Committed To Defence And Security Worldwide

DEFENCE & SECURITY ALERT

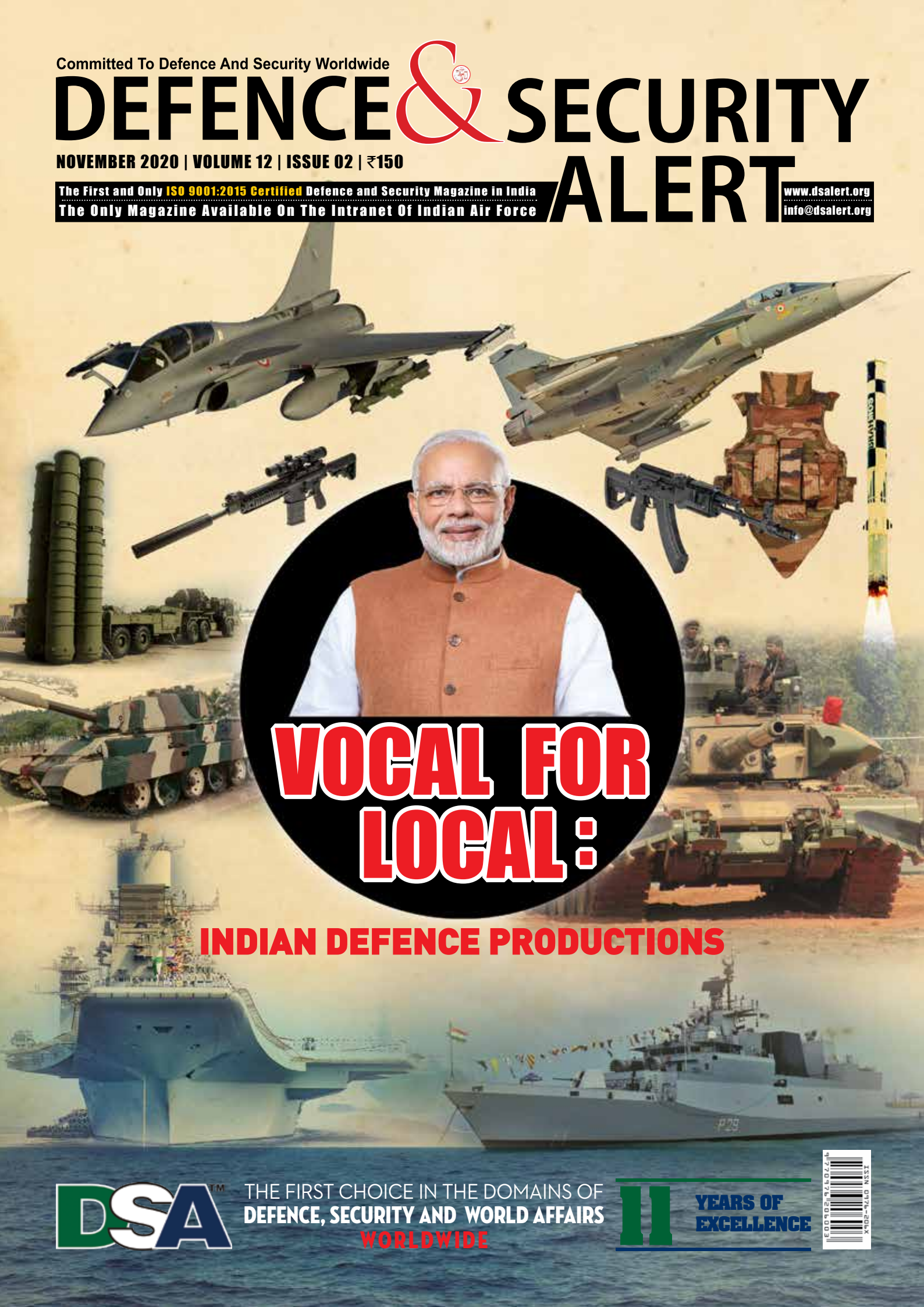
NOVEMBER 2020 | VOLUME 12 | ISSUE 02 | ₹150

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



VOCAL FOR LOCAL :

INDIAN DEFENCE PRODUCTIONS

ISSN 0974-20kX

11 YEARS OF EXCELLENCE

DSA™

An ISO 9001:2015 Certified Magazine

INDIGENOUS CYBER SECURITY AT PRODUCTION STAGE

UMMED MEEL

The author is a Cyber Expert (Police and Defence Advisor). He has delivered 100+ training courses on cyber security and cybercrime investigation for state police and other law enforcement agencies including IAF, BSF, CISF, CAG, BPRD, CDTI and Ministries. He has 6+ years of experience in the cyber security, VAPT, Digital Forensic and Cyber Crime Investigation. His articles have been published in many world-renowned magazines. He has been also interviewed by news channels and newspapers on the subject of cyber expertise. In addition, he has given hundreds of seminars on cybercrime awareness in schools, colleges and universities. He has also helped the investigating agencies in solving around 200 major cases related to cybercrime in the country.

For the monitoring and security of computer resources and services which are being used in military operations, Security Operations Centre (SOC) developed and maintained in India should be used. In view of information security and leakage for defence agencies, SOC should always be deployed in-house. The resources from the defence organisation should be trained for the SOC management because a military personal can understand about the cyber-attacks and their seriousness for defence in a better way in comparison to a civilian.

Today, India is emerging as a world power in the defence sector with technical production and strong security policies. The slogan 'Vocal for Local' propounded by the honourable Prime Minister Shri Narendra Modi from the ramparts of the Red Fort on 15th August 2020 has given a new energy to Defence Production in India. The production of secret communication system, safe military movement, modern surveillance equipments and smart weapons in the country will not only increase military strength but will also give economic momentum to the country. In the financial year 2020-21, a total budget of US $66 billion has been approved for the Indian defence forces, which is the third largest budget in the world after USA and China. India is the second defence product importing country in the world after Saudi Arabia. However, DRDO and its 50 laboratories, 4 defence shipyards, 5 defence PSUs and 41 ordnance factories come up with the defence manufacturing policy 2020 under 'Vocal for Local' and aimed at reducing imports and increasing domestic manufacturing which will give a new dimension to the national security. India is rapidly growing up in cyber intelligence through various labs and organizations but it is a different to say how vulnerable the defence products are from external cyber-attacks.

In this era of modernity, the meaning of war has tremendously changed, instead of the nuclear or military attack on a country, war can be won by ruining the computer infrastructure of the targeted country. In every country, the working of banks, railways, air traffic, communication and hospital are done and controlled only through the Internet. In such a scenario, if the main data centre of the enemy country is hacked and all the data is destroyed from there, then in a very short span of time, without using ammunition, that nation can be destroyed completely.

Indian troops today have been equipped with modern weapons and ammunition, but in the absence of technology, we are trailing somewhere. Conceived by 'Vocal for Local', today a target has been set to manufacture many defence products in India. In this modern era, it is considered safe to have a nation that not only has weapons but also has complete and accurate information about the enemy and its plan ahead of the time. So each country is developing many technologies such as machine learning based monitoring, artificial intelligence-based movement detection system and cyber intelligence to make their army more powerful.

Security agencies need a military graded **secret conversion** system

German-made machine Enigma.

Opportunities for Expansion and Modernization of National Security

Many public and private companies will have to work together in unison to strengthen the national security policy. Here we will focus only on the improvement and opportunity in technology-based defence production, although the army needs modernization in areas other than computer and cyber security also under the 'Make in India' scheme, the work of building secret communication system, internet operated smart device, smart vehicles and advanced monitoring system at advanced level can also be done in India.

Secret Military Communication

During the Second World War, a German-made machine called Enigma was used to send secret messages. To use Enigma, the operator first typed the message and then, by rotating some wheels, they exchanged cryptic letters to the message. At the receiving end, other operators could read the original message after setting up their machine with the same wheel or rotor order to remove the cryptic letters.

In the same way, security agencies today need a military graded secret conversion system. Normal land line calls or mobile calls can be intercepted by going to the same frequency. Encrypted phone communications can be used to avoid spying, interception and wire-tapping of foreign intelligence agencies. It has the ability to encrypt and decrypt phone calls, messages, file shares and storage etc.

Encrypted mobile phones have high-level encryption at both hardware and software levels. They have custom operating systems

that protect it from many known cyber threats and provide protection against electronic monitoring. Call interception can be avoided by using custom encryption algorithms. The phone has a cryptographic chip that handles both encryption and decryption. In this, the secret and military graded voice over the Internet protocol (VoIP) call facility can also be used. By making such software and hardware, during the war, military conversations and messages can be limited to authorised users only.

Internet of Military Things (IoMT)

Internet of Military Things (IoMT) is the Internet of Things for military that is used in combat military operations. It is a complex network of interconnected entities, or "information" in the military domain, through which any work can be carried out in a more efficient and informed manner depending on the physical environment, information and requirement of the time. This concept suggests that future military battles will be based on cyber and Internet of military things (IoMT) and will likely take place in urban environments rather than on the battlefield. Through this technology such devices will be developed which can reduce the physical and mental burden of the front foot soldiers. Not only this, by using the Internet of Things embedded machine in war, the loss of life of soldiers could also be mitigated.

The Internet of Military Things includes a large range of devices that take input through virtual, physical sensors and cyber interfaces and detect potential threats and necessary steps can be taken on their own. Also, the IoMT informs the concerned department for this threat. If there is an illegal intrusion on the border, an alert will be issued in the system, based on the ammunition and weapons available with the intruder, by detecting it with the help of IoMT sensors installed there. These devices include items such as sensors, vehicles, robots, UAVs, human-wearable devices, biometrics, weapons, Armor, weapons, and other smart technology. IoMT items can generally be classified into four categories:

- **Data carrying device:** To connect a physical device to the large communication network.
- **Data-capturing device:** To

read data from the document and conversion into computer readable format takes place.

- **Sensing and Actuating Device:** To sense the surrounding environment and process the associated weapon and devices accordingly.

- **Common Equipment:** To transfer the information into the network.

Using all these technologies, advanced support equipment and smart weapons can be made for the security forces.

Cyber Based Military Training

With strength of over 1.4 million active personnel, India is the second largest military power in the world and the largest volunteer army in the world. It has become imperative to equip Indian military training system with modern methods. It is necessary to emphasize to practise and take help from the upgraded defence equipments at the battle ground. Considering the requirements of the army, the construction of cyber range is also essential for cyber security training; there is a need by public and private sector companies to join hands together and make better products under 'Make in India' scheme.

Bullet Proof Vehicles for Military Transportion

In India, there is a need to manufacture bullet proof and smart vehicles at affordable prices to transport the army safely from one place to another. The manufacture of vehicles with features such as automatic mine detection, camera with artificial intelligence and vehicle control will make the army more robust. If the raw materials, technology and labour skills found in the country are properly utilized in the right direction and at the right time, it can be a defence production revolution.

Advanced Monitoring System

Security agencies are required to have many state-of-the-art equipment and resources such as night vision cameras, telescopes, face recognition CCTVs, long-range flying drones, weapons and ammunition drones, auto alerts on danger on borders. Bomb Disposal Robots (manufactured by DRDO), Artillery Detection Radar, 3D Radar, Short Range Battlefield Survey Radar, Motion Detection Radar etc. Many of these devices are already manufactured in India, some are under trial and some devices are being developed. By making these resources in India with 'Vocal for Local', India's military strength can be increased and kept confidential.

Cyber Intelligence

Cyber intelligence can be defined as hacking any computer system and stealing information from it. In cyber intelligence, instead of physical espionage, information is collected from the enemy's computers, computer resources and computer networks. The cyber intelligence community also provides timely protection against digital threats such as viruses, hackers and terrorists. In cyber intelligence, the computer system of an individual and organization can be targeted. Through technical weakness or social engineering attack, computer system of enemy country, could be hacked and confidential information could be extracted out of them.

Along with designing a software and hardware for defence, it is also important to pay attention to their possible cyber threats.

Secure Cyber Defence Production

We should always use the Secure Software Development Life Cycle (S-SDLC) while developing any product or tool for the defence. Generally, a secure SDLC involves integrating security testing and other activities into the current development process. According to a proverb - "necessity is the mother of invention" - the same applies for S-SDLC. There were also days when organizations would develop an application or device and sell it to security organizations directly and the rest ignored its complexities and security. Those days are gone, now it is mandatory to pay attention to the cyber security of the product along with the development.

After developing the above-mentioned techniques, on one hand, the military strength will be strong and on the other hand the risk of cyber-attacks on these devices will also increase. Secure coding and software should be used from the time of production to protect these devices and equipment against upcoming cyber-attacks. Devices without complete Vulnerability Assessment and Penetration Testing (VAPT) should not be allowed in military operations. In Secure Cyber Defence Production, the device can

Such **computer infrastructure** has to be **protected** not only from external cyber-attacks but also from internal people

Security Operation Center (SOC).

be protected from cyber-attacks through Offensive and Defensive Security exercises. The Defence Security approach focuses on detecting, reacting and preventing cyber-attacks on the device. Whereas, Offensive Security is a proactive approach to protecting computer systems, networks from cyber-attacks.

Second Layer Cyber Defence Production

If any cyber product is made for defence agencies, then computer, computer resources and computer network are definitely used. Such computer infrastructure has to be protected not only from external cyber-attacks but also from internal people. Many times, information can be stolen with the help of insider through honey trapping and social engineering attacks. It is very important to record and monitor the activities of every computer, network device and server which you are using in the military operations. To secure defence computer infrastructure, there are lots of SIEM and SOC solution are already available in the software market. To secure the defence infrastructure, there is a need to build Machine Learning and Artificial Intelligence based tools such as Network Firewall, Web Application Firewall, Data Loss Prevention System (DLP), Intrusion Detection (IDS) And Intrusion Prevention Systems (IPS) Etc. Security Information and Event Management (SIEM) is a core part of the cyber security practices, where software records every security incident associated with products and running services. The Security Operation Center (SOC) is a centralized platform, which analyses security logs received from SIEM and other network devices, based on which it detects the attack, attack type, source and sends an alert mail to the security team.

Taking SOC services from a foreign company is not considered safe according to the Indian defence policy because SOC environment has full access and secret information about the entire computer infrastructure. In such a scenario, if the service provider company steal the intelligence of military operations, it can endanger the national security. Therefore, for the monitoring and security of computer resources and services which are being used in military operations, SOC developed and maintained in India should be used. In view of information security and leakage, for defence agencies SOC should always be deployed in-house. Resources from the defence organization should be trained for the SOC management, because a military personal can understand about the cyber-attacks and their seriousness for defence in a better way in comparison to a civilian. Therefore, this resolution of production for such cyber defence products and their protection will establish a developed and secure nation.DSA