CYBER ATTACKS VIA HARDWARE EXPLOITATION: AN INSIDIOUS AND ELUSIVE MENACE

ASHISH GUPTA

At the heart of the ubiquitous internet and incessantly active cyber space, which sets in motion, and sustains, the momentum of the juggernaut of modern times, is a complex set-up of micro-processing chips. These chips, hidden from the functional, resplendent and vibrant exterior of the cyber world, act as arteries, intricately entwined and woven, and provide it with the necessary sustenance and subsistence. Microchips are the bedrock upon which the digital world has been conceived, nurtured and developed to became an all encompassing entity providing the yarn for weaving the fabric of modern society. The micro-electronics industry, the manufacturer and supplier of hardware capability, drives the anthropocentric nature of cyber space and provides technical scaffolding to achieve greater penetration of the digital services and media in societal interactions and functioning.

The invention of the first Integrated Circuit (IC) in 1958 by Jack Kilby of Texas Instruments,[1] marked the beginning of the age of the microchip. These early chips consisted of a few transistors, diodes, resistors and capacitors placed onto a slice of germanium and linked by gold wires, and were exorbitantly priced. In over a decade, microchips have become the foundation for the realm of high speed computing. Intuitively realising

Group Captain **Ashish Gupta** is Senior Fellow at the Centre for Air Power Studies, New Delhi.

[1] Walt Kester, *The Data Conversion Handbook* (Massachusetts: Elsevier, 2005), p.259.

Armed with the power of the internet, with ingenious and experimental methods, cyber criminals have leveraged vulnerabilities, loopholes, technology shortcomings and glitches, back doors, gullibility of users for financial frauds, identity thefts, theft of state secrets and corporate espionage.

the characteristics and dimensions of this development, in 1970, Gordon E. Moore, almost prophetically described the relationship between the growth of processing power and the increased capacity of microchips. The iconic Moore's Law states that the overall processing power for computers will double every two years.[2] In other words, the number of transistors on a Central Processing Unit (CPU) would double every two years. In 2000, the number of transistors in the CPU numbered 37.5 million, while in 2009, the number went up to an outstanding 904 million.[3]

The growth and proliferation of microprocessing chips pose a new kind of challenge, further exacerbating the chaos to the already tumultuous field of cyber security. Armed with the power of the internet, with ingenious and experimental methods, cyber criminals have leveraged vulnerabilities, loopholes, technology shortcomings and glitches, back doors, gullibility of users for financial frauds, identity thefts, theft of state secrets and corporate espionage. The coalescence of criminal intent and technology has added another vulnerability dimension to the rapidly expanding repertoire of cyber crime and espionage activities. In the ongoing contest between cyber security enforcers and cyber criminals, new tools, techniques and methodologies are ever evolving and are limited only by technology, imagination and ingenuity. A new cyber threat, looming large over the industry, military and critical infrastructure is purposeful manipulation of processing chips during the manufacturing process to provide remote access or take control of a system to shut it down, to steal data or to corrupt it. The acts of cyber crime have reached pandemic proportions worldwide and are causing colossal financial losses, erosion

[2] Moore's Law, "How Overall Computing Power of Computers Will Double Every Two Years," http://www.mooreslaw.org/. Accessed on July 30, 2015.

[3] Ibid.

of reputations and loss of intellectual property. While software security rules the roost as a deterrent and for prevention of breaches of cyber security, hardware security has not been accorded the requisite importance and has generally been relegated to a footnote rather than being assimilated as a core subject in any debate on cyber security.

The design and post design fabrication of these chips have become so intricate and complex that efforts to understand every detail of their architecture overwhelms human intelligence and diligence.

Since the early 1980s, from just a handful of known companies and even fewer chip designers, the microchip industry has made great strides commensurate with the advances in design and fabrication and ever-increasing worldwide demand for sophisticated chips. Today, to keep pace with demands and to reap commercial gains, these companies are collectively creating more than 5,000 new designs each year.[4] These companies have spread their Research and Development (R&D) operations and production across the globe in various countries, based on business opportunities and commercial imperatives as well as the availability of a pool of skilled labour. The design and post design fabrication of these chips have become so intricate and complex that efforts to understand every detail of their architecture overwhelms human intelligence and diligence. These developments, from the perspective of growth and penetration of computer devices, mobile phones and other net enabled devices, are positive and empowering. New manufacturing processes, adoption of new technology and global competition have brought down the cost while adding higher processing power. However, the associated complexities of chips and globally distributed design teams have proportionally increased the opportunities to embed hidden malicious functionality in the chips.[5]

A modern large chip can be subjected to fast automated testing methods

[4] US Committee on the Offshoring of Engineering, *Facts, Unknowns, and Potential Implications* (National Academies Press), p.169.

[5] John Villasenor, "Compromised By Design? Securing the Defense Electronics Supply Chain," Executive Summary, Centre for 21st Century Security and Intelligence at Brookings, November 2013.

to carry out a functionality test, but even this will give inconclusive results as the fastest automated testing would take years to simulate each and every task a chip is capable of performing. Nowadays, modern chips are tested using statistical techniques, in which random samples are subjected to random inputs, and the results are inferred as statistically probable. The statistical model is effective in indentifying the design flaw. However, intentionally introduced design flaws are much harder to find as these may contain a latent functionality that may be triggered after months or years and will remain invisible during testing.

Those who were buoyed by the availability of rather inexpensive highly sophisticated and easily programmable micro chips have been rudely shaken by the episodes and instances of deliberate insertion of malicious functionality in the micro-chips and their exploitation. A detailed examination and analysis of recent major cases will provide an understanding of the severity and consequences of hardware-level vulnerabilities' exploitation.

- In 2011, a small US company was able to win the contract for the supply of more than US$15.8 million in computer parts to various US government organisations, including the US Navy. Many of the electronic items were labelled as "military-grade" and destined for use in advanced fighters, radar systems, and missiles. It was later learned that almost all of these parts were manufactured in China at a single factory, using inferior and recycled materials. The products bore the false markings of well-known chip-makers such as Intel, Texas Instruments and Motorola.[6] Though the bulk of the counterfeit parts was seized and impounded, those which remained in use posed a wide range of existential risks of equipment damage, personal injury and possible death due to malfunction at a critical juncture. The Naval Air Systems Command, without addressing whether some of the counterfeit chips remained in use or circulation, had warned that any failures had the potential to ground military aircraft or prompt mistaken shoot-downs of friendly planes.[7] In order to fathom the monumental impact these counterfeit chips had on national security,

[6] "Counterfeit Chips Plague Pentagon Weapons Systems ", http://www.publicintegrity.org/2011/11/07/7323/counterfeit-chips-plague-pentagon-weapons-systems

[7] Ibid.

investigators at the US Government Accountability Office (GAO), posing as chip brokers, successfully purchased counterfeit circuits from Chinese suppliers that were labelled for use in military systems. It was also reported by GAO that:

- Counterfeit routers with high failure rates had been sold to the US Navy,
- Counterfeit microprocessors had been sold to the air force for use on F-15 flight control computers,
- Oscillators with a "high failure rate" had been sold by a prohibited supplier for use by thousands of air force and navy navigation systems. These failures "could prevent some unmanned systems from returning from their missions,"[8]
- The Electronic Warfare (EW) suite of the F-35 strike fighter uses industry-standard Field Programmable Gate Arrays (FPGAs) to simplify integration and future evolution. [9] A field-programmable gate array is an IC that can be programmed in the field after manufacture. A single FPGA can replace thousands of discrete components by incorporating millions of logic gates in a single IC chip. More than three-quarters of these field programmable gate arrays in the F-35 strike fighter are made in China and Taiwan.[10] If the hardware of these chips is subtly modified to escape detection during quality checks, a trigger, at a later chosen time, to extract tactical or strategic advantage, can effectively degrade or disable the chips and the systems that depend on these. It is also possible to implant an internal time bomb during the inception stage of the chip to trigger a shutdown at someone's date and time of choosing.
- In 2011, when Huawei and ZTE, the top two Chinese telecommunications equipment manufacturers sought to market their equipment to the US telecommunications infrastructure, the House Permanent Select Committee on Intelligence initiated investigations to inquire into the

[8] United States Government Accountability Office, *DOD Should Leverage Ongoing Initiatives in Developing Its Program to Mitigate Risk of Counterfeit Parts* , Belva Martin (Washington D.C.: :Government Printing Office, 2010), p.9.

[9] "F-35 Electronic Warfare Suite: More Than Self-Protection ", http://www.aviationtoday.com/av/military/F-35-Electronic-Warfare-Suite-More-Than-Self-Protection_845.html#.VNrV5ctO7ug

[10] P W Singer, "Hacked Hardware Could Cause the Next big Security Breach", *Popular Science,* March 2015.

The committee concluded that risks associated with Huawei's and ZTE's provision of equipment to US critical infrastructure could undermine core US national security interests. In the report, it was also unambiguously stated that "when those companies seek to control the market for sensitive equipment and infrastructure that could be used for spying and other malicious purposes, the lack of market diversity becomes a national concern for the United States and other countries."

counter-intelligence and security threats posed by these companies doing business in the United States. The committee concluded that risks associated with Huawei's and ZTE's provision of equipment to US critical infrastructure could undermine core US national security interests.[11] In the report, it was also unambiguously stated that "when those companies seek to control the market for sensitive equipment and infrastructure that could be used for spying and other malicious purposes, the lack of market diversity becomes a national concern for the United States and other countries."[12] Some of the concerns stem from the past affiliations of Huawei's founder, Ren Zhengfei. Although the company is selectively mute about his background, some information garnered from other sources indicates that Ren Zhengfei attended the Chongqing University of Civil Engineering and Architecture and served in the People's Liberation Army's (PLA's) engineering corps, reportedly in its information technology research unit. He rose to the position of deputy director but without a military rank. He left the army and moved to Shenzhen, where he set up Huawei in 1987. Though Huawei has projected itself as a company with a explicit commercial intent, the former association of its founder with the PLA and Huawei's refusal to provide details on its R&D programmes and other documents undermine its claim of not working in collusion with the Chinese military or intelligence services. The intelligence community is abuzz with speculation that there

[11] US House of Representatives 112th Congress, *Investigative Report on the US National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE* (2012).

[12] Ibid., p.2.

is more to Huawei's rise than innovation and technology breakthroughs. It is widely believed that its expansion is attributable to a heavy subsidy by the Chinese government, eager to use it as a Trojan horse for infiltration into more and more foreign networks.[13]

- In the year 2007, the Taiwanese Investigation Bureau found that out that Maxtor portable hard discs produced by Seagate Technology for sale in Taiwan contained Trojan horse viruses. The Investigation Bureau said the tainted portable hard drives automatically uploaded any information saved on the computer to Beijing websites without the user's knowledge. It was speculated that deliberate "contamination" was introduced when the products were with Chinese sub-contractors during the manufacturing process. [14]

In the year 2007, the Taiwanese Investigation Bureau found out that Maxtor portable hard discs produced by Seagate Technology for sale in Taiwan contained Trojan horse viruses. The Investigation Bureau said the tainted portable hard drives automatically uploaded any information saved on the computer to Beijing websites without the user's knowledge.

- At one time, the powerful but surprisingly cheap Chinese-made Android Star N9500 Smartphone was considered a sterling example of the Chinese ability to provide state-of-the-art gadgets at surprisingly low prices. Little did the consumers know that this was being used to distribute a dangerous factory-installed Trojan, until discovered by the German security firm, G Data. It allegedly contained the Uupay D Trojan, embedded and disguised as the Google Play Store app. G Data's Christian Geschkat revealed, "Unfortunately, removing the Trojan is not possible as it is part of the device's firmware and apps that fall into this category cannot be deleted. This includes the fake Google Play Store app of the

[13] "Huawei : The Company that Spooked the World," *The Economist* , August 4, 2012, http://www.economist.com/node/21559929.

[14] "Chinese Subcontractors Blamed for Trojan Horses," *Taipei Times*, December 11, 2007, http://www.taipeitimes.com/News/taiwan/archives/2007/11/12/2003387447

N9500."[15]

- Since mid-2013, the US National Security Agency (NSA), in the garb of national security, embarked on a mass surveillance programme codenamed the "PRISM program". The scope, magnitude and technological sophistication required for the programme was colossal even by American standards. The offshoot of the PRISM programme was a repertoire of sophisticated digital tools as listed in the "NSA ANT Catalogue". The catalogue bears testimony to the notorious credentials of the US intelligence agency to spy on its targets. "The leaked NSA ANT Catalogue is a 50-page document created in 2008. Its list goes like a mail-order catalogue of digital tools, from which the employees of NSA can order technologies from the ANT division to use against its targets. The Advanced/ Access Network Technology (ANT) division is part of the NSA's Tailored Access Operations (TAO) Department and they are specialized in covert data-mining and data-skimming operations, especially on specific difficult targets."[16] The range of digital tools developed by ANT uses seemingly innocuous and ubiquitous digital devices such as monitors, mobile phones, cables, USBs, routers, servers, etc. The nightmarish reality became all too pronounced with the knowledge that these products were implanted in the most widely used US brands around the world like Apple, Cisco, Dell, Juniper Networks, Maxtor, Seagate, and Western Digital.[17] In spite of formal denials issued by these companies, there is little doubt that their devices were used by the NSA for digital eavesdropping for covert espionage purposes.

UNDERSTANDING CHIP BUILDING ECOSYSTEM

During the nascent growth of the semi-conductor industry, all the requisite tasks that went into making a chip, ranging from specification, design,

[15] "Chinese Star N9500 Android Smartphone Contains Factory-Installed Trojan, says Security Firm", http://www.techworld.com/news/security/chinese-star-n9500-android-smartphone-contains-factory-installed-malware-says-security-firm-3525608/

[16] Jacob Appelbaum, et. al., "Die Klempner aus San Antonio", *Der Spiegel*, January 2014.

[17] Jacob Appelbaum, et. al., "Shopping for Spy Gear: Catalog Advertises NSA Toolbox", *Spiegel Online International*, December 29, 2013, at http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html. Accessed on July 30, 2015.

manufacturing and testing were undertaken by a single company. Some of the companies still operate in this manner. However, in chip manufacturing, as *functionality and complexity* increased, the costs of building manufacturing facilities went up exponentially. In late 2012, it was reported that the South Korean Electronics giant Samsung Electronics Co. Ltd. would spend US$ 7 billion on a NAND flash wafer fab (fabrication) in Xian, a city in the northwest of China.[18] In research conducted by Gartner, Inc., it was projected that the "costs of manufacturing equipment will drive the average cost of semiconductor fabs to between 15 billion US dollars and 20 billion US dollars by 2020."[19] The prohibitive high costs in having one's own manufacturing capability have spurred the growth of external manufacturing companies. These external facilities known the "foundries" for manufacturing semi-conductor devices, facilitate a semi-conductor company to function and grow with limited resources and capital, without investing heavily in the manufacturing process. In the semi-conductor manufacturing realm, the design and sale of semi-conductor chips while outsourcing the fabrication is termed as 'fabless' manufacturing. In the year 2012, out of 50 top semi-conductor companies, 13 were 'fabless' including Qualcomm, Broadcom, AMD and Nvidia. In 2013, revenue of as much as US$ 78.1 billion came from the fabless IC business and the top 13 foundries accounted for 91 percent of total foundry sales. Out of these 13 foundries, five are Taiwanese while two are Chinese. [20] Overall, the five Taiwanese foundries secured about 60 percent of the global market last year. The remaining 40 percent went to three South Korean companies (Samsung Electronics Co, Dongbu Electronics and Magna Chip Semiconductor), two Chinese companies (Semiconductor Manufacturing International Corp and Hua Hong Grace Semiconductor Corp), two US (Global Foundries and IBM Corp) and one Israeli chipmaker,

[18] EET Asia, "Samsung Plans $7B NAND Fab in China," http://www.eetasia.com/articleLogin.do?artId=8800664879&fromWhere=/ART_8800664879_499486_NT_f709dbeb.HTM&catId=499486&newsType=NT&pageNo=null&encode=f709dbeb. Accessed on July 30, 2015.

[19] Gartner, "Market Trends: Rising Costs of Production Limit Availability of Leading-Edge Fabs", https://www.gartner.com/doc/2163515/market-trends-rising-costs-production. Accessed on July 30, 2015.

[20] Bill McClean, "Top 13 Foundries Account for 91% of Total Foundry Sales in 2013," *IC Insights Research Bulletin*, January 28, 2014, http://www.icinsights.com/data/articles/documents/640.pdf. Accessed on July 30, 2015.

TowerJazz Semi-conductor, among others.[21] Today, the IC design continues to be the fastest growing segment of China's semi-conductor industry. In a decade from 2003 to 2013, China's IC design industry has grown from US$ 541 million to record revenues of US$ 13.2 billion in the year 2013, with an impressive 33 percent growth rate.[22] Similarly, during the past ten years, the top Chinese semi-conductor companies have grown from 26 companies with average revenues of US$ 39 million to 50 companies with average revenues of US$226 million.[23]

What appears to be a sound business strategy is a real challenge for national security due to lack of trustworthiness and quality assurance for components, which might find their way into critical military and infrastructure applications.

The microelectronics industry restructuring has seen horizontal consolidation through elimination of redundancies and capitalisation of synergies, replacing the vertically integrated structure which was slackening the pace of innovation. This restructuring is also driven by the commercial imperative of spreading the capital risks over multiple stakeholders. What appears to be a sound business strategy is a real challenge for national security due to lack of trustworthiness and quality assurance for components, which might find their way into critical military and infrastructure applications. Trustworthiness includes the confidence that the classified or mission-critical information contained in the chip designs is not compromised, the reliability is not degraded and unintended design elements are not inserted in the chips.[24]

Another dimension, which adds more complexity to the debate, is that the weapon systems and military hardware are designed, produced and

[21] Kevin Chen, "Powerchip Gains in Foundry, TSMC Still First," *Taipei Times*, February 5, 2014, http://www.taipeitimes.com/News/biz/archives/2014/02/05/2003582752. Accessed on July 30, 2015.

[22] Raman Chitkara, "A Decade of Unprecedented Growth China's Impact on the Semiconductor Industry 2014 Update," *PwC*, August 2014, http://www.pwc.com/gx/en/technology/chinas-impact-on-semiconductor-industry/assets/2014-section-2.pdf

[23] Ibid.

[24] US Defence Science Board, Dr. William Howard et al., *Report on Defense Science Board Task Force on High Performance Microchip Supply* (Washington D.C. :Government Printing Office, 2005),p.3.

procured based on their envisaged final capability, range, endurance, firepower and sophistication. The acquisition process of military hardware does not include detailed specifications for components; rather, it focusses on achievable functionality as per the specifications. A military system is made up of various sub-systems designed to carry out a specific task and the individual circuits in the sub-system are mostly fabricated with commercially available ICs. These ICs are procured from the global marketplace, partly due to the cost factor and partly due to copyrights issues. It, therefore, becomes vital to ensure that defence systems and mission-critical products are designed and procured with appropriate oversight and controls to ensure their mission functionality and operational availability at all times.

But, as with all technological advancements, its all encompassing penetration and integration into all the facets of social, financial and military activities, brings to the fore the associated challenges, including new vulnerabilities, new attack vectors and perhaps most concerning of all, an almost innate ability to use remote access to cause physical destruction.

CHALLENGE OF UNBRIDLED PROLIFERATION OF IOT DEVICES

The rapid influx of smart, adaptive, and connected devices—the "Internet of Things" (IoT)—virtually across all sectors, is happening at a speed that far outpaces earlier technological developments. The development of IoT is directly linked with accruement of significant societal benefits through enhanced efficiencies, improved reliability and resilience, prompt medical care, detection of faults, and more. But, as with all technological advancements, its all encompassing penetration and integration into all the facets of social, financial and military activities, brings to the fore the associated challenges, including new vulnerabilities, new attack vectors and perhaps most concerning of all, an almost innate ability to use remote access to cause physical destruction. In its report, the US National Security Telecommunications Advisory Committee (NSTAC) described

IoT as an expansion of the global infrastructure through existing and evolving interoperable information and communication technologies that incorporate the interconnection of physical and virtual systems to enable new and automated capabilities.[25] The rapid and unhindered growth of IoT will witness an exponential expansion in attack surfaces due to increased dependencies, the vast number of devices and associated interconnections and the changed threat landscape, with existential and potential increase in kinetic-focussed cyber attacks.

- **By 2020, it is estimated that 50 billion devices will be connected to the internet.**[26] These devices will exchange massive amounts of data and as technical sophistication improves, these devices will be able to make intelligent decisions autonomously and will share information via embedded machine-to-machine communications with other internet-capable devices.[27] The defence industry is probably the harbinger of this revolution and had been at the forefront in development and adoption of IoT before it gained momentum as a commercially viable and technologically workable system. The tactical data is being shared among a number of platforms-planes, ground vehicles, ships, spacecraft and weapon systems which have been networked. At this stage, the types and quantum of vulnerabilities likely to emerge due to IoT dependence **will be speculative, and the challenges to rein in the cumulative impacts due to exploitation of such vulnerabilities will increase.**
- Irrespective of the use and the users of IoT devices, the thread of commonality among all the devices will be their irrevocable dependence on microchips. A deliberate attempt to make a chip function in an unintended fashion poses unfathomable risks. For an individual, the risk may be trivial, ranging from irritation to inconvenience. The scenario will be much more frightening when evaluated over the whole spectrum of IoT services. IoT health care devices, including implantable ones,

[25] National Security Telecommunications Advisory Committee, *Report to the President on the Internet of Things*, DHS-2014-0048 (Washington D.C. : Government Printing Office, 2014), p.1.

[26] Dave Evans, "The Internet of Things: How the Next Evolution of the Internet Is Changing Everything", *CISCO White Paper*, April 2011, https://www.cisco.com/web/ about/ac79/ docs/ innov/ IoT_IBSG_0411FINAL.pdf. Accessed on July 30, 2015.

[27] Ibid.

for example, will have built-in connectivity and if compromised to malfunction, could lead to patient deaths. In January 2014, the Director of US National Intelligence (DNI) stated before Congress stated that in "the cross-networking of personal data devices, medical devices, and hospital networks, cyber vulnerabilities might play unanticipated roles in patient outcomes."[28] The encroaching inroads made by IoT will make personal privacy a thing of the past. The potential national security implications that could arise from the compromise or malfunction of IoT devices embedded in different critical infrastructure systems will be of enormous proportions. Many of the present critical infrastructures are made up of automated and adaptive devices, incessantly collecting and analysing data and then making automated decisions.

Ameliorating the threats emanating from malicious exploitation of vulnerabilities in hardware, introduced deliberately or discovered by serendipity, requires multi-pronged approaches. From a national security-standpoint, manufacturers and suppliers with a high trust quotient must exclusively be entrusted with the responsibility of supplying the hardware. Trust cannot be added to integrated circuits after fabrication; electrical testing and reverse engineering cannot be relied upon to detect undesired alterations in military integrated circuits.[29] An equally important and **far-reaching safeguard against such threats is to dispense with dependence on** off-shore manufactured microelectronic components and rely on in-house expertise to fulfil the needs of ICs, microelectronic components and microchips across the whole spectrum of electronic and microelectronic technologies. In the Indian context, in spite of the country's proven technological prowess and enviable pool of highly qualified, talented professional, the road to realisation of these objectives is not without challenges. Some of these are;

- The production of custom-made hardware components with unique

[28] US Department of National Intelligence, James R. Clapper, *Worldwide Threat Assessment of the US Intelligence Community Senate Select Committee on Intelligence*, Statement for the Record (Washington D.C. :Government Printing Office, 2014), p.3.

[29] n.24, p.3.

functionalities is not commercially viable. The incentives to rope in capital and resources for manufacturing of specific to requirement ICs in limited numbers are inadequate and insufficient. Besides, the chip design ecosystem has become much more globalised and complicated and is driven by economic imperatives, competitive markets, competent and adaptable workforce and demand-based production. Efforts to establish manufacturing pockets of ICs isolated from the global ecosystem will become a formidable challenge and will not accrue proportionate benefits in the long run.

- Even if the requirement of trusted hardware devices is fulfilled by government owned or operated facilities specifically set up for this, keeping pace with technology evolution and maintaining a competitive parity will not be easy. The cost of keeping such facilities perennially near to the state-of-the-art commensurate with their private counterparts, will be prohibitively high. Besides, in response to the demands for new features and capabilities, these facilities will find themselves inadequately equipped or on the verge of technological obsolescence.

In India, at present, approximately 65 percent of the demand for electronics products is met by imports, which is likely to grow from US $28 billion in 2011 to US $ 42 billion this year. The government has instituted a number of policies aimed at holistic development of the Electronics System and Design (ESDM) industry and fostering the growth of the Indian electronics ecosystem.

In India, at present, approximately 65 percent of the demand for electronics products is met by imports, which is likely to grow from US $28 billion in 2011 to US $ 42 billion this year.[30] The government has instituted a number of policies aimed at holistic development of the Electronics System and Design (ESDM) industry and fostering the growth of the Indian electronics

[30] India Electronic & Semiconductor Association, "Indian ESDM Market: Analysis of Opportunity and Growth Plan, An IESA - Frost & Sullivan Report", available online at http://www.iesaonline.org/downloads/IESA-FS-report-Indian-ESDM-Market.pdf

ecosystem. The government instituted National Policy on Electronics (NPE) aims to create an ecosystem for a globally competitive ESDM sector by attracting investments of about US $ 100 billion and generating employment for around 28 million people at various levels.[31] The policy also aims for the Indian ESDM sector to develop core competencies in strategic and core infrastructure sectors like telecommunications, automobiles, avionics, industrial, medical, solar, information and broadcasting, railways, intelligent transport systems, etc.

CONCLUSION

The ever changing landscape of the threat ecosystem calls for innovative, proactive and dynamic posturing and preventive and migration strategies with specific regard to technological changes and developments. The existing governmental support, policy formulation and industry outlook towards reducing off-shore dependency and achieving self-reliance in indigenous designing, fabrication and production of semi-conductor devices are sincere and well-founded. However, the global competitiveness, fuelled by technological advances and sweeping innovations, is hindering the prospect of a fully self-reliant ecosystem capable of catering to the myriad requirements of military hardware. Besides, the overdependence on exports of military hardware from a wide range of defence equipment suppliers, spread across many countries, is a major roadblock in the realisation of this objective. The foreign suppliers are either not mandated to provide the details of microchips or are reluctant to part with this information to thwart emulation/ imitation efforts by the process of reverse engineering. At times,

The foreign suppliers are either not mandated to provide the details of microchips or are reluctant to part with this information to thwart emulation/ imitation efforts by the process of reverse engineering. At times, even the identification marks on these chips are erased or deliberately etched away to make even recognition an impossible task, let alone functionality determination.

[31] Ibid.

even the identification marks on these chips are erased or deliberately etched away to make even recognition an impossible task, let alone functionality determination.

Hence, there is a need to strengthen existing awareness and training programmes among all the stakeholders to widen their understanding of the possible risks and vulnerabilities associated with hardware devices. Role-specific responsibilities must be clearly laid down for those involved in the design, production, procurement, and operation of military hardware. A mission critical device must be checked for the whole range of possible functions by way of simulation. The integration of collaborative engagements between the government and industry, leveraging of industry capabilities and academia's expertise and insight are some of the measures capable of ameliorating the threat emanating from hardware vulnerabilities.