them; and that there will be more "hacking for hire" as seen in the recent Distributed Denial-of-Service, or DDOS, attack, said to be the biggest and longest lasting in the world. Furthermore, lot of work is being done in the field of Automatic Exploit Generation (AEG), a body of research that deals with the ability to generate a successful computer attack with reduced or entirely without human interaction.[2]

As nations, societies and individuals transit to a digital world and the consequent increased connectivity, cyber space too will expand exponentially along with the corresponding increase in vulnerabilities. The following trends are likely to persist in the cyber space:-[3]

- Shift to digitised information (voice, video and data) and the hosting of increasingly vast amounts of (sometimes critical) data;
- Miniaturisation of computing and data-storage devices that carry digitised information;
- An explosion of increasingly networked digital devices coupled with low costs;
- Continued growth in wired and wireless networks and electronic systems with increased connectivity for accessing the Internet;
- Accelerated deployment of secure digital control systems that operate physical systems, from cars to aircraft, home thermostats to power grids and so on;
- Continuous and exponential growth of the hacking community with greater abilities, reach and demand amongst governments, intelligence organisations and the corporate world;
- Increasing popularity of online media and social networking, which, according to one study, has led some people to spend more time each day on their phones or laptops (an average of 8 hours and 41 minutes) than in sleeping!;
- Lower costs, increasing speeds and the standardisation of inter-operative electronic systems, not only make these systems more accessible to everyone but also increase the potential for exploitation.

The recent Ransomware attacks by Petaya, NotPetaya and Wannacry malware, have shown the immense power and exceptional reach of cyber-attacks and have unambiguously shown that a cyber-attack is truly a 'Weapon of Mass Disruption'. It affected hundreds of thousands computers across various sectors including health, finance, transport, ports and so on, in 150 countries! Another, major cyber-attack on HBO took a long time to resolve with the hackers demanding 2.5 million in Bitcoins[4]. Threats of this magnitude require international co-operation by way of shared information, intelligence and technology, backed by a responsive legal system. Notwithstanding that, each nation will have to develop its own doctrine for cyber security and the corresponding strategies to deal with the threats both proactively, and as they happen. Given the broad spectrum and the wide disparities in the way the threats are handled and resolved, the common and essential requirement will be "synergy" through information sharing, collaboration and unity of effort by all agencies and stakeholders.

The Indian Scene

India is very vulnerable to cyber interventions due to certain strategic deficiencies, its fast developing economy, inadequate appreciation of the threats and the rather tardy and disjointed implementation of policies. India was one of the handful of nations to promulgate the Information Technology Act in 2000 as a legal policy document to deal with cyber interventions. The same was revised in 2008. Similarly, the National Policy on Electronics was formulated in 2012 and the National Cyber Security Policy in 2013. Yet, co-ordinated and focused efforts towards ensuring cyber security were missing till a few years ago except for the establishment of Computer Emergency Response Team – India (CERT-In) - and similar organisations at the state level and for the defence forces.

India's cyber security chief Gulshan Rai told the Parliament's finance standing committee in July 2017, that cyber threats had evolved swiftly from the viruses and 'nuisance' attacks of the early 2000s to sophisticated malware and the advanced denial of service. These could become severely destructive attacks by 2020. India will face increasingly sophisticated *destructive* cyber threats as compared to the *disruptive* attacks that are currently adding up to 200 million malware-related and 190,000 'unique' intrusions in any given week. The Government - at Centre and State levels — is the main target of cyber-attacks. These are driven by motives ranging from theft, espionage and data extraction to counterfeiting. In 2015 and 2016, the government sector accounted for 27 percent and 29 percent of all cyber-attacks respectively. Other sectors high on the priority list of cyber criminals are banking, energy, telecom and defence, which along with the government, account for three-fourths of all cyber-attacks. Emergence of new services, applications (apps), cloud and cognitive technologies have made cyber security more challenging, even as the value of data and its applications in commerce is growing by the day, thus making cyber security a critical element of national security. The numbers of e-transactions are also rising, with India logging in an estimated two billion such dealings a day, as compared to around 54 billion worldwide, according to World Payments Report 2016.

Cyber-attacks use techniques and tools that help criminals evade detection with increasing refinement, and this has led the government to recognise cyber security as a 'strategic domain' that has a direct impact on our national sovereignty and therefore devise strategies for deepening cooperation at the international level. Accordingly, the Prime Minister's Office and the National Security Council are overseeing a range of civilian and defence agencies with cyber security mandates.

Threat Landscape

India has fallen victim to a staggering 144,496 cyber-attacks in last three years. The data was tabulated by the Indian Parliament. According to the CERT division of India, as many as 44,679 cyberattacks were reported in 2014. By 2015, the number reached 49,455, and by 2016, the number had crossed the 50,000 mark[5]. India is third among list of countries where most of the threats were detected and it is second in terms of targeted attacks. Symantec detected 133 targeted attacks in India which were the work of organised groups. The majority of these groups are state sponsored - although there are a small number of private operators - and they are usually driven by motives like intelligence gathering, disruption, sabotage, or financial. Broadly speaking, targeted attacks correspond to espionage, although the lines are starting to blur.[6] India was ranked second globally on incidents of spam and phishing (misleading emails, web link etc.). Complex cyber-attacks - ransomware and network attacks - in India increased in terms of the global percentage. Citing his concerns regarding the upward trend, Home Minister Rajnath Singh reviewed the several measures and steps taken by the Government to avert cyber incidents. He also extended his support for strengthening the surveillance and legal framework of the country and exploring methods to deal with financial frauds. This comes at a time when the country becoming a cashless economy. One of the steps the Government plans to take is deploying big data analysis developed by Indian Institute of Technology (IIT) Delhi for identifying the attackers. The move aims to prevent duplication of e-wallets and to keep the customers updated through SMS and email alerts.[7]

The alert mechanism will, according to a PTI report, include the names of the beneficiaries of any financial transaction, wherever necessary for better traceability and cross-checking on the part of the victim, publishing online statistics depicting the specific incidents, frauds against e-wallet companies and banks along with details including investigation, to enable customers to make an informed choice before subscribing to e-wallet services are other initiatives being planned. To keep a tab on phone frauds, the Government recently constituted the Inter-Ministerial Committee on Phone Frauds (IMCPF). The home minister directed his department to analyse and study relevant regional case studies and also examine the issues in consultation with key stakeholders [7.]

From leaking debit card details to influencing the US presidential election, cyber-attacks have become a significant part of our political and social discourse. The exponential rise of *cyber power* in a short span of four decades is both amazing and mind boggling. From cyber-crimes to cyber espionage to cyber terrorism to social engineering to cyber war and now a cognitive dimension for managing human behaviour. There have been substantial improvements in each of these capabilities over the years by way of people, processes, complexity and technology.

Cyber crimes

Cyber crimes pose a real threat today and are rising very rapidly both in intensity and complexity with the spread of internet and smart phones. As dismal as it may sound, cyber crime is outpacing cyber security. About 80 percent of cyber attacks are related to cyber crimes. More importantly, cyber crimes have changed the nature of conflict by blurring the line between state and non-state actors. Cyber crimes are likely to increase exponentially with the fielding of virtual currency, the Internet of Things, big data, cloud technology, drones, robotics, block chain and so on. More severe crimes would be the coin mining as an alternate source of income, spike in supply chain attacks, ransomware attacks and mobile malware. Capabilities of hijacking a car, taking over the controls of an aircraft, cyber murder and remote injunction of viruses through drones and aircraft have already been demonstrated and in some cases, commercialised. The Darknet and the Deepweb are already being exploited for sale of vulnerabilities, weapons, recruitment of people in terrorist groups, drugs and so on. The recent disturbing trends are the emergence of 'crime as a service' (CaaS) and use of robots for cyber crime [7].

One of the biggest cyber-attacks in 2016 was the hacking of Indian debit cards wherein as many as 32 lakh debit cards, belonging to various Indian banks, were compromised resulting in substantial financial loss, following fraudulent transactions as per the National Payments Corporation of India (NPCI). The infamous hacker group "Legion Crew" made headlines in the sub-continent after hacking into the Twitter accounts and partial email dumps, of prominent public figures such as politician Rahul Gandhi, businessman Vijay Mallya, and NDTV journalists Barkha Dutt and Ravish Kumar.

Cyber Espionage

The internet has become a very powerful source for intelligence collection in support of national, diplomatic, military, technology or economic objectives. It is estimated that more than 90 per cent of open source intelligence is being obtained from the cyber world. It is economical and safe. Cyber espionage is also being used for technology theft and for launching probe missions on the critical infrastructure for possible exploitation later. The fact that attack vectors for cyber espionage and cyber war are the same, make cyber espionage a major threat. The recently alleged interference by Russia in the democratic elections in France and the USA and its continued cyber interventions in the Ukraine add yet another dimension to the threat landscape and cyber intelligence.

Cyber Terrorism

Coincidence between the physical and virtual worlds, as demonstrated by the STUXNET attack on Iran's nuclear facility at Natanz in 2010, has put the complete information infrastructure at risk. Targeted attacks on a nation's critical infrastructure like military installations, power plants, air traffic control, surface transport traffic control, telecommunication networks would be considered as a part of cyber terrorism. These are low level, 'short of war' attacks which would cripple parts of a critical infrastructure or adversely affect the functioning of a business. These attacks are not large enough to warrant a military response, but have the potential to inflict enough damage. Numerous attacks over a long period of time could harm the economy, complicating a policymaker's calculus for determining an appropriate response.

Social Media

Social media like Facebook, Twitter, and LinkedIn have emerged as powerful tools for perception management, social engineering, cyber-crimes and intelligence. They have also emerged as major instruments for waging asymmetric warfare through exploitation of the aspirations of people, differential development, varying religious beliefs and cultural leanings. These have also become attractive vehicles for recruitment and radicalisation by the terrorist organisations. Nations across the world are putting in place legal frame works, infrastructure and human resources for monitoring this media to remain proactive. The major issue being privacy vs individual and national security.

Cyber Warfare

It is universally acknowledged that a 21st century war will be highly cyber-centric if not fully led by the cyber theatre. Glimpses of these have been seen in the Russian assault on Estonia and Ukraine. While in Estonia it was pure cyber intervention, in the Ukraine it was a combination of cyber and kinetic attacks, wherein the bits preceded the bullets. This operation is a landmark in cyber enabled warfare. Nations across the world have pronounced their doctrines of cyber warfare, have set up organisations to conduct cyber warfare and are busily making and testing cyber weapons. USA is reported to have used 'logic bombs' in Afghanistan and Syria to effectively neutralise their opponent's communication networks.

Cyber Security Architecture

India is setting up its own 'cyber security architecture' that will comprise: The National Cyber Coordination Centre (NCCC) for threat assessment and information sharing among stakeholders; the Cyber Operation Centre that will be jointly run by the National Technical Research Organisation (NTRO) and the armed forces for threat management and mitigation for identified critical sectors and defence respectively; and the National Critical Information Infrastructure Protection Centre (NCIIPC) to be set up under the NTRO for providing cover to 'critical information infrastructure'. A Central Monitoring System for electronic surveillance will remain proactive against any social engineering efforts by persons or organisations inimical to India[8].

The Government is creating a legal framework to deal with cyber security. It has also launched a drive for creating greater awareness of this threat and training the necessary human resource with requisite skills.

Crisis Management Plan

India has prepared a Crisis Management Plan (CMP) for countering cyber attacks and cyber terrorism for preventing the large scale disruption in the functioning of critical information systems of the government, public and private sector resources and services. The CMP outlines a framework for dealing with cyber related incidents for rapid identification, swift response and remedial action to mitigate and recover from cyber related incidents impacting critical national processes.

Above efforts are aligned towards developing a cyber defence capability. There is no information in the open domain regarding the development of cyber offensive capabilities and their integration. Cyber space is essentially offence dominant by its very character, and cyber power includes both defensive and offensive capabilities backed by appropriate organisation, technology, skilled human resources and a well-developed defence electronic manufacturing and components base. It is on these that we have to lay strong and urgent emphasis. While we must applaud these efforts, it must be noted that we have a long way to go in terms of ensuring our 'technical sovereignty' and evolve a holistic systems approach to realise an indigenous eco-system to ensure full spectrum cyber security that is fundamental for a nation's and individual's security.

For India to develop cyber power commensurate with her geo-political status and security requirements, certain imperatives must be attended to and implemented in the next two to three years. This is because, in all likelihood, the strategic window of opportunity would close by then purely due to the yawning gap vis-a-vis our likely adversary who is decades ahead and is recognised as a major cyber power.

What India Must Do - Now Establish National Cyber Security Commission (NCSC)

NCSC should be a fully empowered body with its own department, on the lines of the Space Commission and the Atomic Energy Commission. The country needs to build thought leadership and weave together India's potential to create cyber power across the spectrum under one organisation, empowered appropriately, with complete responsibility, accountability and budgetary support.

The NCSC will have the onerous tasks of creating synergy amongst various stakeholders through: An enabling policy and legal framework; developing technology, and centres of excellence; skilled manpower with flexible, progressive and innovative employment rules and facilities; a separate cadre for cyber professionals; crowd sourcing; industry clusters for manufacturing secure products; education curricula; standards and certification; intelligence and counter intelligence mechanisms; cyber forensics; security standards; cryptography; language experts; and policy research. It will form Integrated Cyber Security Teams capable of providing full spectrum capabilities, conduct periodic audits to ascertain the readiness for both the present and likely threats, and coordinate with all Ministries and States for protection of the National Critical Information Infrastructure (NCII) in their jurisdiction.

Policy Revision

The National Electronics Policy was promulgated in 2012 and the National Cyber Security Policy in 2013. Besides tardy implementation, there is a complete disconnect among these policies in so far as cyber security requirements are concerned. Absence of a National Data Security Policy is a strategic gap that needs to be bridged immediately. All these policies need to be revisited urgently - and thereafter periodically - and integrated for capability development to cater for emerging technologies and their rapid pace of application and a very dynamic threat scenario. The revised and integrated policies then should be translated into a time bound National Cyber Security Action Plan in consonance with the national cyber security doctrine and be duly approved by the Cabinet Committee on Security and the Parliament.

Develop Cyber War Capability

India urgently needs to develop policies and capabilities in this Fifth Domain of warfare. These cannot wait and must be taken up on top most priority in a mission mode by the Services. The situation and threats to India are unique and hence it is necessary to develop indigenous solution in consonance with the doctrine. Development and operationalisation of information and electronic capabilities would not only add to the operational capabilities of our armed forces for digital warfare of the 21st century but would aid in making them 'lean and mean' as was desired in the first meeting of the newly created Defence Planning Committee.

Cyber space is an integrated civilian and military domain. Military forces must collaborate with civilian owned, managed and operated cyber space elements in order to achieve desired effects. This interaction blurs the lines of when military actions begin and end compared to those of civilian organisations and their personnel.

Create Awareness of Cyber Threats and Cyber Security amongst the Masses

All government offices and establishments, industry and business houses must hold periodic briefings and daily physical checks on cyber security. Norms of behaviour in cyber space and adherence to good practices must be given top priority. Cyber threats, precautions, best practices and security measures should be highlighted periodically by the leaders, management and through print and electronic media. All citizens and establishments must be made aware of the absolute necessity of incidence reporting, and that the failure to do so would invite legal action. Government may consider promulgation of 'Cyber Security Information Sharing Act'.

Energise the 'Make in India' Programme and Hire a Foundry Abroad

Absence of an electronic manufacturing base and indigenous semi-conductor production facilities in the country are strategic deficiencies. These are absolutely essential and fundamental pre-requisites for cyber security and need immediate attention at the highest level. These deficiencies were to be addressed by the National Electronic Policy (NEP) - 2012. As per this policy, India was to establish an Electronic System Design and Manufacturing (ESDM) eco-system and facilities for manufacturing semi-conductors in the country. Unfortunately, the scheme did not take off in spite of the fact that it offered attractive financial and taxation terms. The policy needs to be revised under the Make in India programme and made more attractive for people ready to invest. Given the fact that semi-conductor chips manufacturing foundries are very capital intensive with still longer gestation periods, it may be a good idea to hire facilities abroad, in the interim. That would compress the time frame for development of skills and be cost effective, as we concurrently establish own facilities. This approach would mitigate the risks of supply chain vulnerabilities to a large extent.

Cyber Policy Research Centre

There is no think tank that is studying and analysing policies and documents being produced by groupings of governments, industry, civil society, academia, interested organisations and international policy making organisations. Thousands of pages that are being churned out require deeper understanding through analysis and discussions, to decide on what is in India's best interests. We are unable to address policy, as well as, operational issues due to the lack of focused studies. Numerous Non-Government Organisations (NGO) created at the behest of foreign governments are obfuscating policy discussions to derail national positions. These attempts have to be dealt with both proactively and aggressively. We are the second largest users of, both the internet and mobile phones, in the world and present a very big market. We must ensure that India's voice is not only heard but that no policy detrimental to India is passed. The research facility would make the appropriate expertise available, particularly, when a large volume of cyber security research and policies require timely revision, as the technology evolves,

Cyber Threat Intelligence Centre

India needs to create cyber threat analysis centres which would collect, analyse and share the attack data on infrastructure, financial systems, websites and services. It would also correlate 'big data' generated from the government with financial and commercial data to create patterns and identify anomalies for advance preventive actions.

Cyber Workforce Development

This is perhaps the biggest challenge requiring an out of box, liberal, flexible and innovative approach. The private sector, service providers, academia and government together have to very urgently take on this responsibility. The National Skill Development Plan would act both as a catalyst and facilitator for the development of a cyber security work force with different skills, the associated training infrastructure and faculty. The system should be oriented towards the younger generation and resources like the National and Auxiliary Cadet Corps, and national service should be given priority. Talent search through crowd sourcing and Indian diaspora must be encouraged and formalised. The Government must announce the creation of a cyber security cadre to enable openings for employment and pursuing cyber security as a career.

R&D for Product Development

India needs focused R&D for the development of safe products for: Discovery and analysis of vulnerabilities; fixing attribution; design of 'kill switches' and security patches; creation and analysis of malware; production and delivery of cyber weapons. Effort should concentrate on capability building for electronic combat. The manufacture and export of cyber security products offers a very attractive opportunity for India. Indian Industry can leap ahead and straight away focus on the R&D and manufacture of secure products including industrial control systems. Revised National Electronic Policy must include this provision along with the means to make it attractive with least risk.

Security Standards, Frameworks, Audit

India needs to develop and promulgate her own cyber security standards and frameworks for development and audit processes for protection of our NCII. Enabling policy measures are required to encourage the establishment of testing labs for managing ICT Supply Chain Risks. It is for consideration that the service providers and original equipment manufacturers are mandated to establish the testing labs, be made responsible for the assured grade of service mutually agreed to in the contract and cyber insurance to cover the risk.

Cyber-crime Investigation

Given the ever expanding proliferation of devices, platforms, big data, the Internet of Things, mobility and social media, there is an urgent need for development and continual upgradation of cyber forensics capabilities and investigating skills of our law enforcement agencies (LEAs), to enable them to handle cyber crimes. A committee headed by Gulshan Rai, National Cyber Security Coordinator, has submitted a 'Roadmap for Effectively Tackling Cyber Crimes in the Country' to the home ministry. This Committee has made some important recommendations which need to be actioned by a dedicated team within the stipulated time frame. Some important recommendations are:- [9]

- Establish a new Indian Cyber Crime Coordination Centre and link the same with the NATGRID (National Intelligence Grid) and CCTNS (Crime and Criminal Tracking Network System) and their branches in states to curb the cybercrime. The centre would check attempts of international gangs to penetrate the Indian government official communication network.

- Devise an advance application for social media analytics to monitor the social media platform activities related to ministries of home, external affairs, defence and other government organisations.
- Reduce the government's dependence on foreign servers and ensure one dedicated secure gateway for all government communication.
- Set up a separate agency for online cyber crime registration, monitoring and integration of CCTNS data with the same.
- Amend the Evidence Act to suit the current requirements for prosecuting cyber crimes.
- Sensitise the states by setting up cyber forensic laboratories in states along with holding workshops and international cooperation.

Assurance Framework, Test and Certification

There is an immediate requirement for the setting up of a national cyber test facility providing for network emulation, monitoring and audit, vulnerability analysis, simulated attacks, graduated response, performance analysis and security assurance modelling.

Build Thought Leadership, Executive and Political Sponsors

Develop a cyber security savvy leadership, subject matter experts, solution architects and system engineers so as to address the inadequate cyber security capabilities and their impact on national security including, the military dimension.

Leveraging the Diaspora

The Indian diaspora is at the fore front of developing security technologies, platforms and solutions across world class institutions and industry in the USA and Europe. They can be the biggest catalyst for the creation of cyber security capabilities. Proactive and aggressive steps should be taken to leverage the diaspora.

Outreach Programme to Attract Industry

Both the Government and industry must recognise the absolute necessity of investing in cyber security and risk management while concurrently exploring the huge business opportunity for exporting cyber security related products and services and cash in on this by adopting a focused and proactive approach as was done for IT. The Government needs to make it attractive for the private sector to invest in capability building through innovative mechanisms and an enabling legal and policy framework.

An Agency for Information Management and Assurance

India is very vulnerable to social engineering, fake news and propaganda that creates the perception of a possible failure of governance and chaos. Our likely adversaries have, and continue to exercise these capabilities on an almost daily basis. There is an urgent need to counter this threat on a real time basis in view of the tremendous speed of the electronic and social media. India needs an Information Management Agency to proactively counter these threats by analysing the contents and launching counter-offensives. This agency would also be responsible for creation of content for our possible offensive.

International Cooperation

In this digitally inter-connected world with over six billion connected people and devices, new threats that have a direct impact on the security and privacy of people are emerging every minute. Consequently, cyber security has become the single most necessary capability and constitutional responsibility for nations. Due to its ubiquitous nature and application in all facets of our existence, it has become a measure of a nation's sovereignty and degree of freedom of navigation in the cyber space. Essentially, it means ensuring the availability of cyber space, a global domain, to nations, societies, industry and people to conduct their respective affairs with complete freedom.

In the 21st century global economy, cyber space is perhaps the single most important factor that links all the players together, boosts productivity, opens new markets and enables management structures that are flatter, and yet have a far more extensive reach. No nation can ensure cyber security on its own. It has to be a combined effort that warrants international cooperation. India must continue to enter into bilateral, regional and multilateral agreements to share: The threat perspective; risk assessment; technology; conduct of joint training; and research. India, should also form an advocacy groups to ensure that our national security, as well as her views are respected in internet governance.[10]

Development of a full spectrum cyber security eco-system and its integration with other instruments of power has become a strategic imperative for ensuring national sovereignty in this Information Age. There is already a debate on the necessity of developing cyber deterrence while many nations are already busy in developing such capabilities. India must not miss the train as she did in the nuclear field. Immediate action as per the National Cyber Security Development Plan mentioned in this paper, must begin with an empowered, dedicated organisation and assured budgetary support. It has to be a national effort, a dynamic process that will remain a work in progress in view of constantly evolving threats and technology. Let us, together, make India a global cyber power with full spectrum cyber security capability and an eco-system commensurate with her status in the comity of nations.

We can and we must.

End Notes:

1. Emerging Cyber Threats and Implications - RAND Corporation https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/.../ RAND_CT453.pdf by IR Porche III - 2016.

2. Automatic Exploit Generation – CanSecWest https:// cansecwest.com/slides/.../ CSW2016_DAntoine_AutomaticExploitGeneration.pd

3. Emerging Cyber Threats and Implications - RAND Corporationhttps://www.rand.org/content/dam/rand/pubs/ testimonies/CT400/.../RAND_CT453.pdf by IR Porche III - 20

4. The top 10 worst ransomware attacks of 2017 – TechRepublic https://www.techrepublic.com/.../the-top-10-worst-ransomware-attacks-of-2017-so-far.

5. 1,44,496 cyber attacks in India in the last three years - CISO Mag https://www.cisomag.com › Threats Nov 15, 2017.

6. India ranks 3rd among nations facing most cyber threats: Symantec PTI April 04, 2018.

7. Internet Security Threat Report.

8. Cyber Security Status And Challenges, Monograph by Lt Gen Davinder Kumar VIF.

9. Key Recommendations of Gulshan Rai Committee on Cybersecurity… https://www. gktoday.in/.../key-recommendations-of-gulshan-rai-committee-on-cybers... Oct 5, 2015.

10. India's Cyber Security Architecture and Imperatives, Lt Gen Davinder Kumar, India Foundation, September 2017.

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