199-211

ATMANIRBHAR BHARAT: TOWARDS BUILDING A CREDIBLE DEFENCE AGAINST IEW

Gp Capt Kancherla Arun Kumar

"Faith is of no avail in absence of strength. Faith and Strength, both are essential to accomplish any great work."

- Sardar Vallabh Bhai Patel

Abstract

Modern weapon systems predominantly have embedded Information and Communication Technology (ICT) devices. Today network centric operations are a norm considering the usage of smart weapons systems, autonomous systems and remotely operated / controlled system. In the present situation, majority of military acquisitions have been from global manufacturers. These systems are susceptible to IEW attacks and pose a serious concern for the national security. The geopolitical situation is dynamic and the coalitions and collaborations are not permanent. It is all a 'marriage of convenience'. Cooperations and collaborations are promoted by many developed countries purely to further their geopolitical aspirations. Inequality, in any sphere, between the two partners tilts the balance more in favour of the technologically developed nation. The other partner would be at the mercy of the developed nation in absence of credible negotiating instruments. Bharat has today realized its potential and strives to maintain its strategic independence and hence wants to be self-reliant and self-

sufficient as far as possible. Defence industry is one such area where the government has initiated many steps to have greater self-reliance. The initiatives aim to give greater autonomy to the nation in terms of both hardware and software. Atmanirbharta in the field of design and development of electronic equipment would play a major role in building a credible defence against IEW attacks.

INTRODUCTION

It is once in a long time that one would come across news like 'Pager Attack'. The recent event where more than 3000 pagers blew up injuring or killing the owners of the pagers. The pager attack was followed immediately with an 'Walkie-Talkie attack' where personal communicators exploded killing many people. News reports and studies suggest that most of the victims were Hezbollah members and the pager attack and the Walkie-Talkie attack was planned and triggered by Israeli intelligence agencies. It is too early to arrive at conclusions. However, the incident does highlight some important aspects of Information Warfare. It is believed that the Hezbollah was using these low tech 'pagers' and 'walkie-talkies' to guard against cyber-attacks on the sophisticated communication equipment which can be traced and intercepted. However, even these so called 'low tech' equipment were not immune to IW attacks. The whole incident presented an excellent case study for research scholars, intelligence agencies and other law enforcing agencies. There are lot of lessons to be learnt from this incident.

Another recent event that garnered interest was the Microsoft Windows systems crash worldwide owing to a glitch during the software update by 'Crowd Strike Holdings Incorporation', a cybersecurity firm. The so-called security update resulted in shutting down of many essential services across the world. Some of the major services affected by the crash were banking services, airline services, hospitals & healthcare services etc.

Stuxnet Computer Worm was in news a few years back as a malware that was supposedly developed to attack Iran’s nuclear facilities. It is believed that it has since mutated and spread to other industrial and

energy-producing facilities. Such malwares are a big threat to critical production / industrial facilities that use Supervisory Control and Data Acquisition (SCADA) systems or the Programmable Logic Controllers (PLCs) for controlling, monitoring, and analyzing industrial devices and processes. PLCs and SCADA systems play a critical role in modern industrial automation.

For those in the field of Information Warfare (IW), these events bring forth aspects needing further focus. While the first and third events are considered to be an act of aggression by parties in conflict, the second event is an example of how internal players can cause major breaches in the systems. The incidents also indicate that the threat can be through either hardware or software or through both. One of the most glaring facts is that in all the three cases the victim parties were dependent on external sources for the hardware and the software.

RELEVANCE OF THESE EVENTS FOR BHARAT AND ATMANIRBHARTA

Though our country holds rich heritage and fathomless knowledge in our ancient texts, the foreign invasions and foreign rule has pushed back the country from a prosperous country to a third world country by the end of foreign rule. Since independence the country has grown and improved its economic status. The industry has grown and the manufacturing sector is catching up the pace with the developed countries. However, there is a lot to be done in the field of technology, especially when it comes to development of indigenous components for critical systems. Some glaring examples that point at the roadblocks in our technological growth are absence of development in core technologies like Semiconductor chip design, miniature / microelectronic components etc. which are basic building blocks of the computer & control systems that are the brains of the smart systems. Any electronic gadget that is assembled in our country has some critical components that are imported as the country lacks depth in design and development of such critical components.

In absence of some indigenous core technologies, our R&D organisation and private industry depends predominantly on foreign technology giants for supply of these core components. In most of the cases, the foreign players have non-disclosure agreements and restrictive clauses which inhibit greater insight into the technology used. Governments of the most of the developed countries control the Intellectual Property Rights (IPR) of the critical technology and discourage Transfer of Technology (ToT) of such technology.

Urgent operational requirements necessitate development or acquisition of weapon systems, the R&D organisations and their private suppliers are forced to integrate these systems at the cost of greater insight into the systems. In such cases trust predominantly plays a major role in finalizing the deals / contracts. There are some safeguards that have been introduced in the Defence Acquisition Procedures 2020 (DAP 2020, Chapter VIII, Acquisition of Systems Products and ICT Systems). However, these safeguards are predominantly based on the trust factor where the supplier / vendor provides the requisite certificates (as per Appendix B to Chapter VIII of DAP).[1] It is necessary to understand that these safeguards may not be sufficient from strategic point of view. As long as we are dependent on external agencies for critical core technologies, we are vulnerable to external pressures and threats.

While speaking at the Cyber Security Conclave held by the Cyber Security Association of India, Dr. VK Saraswat, ex-DRDO head and member of the Niti Ayog, aptly highlighted that 'security begins with a trustworthy hardware'.[2]

STRATEGIC INDEPENDENCE & AUTONOMY

The current geopolitical situation is fluid and there are lot of groupings. There are many so called friendly nations that have friendly relations even with those countries that have difference of opinion with Bharat. For example, Bharat and the United States of America have an enabling agreement Communications Compatibility and Security Agreement (COMCASA) which facilitates interoperability between militaries and

sale of high-end technology. The US government shares this high technology with NATO members including Pakistan as 'global partner'. There is difference of opinions between the US and People's Republic of China. However, China and Pakistan have friendly relations. This is a good example of 'marriage of convenience', which indicates that there are no permanent friends or permanent adversaries. This uncertainty raises questions regarding certain trust based agreements and commitments by the concerned parties.[3]

Apart from the nation states, non-state actors (NSAs) too have an impact on the dynamics of the world. These NSAs, like NGOs, multinational companies, terrorist and religious groups, hackers etc. influence the economies of nations and their future course of action. There are instances where nation states have indirectly supported the NSAs to counter their adversaries.

This poses a major question regarding the degree of trust that exists between the Nations in the volatile, uncertain, complex and ambiguous (VUCA) World.

Bharat has, since independence, believed in non-alignment with the power blocs of erstwhile cold war era. The grouping still continues post the Cold War. However, the grouping in the present situation is more fluid and is governed by economic interests of different players. However, Bharat aspires strategic independence and autonomy to ensure that it has the right to choose a path that would be the best in interest of the Nation. The success of this particular approach necessitates greater self-dependence i.e., 'Atmanirbharta' on many fronts.

One such major front is development of indigenous core technologies for ICT devices that are predominantly used across the spectrum.

SUPPLY CHAIN

A preliminary study of the first incident described above discusses the possibility of introduction of the explosive material and malicious codes into the pagers or the personal communicators somewhere enroute from

the manufacturer to the consumer. The supply chain was meticulously studied, identified, and compromised. The execution of the attack was controlled by the Israeli agencies through the malicious code. This points towards the need for a robust and secure supply chain for the products or the components being imported.

Supply chain disruptions could also happen due obsolescence of some products or components. Technology growth and changes in the last few decades follows the Moore's Law. This pace of growth results in faster rate of obsolescence of modern equipment as the industry adapts to the newer technology for performance enhancement and economic reasons. In such a scenario, there might be situations where alternate sources of these products or components are explored. These sources could be second hand equipment or substitutes developed by a lesser known third party. How far these sources are vulnerable to compromise, by vested parties, is a question that one needs to ask before procuring products or components from them. This increases the risk factor in terms of IEW attacks or cyber attacks.

Strategic grouping and geopolitical scenarios might also cause disruptions in supply chain of critical products or components. Sanctions by source countries might restrain the OEMs from supplying the products and components during critical stages to put pressure on the government to tow their views or line. In absence of support from the OEMs, there might be situations where regular updates (essentially for software) are not available and one is forced to operate with outdated systems with vulnerabilities that are publicized on open sources like internet. In case of hardware, as discussed above, a third-party supplier is explored to provide the product thus creating weak links in the supply chain.

COMPLEXITY OF SYSTEMS

State-of-art weapon systems consist of systems of systems and their architecture is complex in nature. Different embedded systems are used in integration and manufacturing of complex weapon systems. These

systems are used for operations and maintenance of the systems. Each system comprises of thousands of electronic components. Further, these systems come with custom made firmware and software. Any vendor would not like to share the software code for obvious reasons; therefore, 100 percent security evaluations of such systems is extremely difficult. Exploits like logic bombs and trojan horses are extremely stealthy and difficult to identify and neutralize.

Further, there are systems that require regular updates to cover vulnerabilities, or for health monitoring etc. There are systems which necessitate connecting the unit to internet for patch updates or for live health monitoring from remote locations. Such requirements increase the risk factor.

Penetrative testing by experts may help in identifying some of the vulnerabilities but it is very difficult to identify exploits like the logic bombs. Another relevant question that arises is the need for resources to carry out complete system analysis after each update. Over and above such risks, the risk of inadvertent damage to systems is possible as was seen in the case of 'Crowd Strike' security services. As mentioned earlier, there are some safeguards in DAP 2020 for acquisition of such systems, but these safeguards depend on 'trust' and reputation of the OEMs.

The three incidents described at the beginning of the paper reiterate the need for strengthening self-reliance in both software and hardware. The vulnerabilities exist in both software and hardware.[4] Further, with advent of Artificial Intelligence (AI) and it’s usage in advance weapon system poses a major challenge in terms of assessing cyber security aspects of the systems.

NEED OF THE HOUR

From above we can come up with the following major issues that pose challenges to Bharat:

- Bharat predominantly depends on imports for complex weapon systems.

- Most of the modern weapon systems are system-of-systems integrated using processors and computing devices. This means that the systems comprise of customized computing and software/ firmware. OEMs are not forthcoming in sharing the technology behind the systems.
- Bharat aspires to attain strategic independence and hence is balancing its relationship with the different power centers of the world. This balance comes at a cost – 'Trust Deficit'.
- Dynamics of the geopolitical situation in the World poses multiple challenges and impact supply chains. Having a credible supply chain is not guaranteed.
- Complexity of the latest weapon systems makes it very difficult to carry out a comprehensive cyber safety assessment of the system.

All these issues, in one way or other, can be related to IW. These issues create vulnerabilities for Bharat and there is a need to address them as comprehensively as possible. In the present scenario, defensive IW solutions can be considered to be more of tactical nature. The major efforts are directed at neutralizing the attack vectors by building multi-layered protection.

However, there is a need to focus on strategic solutions to counter threats that may not directly appear to be factors in IW. The cases mentioned here are some of the examples that indicate towards some methods which highlight ingenuity of human mind and use of unthinkable tactics to disable systems of adversaries or even cause physical damage to the systems.

IW is not a normal convention form of warfare. The threat from such warfare exists throughout, at all times, irrespective of visible geopolitical relationships. These tactics can be used even by so called 'friendly' partners as negotiation instruments to gain favourable policy decisions in their favour. Manipulation of industrial facilities, economic activities

(like banking, airlines etc.) can be resorted to by parties with vested interests at any time without declaring any direct conflict with the nation. Declaring such acts as intentional action is difficult to prove.

This brings into focus the need for greater self-reliance on design, development and manufacturing of critical components of processors, control units and other ICT devices that are vulnerable to IW. Controlled design, development and manufacturing of such devices with better mechanism to monitor and oversee the activities would ensure better security in the fast developing digital and cyber domain. A robust industry would also give Bharat an opportunity to transform into a major exporter.

ENDS, WAYS AND MEANS – TARGET ATMANIRBHARTA

Having said that, it is necessary to understand that achieving strategic independence and Atmanirbharta is not an easy journey. It involves different stages starting with establishment of strategic intent, formulation of strategy, implementation of the strategy and then evaluating the strategy. This is in iterative process where feedback from each stage is given to the earlier stages to facilitate mid-course path corrections if required or change of strategy in some cases. Dynamic interactions between the nation states and other players would mean that there would be constant need for re-visiting the strategies and effecting course corrections where required.

Government of Bharat has taken many policy decisions in direction of attaining self-reliance. Some of the prominent decisions for Defence are:

- 'Make in India' thrust – encourage FDI through steps like increasing the investment limit to 76 percent, tax incentives etc.
- Revision of Defence Procurement Procedures (DPP) giving rise to the DAP 2020. This has been refined further over time to introduce clauses from time to time. DAP 2020 introduced concepts like strategic partnership to enhance participation of Indian industry. Higher priority has been given to Indigenous systems over global acquisition.

- Establishment of dedicated Defence Corridors in UP and Tamil Nadu to encourage private defence industry.
- Innovation for Defence Excellence (iDEX), an operational framework of the Defence Innovation Organisation (DIO). DIO is a Special Purpose Vehicle (SPV) under the aegis of the Department of Defence Production, MoD. There are many initiatives like having iDEX challenges to encourage MSMEs and start-ups to participate in the innovation drive etc.

The above are but some of the many policy decisions taken by the Government to encourage indigenization and innovation in the field of Defence Equipment. Further, the government has also introduced some reforms like reorganisation of the erstwhile ordinance factories. Review and reorganisation of the Defence R&D Organisation is in progress.

TARGET SEMICONDUCTOR DEVICES – A MAJOR STEP IN ENHANCING IEW DEFENCE

India Semiconductor Mission (ISM) was launched, in 2021, by Ministry of Electronics and Information Technology (MeITY). It aims to establish a strong semiconductor ecosystem in the country. it is a specialized and independent business division within the Digital India Corporation that aims to build a vibrant semiconductor and display ecosystem to enable India's emergence as a global hub for electronics manufacturing and design.

As a part of the initiative, ISM has conducted seminars, webinars, workshops, exhibition and conferences in name of SEMICON India. The first SEMICON was held in 2022. The last SEMICON was held in September 2024. The conference had discussions on various aspects like training, supply chain management, latest manufacturing technology etc. Industry-academia interactions during the conferences also contribute towards better synergy.

Organisations like Electronics Sector Skills Council of India (ESSCI) have been conducting workshops and training sessions for Semiconductor manufacturing.

MeITY had earlier introduced a Design Linked Incentive (DLI) scheme for fostering semiconductor design companies. This is akin to the Production Linked Incentive (PLI). Another scheme which encouraged manufacturing of specified electronic goods is the Scheme for Promotion and Manufacturing of Electronic Components and Semiconductors (SPECS).[5]

SOFTWARE AND FORENSICS

Bharat has been recognized for its prowess in software development. However, there is a lot to be desired for addressing IEW issues that have been discussed. Programming for military systems requires specific skills. Skill development is necessary in such areas.

C-DAC developed the Bharat Operating System Solutions (BOSS). Similarly, a start-up incubated by IIT Madras has developed Bharat OS. These kinds of initiatives would facilitate customization of software for the indigenously developed hardware. There is a need to coordinating agency that would bring together various software development agencies and contribute towards indigenization. Today there are multiple startups having talent and capabilities. There is a need to tap these startups in contributing towards 'Atmanirbharta'. Different challenges being hosted under iDEX is a crucial step in this direction.

The Indian Armed Forces too have been working towards autonomy in the software being used for various systems in the Armed Forces. IAF has specific agency for indigenous software development required for advanced weapon systems. The institute is not only involved in software development but also involved in activities like testing and evaluation of software.

Cyber forensics is another area which would contribute immensely towards understanding various exploits and threats. Institutes like National Forensic Science University (NFSU) and Rashtriya Raksha University (RRU) have been recognized as institutes of national importance and are being empowered to work in cyber security and cyber forensics fields.

A major step taken in this direction is setting up of Defense Cyber Agency (DCA), which is a tri-service agency for providing direction on cyber security aspects. Preparation of cyber strategy, doctrine and policies for the Armed Forces and coordination with other cyber security agencies.[6] One of its primary responsibilities includes policy on eliminating the use of foreign hardware and software in the Indian Armed Forces. Coordination between the Cyber Security Division of MeitY, Cyber and Information Security (C&IS) division of MHA etc. would reap dividends in achieving autonomy in field of Cyber Security.

CONCLUSION

Today as we are moving away from conventional warfare to a multidimensional warfare scenario. Independent or Joint, both types of operations are graduating into Network Centric Operations. Smart Weapon systems, autonomous systems and remotely controlled systems are all part of an effective Combat situation. Embedded ICT devices of such systems are targets for IEW attacks. Susceptibility of such targets to IEW attacks increases multifold if the user does not know the system well. This happens in most of the cases where the systems are imported and ToT is not part of the acquisition contract. Lack of in-depth knowledge hampers building of credible defence against such attacks. Indigenous systems would facilitate better understanding and control of the devices. The degree of threat decreases multifold if the system is indigenous. It also ensures a healthy supply chain and flexibility for scaling up the production as and when required. An indigenous design, development and manufacturing capability would facilitate better monitoring of the complete process. This would enable better governmental control of technology and also ensure that Bharat defends itself from IEW threats that arise due to dependence on technology and components on others This would also strengthen Bharat to resort to offensive IEW tactics, if and when required, in defense of its national interest and security. Atmanirbharta strengthens the national desire to be strategically

independent. This enhances the national power and contribute to overall growth of the nation.

★★★

Gp Capt Kancherla Arun Kumar is a commissioned officer in the Aeronautical Engineering branch of IAF. He has a Bachelor's Degree in Computer Science and Engineering (BE Comp Sc & Engg.). He has a master's degree in Quality Management (MSQM) from BITS Pilani and HRM (MA HRM) from Jamia Millia Islamia. He is a Fellow of the Institution of Engineers (FIE), India and a Member of the Aeronautical Society of India (MAeSI). He is also an alumnus of the College of Defense Management, Secunderabad. During the course of his service, the officer has gained vast experience in maintenance of ISR equipment. He also has expertise in project management and defence acquisition.

NOTES

1 *Defence Acquistion Procedures 2020, Ministry of Defence, Bharat*

2 *Dr. VK Saraswat; Cyber Security (talk during the Cyber Security Conclave, Vigyan Bhavan, New Delhi, 2019)*

3 *Lt. Gen Anil Ahuja (Retd.); Prospects of India – US Defence Cooperation (National Security Vol.IV Issue II, Apr-June 2022, pp 125-138, Vivekananda International Foundation)*

4 *B Poornima; Cyber Preparedness of the Indian Armed Forces (Journal of Asian Security and International Affairs,IO(3)301-324, 2023)*

5 *Giri Hallur, P Ashok; Semiconductor Sankalp: A Vision for India's Tech Dominance (Intelligent Computing and Control for Engineering and Business Systems 2023, IEEE)*

6 *Arindrajit Basi, India's International Cyber Operations: Tracing National Doctrine and Capabilities (United Nations Institute for Disarmament Research, 2022)*

Bibliography

1 *India's Place in the World, Policy Watch Volume XII, Issue 5, May 2023, New Delhi*

2 *Non-state Actors Playing Greater Roles in Governance and International Affairs, Memorandum, National Intelligence council, US, 5 Jul 2023.*

3 *Pranay Kotasthane, Arjun Gargeyas; Harnessing Trade Policy to Build India's Semiconductor Industry, Hinrich Foundation, Advancing Sustainable Global trade, May 2022*