Committed To Defence And Security Worldwide

DEFENCE & SECURITY ALERT

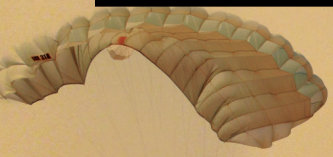
JANUARY 2022 | VOLUME 13 | ISSUE 04 | ₹150

The First and Only ISO 9001:2015 Certified Defence and Security Magazine in India

The Only Magazine Available On The Intranet Of Indian Air Force

www.dsalert.org

info@dsalert.org



INDIAN ARMY

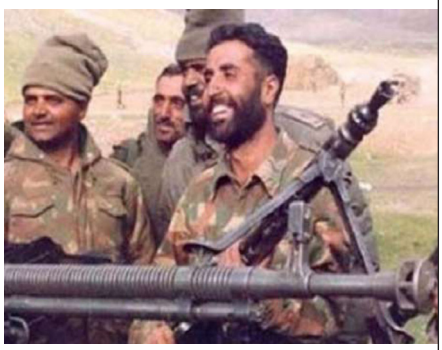
AND REPUBLIC DAY SPECIAL

DSA™

THE FIRST CHOICE IN THE DOMAINS OF
DEFENCE, SECURITY AND WORLD AFFAIRS
WORLDWIDE

12 YEARS OF EXCELLENCE

ISSN 0976-206X



CYBER PREPAREDNESS VIS A VIS DEFENCE PREPAREDNESS

As per expert assessments, India is still in the early stages of developing a path towards cyber resilience and cyber preparedness, and yes, of course, that we are currently moving rapidly from the planning stage to the implementation.

The unprecedented effort to build a modern cyber army will give a new dimension to the nation's security posture. Following the IT Act amendment of 2008, the "Indian Computer Emergency Response Team" (CERT-In) was formed to streamline cyber security in the country. The Defence Ministry (MoD) has also mandated Defence Information Assurance and Research Agency (DIARA) as the nodal cyber security agency for the Tri-Services. However, today most of the critical computer infrastructure in the country is built and maintained by National Informatics Centre (NIC). In order

to reduce the security pressure on an agency, the National Center for Protection of Critical Information Infrastructure (NCIIPC) unit was created under the guidance and direction of the NTRO. NCIIPC is an Indian government organization formulated under Section 70A of the Information Technology Act, 2000 amended in 2008 vide gazette notification issued 16 January 2014. NCIIPC works with a motive to increase information security awareness among all stakeholders as well as protect the security of Critical Information Infrastructure (CII) from unauthorized access, modification, use, disclosure, interference and inefficiency.

The first Internet service for the public was launched in India on 15 August 1995 by Videsh Sanchar Nigam Limited (VSNL). Since then the central government has continued to support the Internet as a catalyst for economic growth, job creation, more efficient government operations, public services and increased access. For the past several years, the government has been emphasizing on digitalisation for making government services available to the citizens electronically, however, these goals seem difficult to achieve due to the large offline population. India faces many challenges due to agenda-less and volatile politics that make it difficult to determine how cyber security should be prioritised. In fact, the primary objective at present is to protect law and order and provide security. But the most crucial concern is to improve the national security posture to keep the CII safe.

Cyber security hardware and software can only be **procured** by an **Indian manufacturer** or supplier

VSNL Tower Kolkata.

UMMED MEEL
B TECH, LLB (CYBER LAW)

The writer is a renowned Cyber Expert (Police and Defence Advisor). Is a Certified Ethical Hacker (CEH) and Certified Computer Hacking and Forensics Investigator (CHFI). He has delivered 100+ training and workshops on cyber security, intelligence, cybercrime investigation for state police and other law enforcement agencies including India Air Force, BSF, CISF, CAG, BPRD, CDTI and Ministries His articles have been published in many world-renowned magazines and journals and has also been interviewed by multiple news channels and newspapers on the subject of cyber-related solutions. He has also helped various investigating agencies in solving around 200 major cases related to cybercrime in the country.

In the coming few days we are going to celebrate 73rd Republic Day, and as a developing nation, we should promote cost-effective and indigenous solutions in line with cyber security challenges for

national security. Even though India has emerged as the second-largest exporter of information and technology services in the world and is also making significant progress in the e-commerce business, the private and public sector still lags behind in terms of cyber security policies and solutions.

National Cyber Security Posture

Indian National Security Advisor Ajit Doval has called cyberspace a "global common", requiring new approaches and new norms when it comes to diplomacy or conflict. The National Technical Research Organisation (NTRO) was formed in 2004 as a specialised technical research and intelligence gathering unit under the Prime Minister's Office. NTRO is working with several research institutes to create secure and resilient cyberspace for Tri-Services. Additionally, the National Institute of Cryptology Research and Development (NICRD) was formulated in the year 2007 with the aim of designing and developing encryption products for national security. The Intelligence Bureau (IB) is the principle intelligence body that focuses on internal security mainly. However, it also runs a cyber-intelligence wing, which works independently. In addition, the National Cyber Coordination Center (NCCC) was formulated; NCCC coordinates real-time situational awareness and crisis response to cyber security incidents among intelligence, law enforcement and defence forces. The main functions of the NCCC are to bring public and private sector entities, intelligence agencies, law enforcement, and respective industries under one roof to share the cyber intelligence, mitigate the effects of cyber-attack and prevent the intrusion.

Indian National Security Advisor Ajit Doval.

After witnessing several major cyber intrusions around 2010, the government is making several tireless efforts to strengthen the nation's cyber security infrastructure. A National Cyber Security Policy was published by the Department of Electronics and Information Technology (DeitY) in 2013 with the main objective of protecting the public and private infrastructure from cyber-attacks. To create a secure cyber ecosystem in the country, a workforce of 500,000 skilled professionals will be required over the next few years. With the collective effort of the concerned entities, the critical computer infrastructure is being designed and managed in line with global security standards and best practices to protect against cyber-attacks. The Data Security Council of India (DSCI) and the National Association of Software Services and Companies (NASSCOM) under Public-Private Partnership (PPP) provide a wide range of training and consultancy on cyber security to government agencies.

Cyber Research And Development

To produce world-class security solutions and skilled professionals, R&D is one of the best-proven

The Indian Army is testing the indigenous BOSS (Bharat Operating System Solutions) to guard its communication and information networks from espionage by foreign players.

methods. India needs to have a strong research base and strong policy for technology development, testing, evaluation and standardisation to broadly enhance the cyber security posture. MeitY is working closely with several academia and R&D laboratories towards undertaking R&D work. Today many reputed institutions including C-DAC, DSCI, IIT Kharagpur, IIT Bhilai and IIT Guwahati researching closely on important issues like Zero Trust Network Access System, Framework for Safe and Healthy Internet Use (SAFENET), Social Media Content Analysis, Security Operations Center (SoC) and mobile security. However, CDAC has researched several important issues with MeitY in the past and provided effective solutions.

To prepare the skilled manpower for the future, many renowned Indian Institutes of Technology (IITs) offer degree programs at the undergraduate, graduate and doctoral levels where the student or researcher can focus on cyber security. NASSCOM and DSCI have created several practical laboratories at various locations in India for both defensive and offensive directions, which have proved to be very useful in cyber research and training.

India has emerged as the **second-largest exporter** of information and **technology services** in the world

Cyber Crisis Response

Crisis Management plan includes steps to recover CII services from cyber-attack or system disruptions. National Cyber Policy and CERT-India advise every government and non-government organisation to retain regular and cross-platform backups of CII. More than 700 Indian government websites were hacked between 2013 and 2016. The NSG website was also hacked in January 2017, however, it was immediately blocked by the Computer Emergency Response Team (CERT-In). In April 2018, the website of the Ministry of Defence was hacked, raising a serious question on the country's security system. However, the website was immediately restored due to the backup availability. Cyber Incident Response Teams are aimed to involve key personnel and technologies to prevent further intrusions, isolate the infected equipment, collect

evidence, restore back-up and conduct further investigation.

NCIIPC has been running the Responsible Vulnerability Disclosure Program (RVDP) for the past several years, where any security researcher can share newly discovered vulnerabilities related to Critical Information Infrastructure. And in close collaboration with CERT-India, the findings are shared with relevant stakeholders. NCIIPC and CERT-India issue alerts and adequate guidance advisories from time-to-time to address the threats / vulnerabilities in the security of CII. The major responsibilities of NCIIPC include: identifying the CII of the country; issuing cyber advisory on a daily or monthly basis; performing digital forensics, ransomware and malware analysis; tracking the malware source; spreading cyber security awareness; and operation of 24x7 help desk for government departments. While purchasing security equipment and software, it is imperative to comply with global cyber security standards as well as fulfill all the requirements of India's internal cyber security policy. Cyber security hardware and software can only be procured by an Indian manufacturer or supplier. Today, only cert-India empaneled companies can provide cyber security-related services to government departments; this has seen a lot of improvement in service quality. Similarly, Tri-Services can get cyber security solutions only after consultation with DIARA.

Security Operations Center (SOC) – Monitoring

A Security Operations Center (SOC) is a centralised function within an organisation that continuously monitors technical activities and improves the security posture of the organisation. Collector Engine (CCE) and Parser collect row logs across an organisation's IT infrastructure, including its network devices, servers, applications, equipment, and information stores, wherever those assets reside. The Analytics and Policy Engine (APE) correlate and analyse the logs and articulates severity-based alerts. The best advantage of SOC is that you can monitor your entire organisation from a single console and see the security posture. Many advanced SOC solutions also provide inbuilt security orchestration, automation and response (SOAR) features for automatic treatment of cyber-attacks or abnormal activities based on predefined rule books. Under Public-Private Partnership, so far many government organisations are using on-premises SOC solutions and many are planning to implement them.

Cyber Security Preparedness

Every year CERT-India invites public and private sector organisations to participate in the panel exam, only after clearing four difficult stages of evaluation the institute gets CERT-In empanelment. CERT-In empanelment is considered valid for three years. The intelligence wing of higher defence authorities in India, including the Central Bureau of Investigation (CBI), which is the principle body investigating violations of central laws; analyse cyber-attacks from two different

perspectives: one is that computers are the means of attack, and the other is that computers are the target of the attack. Accordingly, from time-to-time, the Ministry of Defence creates new organisations, departments and teams. There is a division of Ministry of External Affairs (MEA) "e-Governance and Internet Technology" (EG&IT) which is completely dedicated to cyber security. The ministry also has a Global Cyber Issues Cell that tracks cyber-attacks and handles international matters affecting national policy and provides diplomatic protection to Indian CIIs from foreign powers and hackers.

Cyber Crime Investigation Cell in CBI was established in 2001, this Interpol team also takes help from police forces of other countries to investigate the issues of international cyber terrorism. As of December 2019, India has Mutual Legal Assistance Treaty (MLAT) with a total of 42 countries and under this, the Indian Court can seek assistance from the concerned country in the investigation or prosecution of a criminal case.

The **government** is making **several tireless efforts** to strengthen the nation's **cyber security infrastructure**

Bottom Line

NTRO conducts strategic surveillance of communications at landing points of terrestrial internet and satellite to prevent the spread of international cyber terrorism. The Defence Intelligence Agency (DIA) works to combine the intelligence captured by the Tri-Services - the Army, Air Force, and Navy into actionable information for the ground units.

India is working tirelessly along with many countries towards secure internet governance. In line with this, India signed the "US-India Cyber Relations Framework" with the US in September 2016, mentioning that both countries are committed to a multi-stakeholder model of Internet governance. While India is improving its economic position, it is also developing a national cyber security strategy to reflect a more balanced approach. As per expert assessments, India is still in the early stages of developing a path towards cyber resilience and cyber preparedness, and yes, of course, that we are currently moving rapidly from the planning stage to the implementation.DSA