ORF ISSUE BRIEF

SEPTEMBER 2016
ISSUE NO. 159

India must attain e-SWARAJ

R K SHARMA

ABSTRACT India is a sovereign nation; is it digitally sovereign, too? This paper examines the degree to which India is self-reliant in electronic hardware. After all, for a country to be self-reliant in the information age, it has to either attain indigenous capability in electronic manufacturing and services or be equipped to protect data and mitigate the threats associated with supply chain vulnerabilities. This paper refers to self-reliance in electronic hardware as 'electronic sovereignty or 'e-Swaraj'. It aims to provide an overview of risks in the global supply chain and suggest solutions to mitigate them in the Indian context.

INTRODUCTION

Information and communication technologies (ICT), and the Internet in particular, have become major driving forces of socioeconomic development: by one estimate, a 10-percent increase in mobile and broadband penetration increases the per capita GDP by 0.81 percent and 1.38 percent, respectively, in developing countries.[1] India, too, has taken steps to utilise ICT for development. Transforming the country into a digitally empowered society and knowledge-driven economy is at the heart of 'Digital India', which is among the Modi government's flagship programmes. The initiative seeks to guarantee the availability of government services and information on a 24x7 basis irrespective of the user's geographical location. For this programme to succeed, it is necessary to set up information networks and ensure their interconnection with almost all systems of the state like transport, energy, railways, banking, government institutions or public services. This interconnection is bound to deepen with the advancements in technology and Internet of Things.

Observer Research Foundation (ORF) is a public policy think-tank that aims to influence formulation of policies for building a strong and prosperous India. ORF pursues these goals by providing informed and productive inputs, in-depth research and stimulating discussions. The Foundation is supported in its mission by a cross-section of India's leading public figures, academics and business leaders.

To know more about ORF scan this code

ICT systems and digital technologies are the mainstay of an information society as these networks and physical infrastructure form the digital highways on which data flows. Most equipment and technology for setting up such infrastructure in India are currently procured from global sources. These systems are vulnerable to cyber threats just like any other connected system but perhaps the most important known attack vector is through the digital 'supply chain', information infrastructure and various networks and systems of government and the private sector that extensively leverage latest technology and commercial electronic components, viz. hardware, software and firmware sourced from global sources. Global procurement has an inherent advantage of getting state-of-the-art technology at competitive prices. But it also raises the possibility of the supply chain being compromised by a state or non-state adversary in the form of tampering components during their development, delivery, or firmware maintenance. Another concern is that of deliberately infecting products and services to render their operations under the control of a third party to extract information, manipulate data integrity or make the system fail under specific conditions.

'Supply Chain': A Definition

The European Union Agency for Network and Information Security (ENISA)[2] defines 'Supply Chain", "Integrity" and "Supply Chain Integrity" as:

(a) **Supply Chain:** "A system of organizations, people, technology, activities, information and resources involved in moving a product or service from producer to customer."

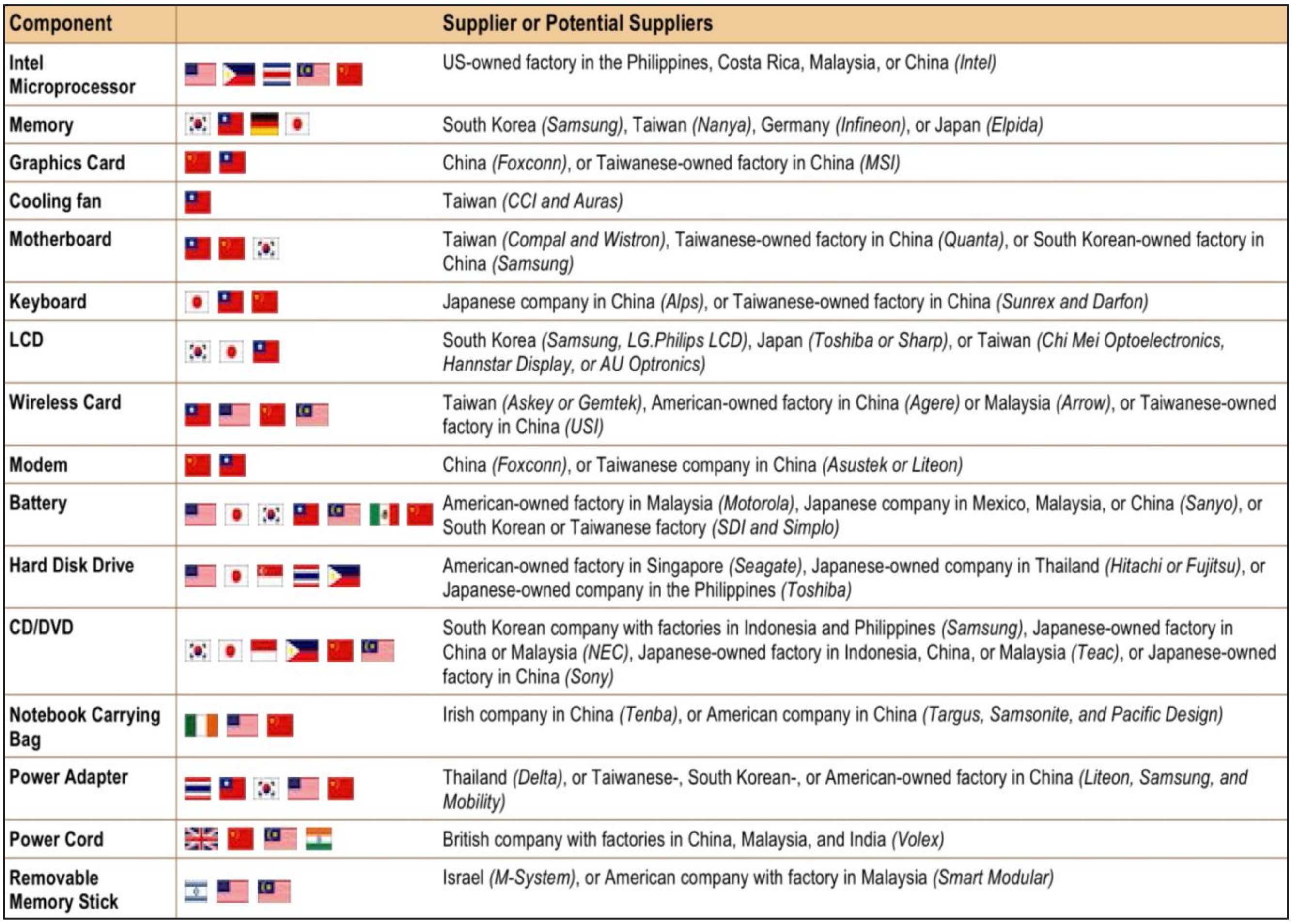
(b) **Integrity:** "A concept that is related to perceived consistency of actions, values, methods, measures, principles, expectations and outcome."

(c) **Supply Chain Integrity (SCI):** "Indication of the conformity of the supply chain to good practices and specifications associated with its operation."

The 'supply chain' in effect encompasses all actions associated with the lifecycle of a product including conception, design, production, quality assurance, transportation, usage, maintenance, discard and even reuse/ recycle, where feasible. SCI is a complex interaction between various processes, organisations, technology and resources. Integrity for information products implies that the product behaves in exactly the same manner as understood when it had been procured. The normative aim of SCI is to ensure that procured information system and components fulfil the sought specifications without compromising the privacy of the user. This paper examines the nuances associated with India's information systems supply chain.

THREATS

The primary component related to electronic sovereignty is communication networks and its components. These systems used by governments, businesses, telecommunication providers and end-users are often imported. The same holds for software and firmware. To illustrate the diversity of supply chain sourcing, journalist-author Thomas Friedman used the example of the average Dell laptop and the geographical distribution of its sources. This distribution is reproduced below:[3]

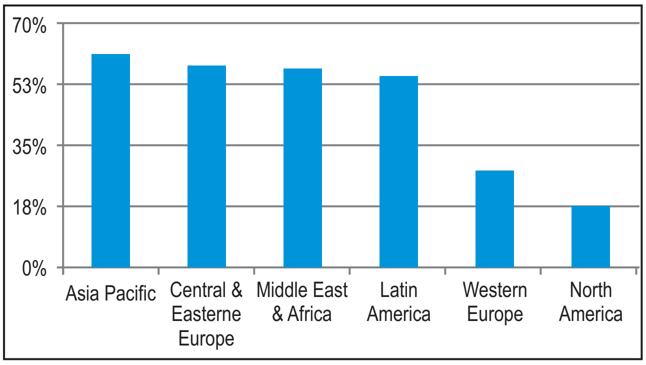


Component		Supplier or Potential Suppliers
Intel Microprocessor	🇺🇸 🇵🇭 🇨🇷 🇲🇾 🇨🇳	US-owned factory in the Philippines, Costa Rica, Malaysia, or China *(Intel)*
Memory	🇰🇷 🇹🇼 🇩🇪 🇯🇵	South Korea *(Samsung)*, Taiwan *(Nanya)*, Germany *(Infineon)*, or Japan *(Elpida)*
Graphics Card	🇨🇳 🇹🇼	China *(Foxconn)*, or Taiwanese-owned factory in China *(MSI)*
Cooling fan	🇹🇼	Taiwan *(CCI and Auras)*
Motherboard	🇹🇼 🇨🇳 🇰🇷	Taiwan *(Compal and Wistron)*, Taiwanese-owned factory in China *(Quanta)*, or South Korean-owned factory in China *(Samsung)*
Keyboard	🇯🇵 🇹🇼 🇨🇳	Japanese company in China *(Alps)*, or Taiwanese-owned factory in China *(Sunrex and Darfon)*
LCD	🇰🇷 🇯🇵 🇹🇼	South Korea *(Samsung, LG.Philips LCD)*, Japan *(Toshiba or Sharp)*, or Taiwan *(Chi Mei Optoelectronics, Hannstar Display, or AU Optronics)*
Wireless Card	🇹🇼 🇺🇸 🇨🇳 🇲🇾	Taiwan *(Askey or Gemtek)*, American-owned factory in China *(Agere)* or Malaysia *(Arrow)*, or Taiwanese-owned factory in China *(USI)*
Modem	🇨🇳 🇹🇼	China *(Foxconn)*, or Taiwanese company in China *(Asustek or Liteon)*
Battery	🇺🇸 🇯🇵 🇰🇷 🇹🇼 🇲🇾 🇲🇽 🇨🇳	American-owned factory in Malaysia *(Motorola)*, Japanese company in Mexico, Malaysia, or China *(Sanyo)*, or South Korean or Taiwanese factory *(SDI and Simplo)*
Hard Disk Drive	🇺🇸 🇯🇵 🇸🇬 🇹🇭 🇵🇭	American-owned factory in Singapore *(Seagate)*, Japanese-owned company in Thailand *(Hitachi or Fujitsu)*, or Japanese-owned company in the Philippines *(Toshiba)*
CD/DVD	🇰🇷 🇯🇵 🇮🇩 🇵🇭 🇨🇳 🇲🇾	South Korean company with factories in Indonesia and Philippines *(Samsung)*, Japanese-owned factory in China or Malaysia *(NEC)*, Japanese-owned factory in Indonesia, China, or Malaysia *(Teac)*, or Japanese-owned factory in China *(Sony)*
Notebook Carrying Bag	🇮🇪 🇺🇸 🇨🇳	Irish company in China *(Tenba)*, or American company in China *(Targus, Samsonite, and Pacific Design)*
Power Adapter	🇹🇭 🇹🇼 🇰🇷 🇺🇸 🇨🇳	Thailand *(Delta)*, or Taiwanese-, South Korean-, or American-owned factory in China *(Liteon, Samsung, and Mobility)*
Power Cord	🇬🇧 🇨🇳 🇲🇾 🇮🇳	British company with factories in China, Malaysia, and India *(Volex)*
Removable Memory Stick	🇮🇱 🇺🇸 🇲🇾	Israel *(M-System)*, or American company with factory in Malaysia *(Smart Modular)*

The threats projected in the electronic supply chain[4] include the following:

(a) **Hardware or Software containing Malicious Logic:** The product supplied is intentionally injected with malicious logic during manufacture or project implementation stage to gain or change sensitive information, denial of service or even destroy the system under specific conditions.

(b) **Non-Genuine Hardware or Software:** Pirated software or fake hardware can cause immense damage to the mission critical system or critical infrastructure as a product which is not genuine threatens the reliability of the system. As per BSA's Global Software Survey (May 2016), 39 percent of software installed on PCs around the world in 2015 was not licensed, and even in certain critical industries, unlicensed use was high.[5] The broad statistics[6] of unlicensed software usage are:



(c) **Disruption in Supply Chain:** Disruption in the supply chain on account of production failure, loss of reserve inventory owing either to natural causes (floods, earthquakes, hurricanes, tsunamis, etc.) or man-made crises like strikes and riots can directly affect operations which could be critical to the system.

(d) **Vendors/Contractors:** Vendors/contractors who are entrusted with project implementation by virtue of their job have an access to information which may be sensitive, and the feasibility of its exploitation for nefarious activities cannot be ruled out.

(e) **Hardware/ Software Containing Unintentional Vulnerabilities:** These are the unintentional "zero-day" vulnerabilities present in the system and lend themselves for exploitation if found out by adversary/non-state actors.

(f) **Insertion of Malicious Software during Maintenance:** Malicious software can also be injected into the system during maintenance by the vendor or during updating software.

Factors Responsible for Supply Chain Menace

(a) **Lack of Indigenous Capability:** If a nation does not have indigenous capability then it has to perforce rely on the global market which is a complex and interconnected arena involving people, processes and technologies. Components used in networks are manufactured in some countries, assembled in others and eventually sold across the globe. The systems may be contracted by local sellers and integrators and subsequently installed and operated by different organisations. In a competitive bidding system, the vendor with the lowest quotes gets the order: this system may lead to provisioning of substandard products and that too from a source which may not be conforming to standards.

(b) **Lack of Policy Guidelines:** Detailed procurement policies whether from an Indian vendor or from global sources will to an extent remove anomalies or grey areas. Indian defence procurement procedure, for example, has evolved over a period of time and to an extent addresses the issues, but the problem in electronic systems is that policy formulation is unable to keep pace with technological advancements. Lack of policies and guidelines makes it difficult to ensure equipment integrity.

(c) **Non-Availability of Testing Facilities:** For testing of procured electronic systems, there is a requirement of state-of-the-art facilities. Establishment of these is feasible only when the know-how is available—which will not happen unless the country obtains access to the complete technology. Also, system delivered to end-users cannot always be evaluated because of lack of appropriate evaluation approaches, methodologies and tools.

(d) **Lack of Coordination:** Coordination and sharing of information among government agencies as well as the private sector, especially of good practices, approaches and methodologies, needs to be enhanced.

(e) **Non-Availability of Standards:** Standards are a means of achieving harmonisation in processes so as to have a product/process which meets the desired specifications. The table below lists some standards laid down for supply chain and supply chain integrity.[7] The list is not comprehensive, but indicative of the fragmented approach being taken in the field.

(f) **Lack of Skilled Security Professionals:** Availability of skilled manpower is an asset when it comes to managing information systems and handling cyber incidents, apart from ensuring 'cyber hygiene' in processes.

Approaches Adopted by Countries: The actions taken by cyber-mature nations are highlighted below:

THE US

As per the comprehensive National Cyber security Initiative of the USA:[8]

"Risks stemming from both the domestic and globalized supply chain must be managed in a strategic and comprehensive way over the entire lifecycle of products, systems and services. Managing this risk will require a greater awareness of the threats, vulnerabilities, and consequences associated with acquisition decisions; the development and employment of tools and resources to technically and operationally mitigate risk across the lifecycle of products (from design through retirement); the development of new acquisition policies and practices that reflect the complex global marketplace; and partnership with industry to develop and adopt supply chain and risk management standards and best practices."

Consistent with these principles, Section 806 of the National Defense Authorization Act for Fiscal Year 2011 authorises the Secretary of Defense or the Secretaries of the Army, Navy and Air Force to exclude vendors or their products if they pose an unacceptable supply chain risk.[9] The US in fact emphasises on building both global and national capabilities to address supply chain risks without undermining international competitiveness and legitimate trade flow.[10] These capabilities include:

Classification and Identification of SCI Standardisation Efforts

S.No	Classification	Standard Development Organisation	Standard	Comments
1.	Origins (sources) of supply chains	ISO SC27	ISO/IEC 27036: Guidelines for Security of Outsourcing	These are generic documents and not specific to SCI
2.	Processing and configuration	ISO SC31	RFID supply chain applications	Nothing specific to SCI
3.	Delivery and governance of the Supply Chain	iNEMI Supply Chain study group HDPUG Supply Chain study group: NASPO (North American Security Products Organization) NIST	Risk Modelling pilot Data Exchange pilot	Nothing specific to SCI
4.	Integrity techniques	JTC1-SC27 Safe code Open Group	N10656:update to ISO 27002: security techniques Open Trusted Technology Framework	Nothing specific to SCI
5.	Verification and checks	ISO TC247	Fraud Controls and Countermeasures SEMI T20: Traceability (semiconductor industry)	Nothing specific to SCI

(a) Understand threats, vulnerabilities and consequences associated with acquisition decisions.

(b) Develop and employ tools to technically and operationally mitigate risk across the lifecycle of products.

(c) Develop new acquisition policies and practices that reflect the complex global marketplace.

(d) Develop partnership with industry to develop and adopt supply chain and risk management standards and best practices.

CHINA

China has emphasised indigenous innovation, placing a high priority on investing in domestic research and development (R&D) in all segments in the ICT sector, i.e. chips, hardware and software.[11] China has adopted various administrative measures for the multi-level protection of information security (Multi-Level Protection Scheme or MLPS).[12] This imposes several requirements on security products destined for use in information systems including the following:-

(a) The entity that researches, develops and manufactures the product must be invested or controlled by Chinese citizens, legal persons or the state and have independent legal representation in China.

(b) The core technology and key components must have independent Chinese or indigenous intellectual property rights.

(c) The entity that develops and produces the product must confirm that the product contains no functions or programs that are intentionally designed as a vulnerability, backdoor or Trojan.

(d) Products that have been listed in the Certification and Accreditation Administration of People's Republic of China catalogues of information security products must acquire a certificate issued by the China Information Security Certificate Centre.

(e) For products containing encryption technology, the MPLS requires approval from the office of State Commercial Cryptographic Administration and no imported products with encryption functionality can be used without approval.

China is subjecting technical imports to heavy security scrutiny. It is investigating the encryption and data storage features of technology products sold by large foreign companies in the country. The authorities are focusing on whether the products pose a security threat.[13]

RUSSIA

Russia's approach is similar to China's, having implemented a certification regime that focuses on non-disclosed functionality. This intends to address concerns about backdoors and other functionality which might not be disclosed to users. The country is also creating a National Software Programme to reduce its dependence on foreign products and facilitate domestic production.[14] It had initiated plans to migrate its computer infrastructure from Windows to open source operating systems like Linux.

INDIA'S ELECTRONIC MANUFACTURING SCENE

In recent years, there has been an unprecedented demand for electronic goods and the requirement which was just $76 billion in 2013 is likely to cross $400 billion by 2020.[15]The domestic estimated production is expected to reach $104 billion by 2020, implying a huge gap of $296 billion. With an aim to build domestic capacity in electronic manufacturing, government has released the National Policy on Electronics (NPE) in 2012. The vision articulated in NPE is "to create a globally competitive electronics design and manufacturing industry to meet the country's need and source the international market."[16] The government has taken numerous initiatives for boosting domestic capacity in the electronics industry under the 'Make in India' programme. According to the Ministry of Electronics and Technology (MEITY), the semiconductor design market in India is expected to grow from $14.5 billion in 2015 to $52.58 in 2020.[17] Electronics manufacturing is one of the pillars of Digital India, which focuses on its promotion with the target of net zero imports by 2020.[18] Setting up two semiconductor projects in February 2014 has been approved by the government. These projects, were to be led by Jaiprakash Associates and HSMC Technologies India in collaboration with foreign firms, but even after 24 months of approval, no confirmation of their progress is available in the open domain.

One reason for India's inability to nurture its domestic electronics manufacturing lies in the inefficient labour market, unreliable power supply, and inadequate transportation infrastructure.[19]

Indigenous manufacturing is one of the many facets associated with supply chain integrity; even if a chip is manufactured in one country, the system for which it is required may need components/hardware manufactured/ assembled elsewhere. It is unlikely that in today's competitive global context, a country can fulfil its requirements from the domestic market alone because of inadequate expertise and wherewithal required for such ventures. The chip-making industry is highly competitive and has been around for about 50 years. It has well-established and well-entrenched players. China's state-funded Semiconductor Manufacturing International Corporation was founded in 2000, but it could not make any difference to chip-making industry's dynamics despite 16 years of state-sponsored effort.[20]

The National Cyber Security Policy promulgated in 2013 also articulates the method for reducing supply chain risks:

(a) Create and maintain testing infrastructure and facilities for IT security product evaluation and compliance verification as per global standards and practices.

(b) Build trusted relationships with product/system vendors and service providers for improving end-to-end supply chain security visibility.

(c) Create awareness of the threats, vulnerabilities and consequences of breach of security among entities for managing supply chain risks related to IT (products, systems or services) procurement.

The government has launched the Digital India and Startup India programmes to boost digital economy and local entrepreneurship ecosystem. Indian companies which saw growth a few years ago are today facing competition from international companies which have deep pockets and access to technology. The position can be compared with Europe and China. Europe is more or less an extension of the US digital economy while China carefully nurtured local digital businesses before allowing global companies to enter. China's digital economy will drive 21 percent of its GDP growth for the next 10 years, driven by the fact that its digital economy is indigenous and has employed and developed lakhs of highly skilled digital technology talent – many from rural parts of the country. Baidu and Tencent (the Google and Facebook of China)—two of hundreds of large internet companies in China – employ nearly 75,000 locals. Meanwhile, Europe struggles to develop real centres of innovation in technology. To have a thriving local digital economy and technology, the government must implement policies that enable and nurture local digital talent and give domestic companies a level-playing field.[21]

Challenges in Mitigating Supply Chain Risk: In the competitive global marketing environment, information systems and network products are dependent on a complex, globally distributed and interconnected supply chain comprising a mix of both government and private organisations. Because of the very nature of the problem, complete elimination of risks associated with supply chain is not feasible. Hence, the aim should be to manage the risks to minimise the vulnerability and threats associated with it. The main challenges being encountered in mitigating the supply chain are enumerated as under:

(a) **Cost:** The most preferred approach is to look inward, i.e. indigenous software, hardware. These involve an additional cost in R&D. And R&D is both capital and time-intensive. Are we as a nation willing to wait till an indigenous capability is developed, which may take decades? The economies of scale will also weigh against this route.

(b) **Public Private Partnerships (PPP):** It is a well-known fact that the private sector has expertise and the wherewithal that is not available with government. Hence involvement of private industry as a partner with government is of paramount importance. PPP is required in fields associated with incident sharing, R&D and remedial action.

(c) **Multiple Agencies:** Supply chain has multiple stakeholders spread across a vast spectrum of engineering, technology, procurement agencies, system integrator and maintenance organisations. It is not humanely feasible to have a security vetting of all processes and associated people.

(d) **Indigenous Capabilities in Manufacture:** Current indigenous capability is at a nascent stage. According to the Minister of Communication and Information Technology, the government will push for setting up chip-manufacturing facilities in India. In February 2014, the government approved setting up two electronic chip-making plants entailing an investment of about Rs 63,412 crore. The government also offered sops for electronics manufacturing in eight cities.[22] Given that initiatives will take time to fructify, however, the risk of malware looms large owing to India's dependence on imports.

(e) **Testing Facilities:** India has only one Standardisation Testing Quality and Certification (STQC) organisation. There are six levels of testing, but the Kolkata-based laboratory has the capability of testing only up to level 4 against the requirement of testing up to level 7. This limitation can jeopardise equipment safety because the supplier knows that there can be no full testing.

(f) **User Awareness:** The common user may not be aware about the implication of security features, and may want cheaper electronic items. The cheaper an item, the more are vulnerabilities. Most equipment, objects and services currently available do not have the level of data security that enables them to avoid an incident.

RECOMMENDATIONS:

Information security has a direct bearing on national security and the threat landscape is going to increase further with more and more systems getting interconnected. Following are some of the measures recommended for achieving self-reliance in core technologies and to mitigate the threats to information systems:

(a) Short-term Measures:

(i) **Follow Good Practices:** Study and implementation of good practices being followed in various nations/industries, especially defence procurement procedures. The present system being followed by the Ministry of Defence for procurement is in line with the Defence Procurement Procedure (DPP) manual, which is reviewed periodically. A cue can be taken from this by other government agencies for aligning their procurement processes.

(ii) **Import through a Central Agency:** A central agency may be nominated for importing the requirements of government agencies and for critical systems needed for national security-sensitive organisations. This organisation should function as a repository of database of firms which can be trusted for procurement. The agency should also share good practices being followed globally.

(iii) **Import Classification:** Categorising the import of electronic equipment into two types: Type A, meant for critical infrastructure, sensitive establishments; and Type B, meant for normal usage. Stringent procedures can be laid for Type A and less stringent measures for Type B imports.

(iv) **Audit:** Audit by an independent organisation from commencement of project implementation till its final launch must form a part of the contract.

(v) **Standards:** Specifying standard-based processes will go a long way in risk mitigation. Following specified global standards enhances both transparency and trust between buyer and the seller/system integrator. All efforts must be made to bring procurements up to internationally acceptable standards.

(vi) **Masking the End-User:** The ultimate user in case of sensitive departments may be hidden from the vendor/original equipment manufacturer). This practice will be useful while dealing with targeted insertion of malware.

(vii) **Malicious Code Certificate:** As per DPP 2013,[23] a certificate as under is to be provided by the vendor:

"This is to certify that the Hardware and the Software being offered, as part of the Contract, does not contain embedded malicious code that would activate procedures to:-

(a) Inhibit the desired and designed function of the equipment.

(b) Cause physical damage to the user or equipment during the exploitation.

(c) Tap information resident or transient in the equipment/ networks."

The firm will be considered to have breached the procurement contract in case physical damage, loss of information or infringements related to copyright and intellectual property rights are caused due to activation of malicious code in embedded software.

However, in case of breach of this clause, it is unlikely that vendor will accept the same. Moreover, by the time the vulnerability is known, the damage would have already been done. Nevertheless, it should form part of the deal as self-certification acts as a deterrent.

(viii) **Ask the Experts:** Associating experts with strategically important projects, from the request for information stage of procurement till its implementation.

(ix) **Encryption:** A sound encryption policy will facilitate trust among various agencies.

(x) **Incident Response:** It must be made mandatory to constitute computer emergency response teams for developing analysis and response capabilities.

Long-term Measures:

(a) **'Make in India':** The Make in India initiative should give impetus to the indigenous design, development and manufacture of system, sub system, components and software. This, however, should be restricted to sensitive portfolios only for the reasons mentioned above in the paper.

(b) **Testing Capability:** At present, there is only one STQC facility, that in Kolkata. This can be replicated in other locations. The fact that import of high-end equipment will only increase underlines the need for setting up more domestic testing facilities. Till indigenous facility is built, testing could be undertaken of random samples at third country premises.

(c) **Policy and Guidelines Formulation:** These are a must for developing indigenous capabilities as well as for streamlining import procedures, including testing of electronic inventory. Policies are the pillars for mutual trust between the government and private industry.

(d) **Data Protection:** Protection of a data is important, especially when the data available on the internet is residing outside the geographical boundaries of the country.

(e) **Network Providers:** Data rides on networks created by telecom service providers(TSPs). TSPs should be held accountable for providing communication channels free from malware infections. TSPs should devise measures to ensure that only malware-free devices are hooked to their network.

(f) **Public- Private Partnerships:** The expertise lies with private industry while formulation of policies is the domain of the government.

(g) **Trusted Agency:** Incorporating the Defence Research and Development Organization and Department of Electronics and Information Technology in strategic projects from conceptual stage to mitigate the problems.

CONCLUSION

India is experiencing a rapid transition to a digital technology-driven country. Although this shift carries enormous possibilities for the country's growth, it also exposes it to cyber threats. The government has launched 'Digital India' and 'Make in India' programmes to digitally empower the society, but it has apparently failed to articulate on India's data and digital sovereignty.[24] As the world becomes increasingly interconnected, the protection of privacy, data and digital infrastructure of the nation would assume utmost importance. These factors would play a vital role in its digital sovereignty—or believing that a nation has attained e-Swaraj.

ENDNOTES:

1. Digital India: Unleashing Prosperity", Deloitte, accessed March 1, 2016, https://www2.deloitte.com/content/dam/Deloitte/in/Documents/technology-media-telecommunications/in-tmt-tele-tech-2015-noexp.pdf
2. "Supply Chain Integrity -An overview of the ICT Supply Chain risks and challenges, and vision for the way forward (2015), accessed March 1, 2016, https://www.enisa.europa.eu/publications/sci-2015
3. "*From The World Is Flat* by Thomas Friedman Dell Inspiron 600m Notebook: Key Components and Suppliers", Do You Have The Right Practices In Your Cyber Supply Chain Tool Box? , NDIA Systems Engineering Conference October 29, 2014, accessed September 23, 2016, http://www.dtic.mil/ndia/2014system/16888WedTrack1Moss.pdf
4. "US Govt Accountability Office Report to Congressional Requesters,,IT Supply Chain, National Security Related Agency Need to Better Address Risks", Government Accountability Office, accessed September 23, 2016, http://www.gao.gov/assets/590/589568.pdf
5. "Seizing Opportunity Through License Compliance, BSA Global Software Survey, May 2016", BSA The Sofware Alliance, accessed August 23, 2016, http://globalstudy.bsa.org/2016/downloads/studies/BSA_GSS_US.pdf
6. *Ibid*
7. "Supply Chain Integrity -An overview of the ICT Supply Chain risks and challenges, and vision for the way forward (2015), accessed March 1, 2016, https://www.enisa.europa.eu/publications/sci-2015
8. "The Comprehensive National Cybersecurity Initiative", The White House, ,accessed August 23,2016, https://www.whitehouse.gov/sites/default/files/cybersecurity.pdf
9. Cyber Supply Chain Risk Management white paper.pdf by Microsoft
10. "Securing Our Cyber Frontiers NACOM-DSCI Cyber security Advisory Group Report", DSCI, accessed September 23, 2016, https://www.dsci.in/sites/default/files/NASSCOM-DSCI%20Cyber%20Security%20Advisory%20Group%20(CSAG)%20Report.pdf

11. Cyber Supply Chain Risk Management white paper.pdf by Microsoft
12. *Ibid.*
13. “China Subjects Tech Imports to Heavy Security Scrutiny”, TechNewsWorld, accessed August 20, 2016, http://www.technewsworld.com/story/83526.html
14. Cyber Supply Chain Risk Management white paper.pdf by Microsoft
15. “Semiconductor Industry in India”, IBEF, accessed March 1, 2016, http://www.ibef.org/industry/semiconductors.aspx
16. “Electronics System Design & Manufacturing”, Ministry of Electronics and Information Technology ,accessed March 1, 2016, http://www.deity.gov.in/esdm
17. “Semiconductor Industry in India”, IBEF, accessed March 1, 2016, http://www.ibef.org/industry/semiconductors.aspx
18. “Electronics Manufacturing”, Digital India, accessed March 1, 2016, http://www.digitalindia.gov.in/content/electronics-manufacturing
19. “India Wants to Build its Own Chips to Satisfy Electronics Demand”, Bloomberg, accessed September 23, 2016, http://www.bloomberg.com/news/articles/2014-02-27/india-wants-to-build-its-own-chips-to-satisfy-electronics-demand
20. “Does India really need a $5 billion semiconductor unit?”, The Economic Times, accessed February 15, 2016, http://economictimes.indiatimes.com/tech/hardware/does-india-really-need-a-5-billion-semiconductor-unit/articleshow/48156199.cms
21. “Digital India is dying: Without intervention, Digital India looks to simply be a colony of US and China”, The Times of India, accessed August 22, 2016, http://blogs.timesofindia.indiatimes.com/toi-editorials/digital-india-is-dying-without-intervention-digital-india-looks-to-simply-be-a-colony-of-us-and-china/
22. “Government to offer sops for electronics manufacturing in 8 cities: Ravi Shankar Prasad”, The Indian Express, accessed June 17, 2014, http://indianexpress.com/article/business/economy/government-to-offer-sops-for-electronics-manufacturing-in-8-cities-ravi-shankar-prasad/
23. “Defence Procurement Procedure 2013”, Ministry of Defence, accessed March 12, 2016, http://mod.nic.in/writereaddata/DPP2013.pdf
24. “The Valley in Digital India”, The Hindu, Accessed March 5, 2016, http://www.thehindu.com/business/Industry/the-valley-in-digital-india/article6515038.ece

ABOUT THE AUTHOR

Col. R K Sharma holds the Chair of Excellence for Defence Forces at the Observer Research Foundation, New Delhi.

ORF OBSERVER RESEARCH FOUNDATION

Ideas • Forums • Leadership • Impact

20, Rouse Avenue Institutional Area, New Delhi - 110 002, INDIA
Ph. : +91-11-43520020, 30220020. Fax : +91-11-43520003, 23210773
E-mail: contactus@orfonline.org
Website: www.orfonline.org