Vol. XII & Issue No. 7 July - 2019
INDUSTRIAL ENGINEERING JOURNAL

APPROACH TO HANDLING CYBER SECURITY RISKS IN SUPPLY CHAIN OF DEFENCE SECTOR

J Angel Reuben
Nilesh Ware

ABSTRACT:

The primary objective of this paper is to understand the various sources of supply chain poisoning, and then provides some mitigation strategies, finally, a framework with recommendations for mitigation to cyber security risks in supply chain in defence has been worked out based on the research carried out. Supply chain is the backbone of any organization, especially more critical in defence since it directly impacts the national security. It is observed that more the process in the supply chain more the exposure to various risks, especially in market competition the cyber security risk are vital. Supply chains are flexible and producers from different countries may be used, so that two fully assembled devices may have different supply chains, with different component manufacturers. While this practice minimizes costs and maximizes production capability, it makes it more difficult to assure security and quality. The research is carried out based on comprehensive literature survey followed by interviewing procurement and cyber security personnel from armed forces, DRDO, industry and Government. India is vulnerable since the defence industry is dependent on the import of advanced technology equipment.

KEYWORDS: *Supply Chain Poisoning, embedded system security, defence equipment, vulnerability, threats.*

1. INTRODUCTION

1.1 Background

Imagine a scenario where the air defence radar doesn't detect any adversary targets in a specific sector or clutters the moment there is an intrusion by an adversary or a delay of milliseconds inserted during transmission of air defence data. These are all possible in the current day cyber-attack scenario, wherein each nation state is in constant state of attack (cyber) by the adversary. The supply chain poisoning can be carried out during manufacturing, assembly, and distribution of hardware, software, and services. When[1] the threats are deliberately created in the supply chain with an intention to exploit the threat at an opportune time, then it is termed as supply chain poisoning.

1.2 Complexity of IT Systems

Twenty first century is the age of information technology and digital assets. The world is enjoying the fruits delivered through the latest technologies being developed and especially related with the field of communication and computers or ICT The developed nations are mostly producing the ICT devices and controlling the big companies and organizations who are responsible for Internet services world over. This facilitates them in carrying out surveillance over almost all countries/ citizens of the world. Electronic hardware used in Defence systems is procured through vendors that use complex supply chains, which are thus vulnerable to insertion of malicious hardware or embedded software that may be used to compromise weapons and information systems. Exploits that have been discovered, as well as vulnerabilities that have been analysed make it clear that this problem is significant. For example, normal counterfeiting operations are motivated by profit, but counterfeiters may also provide the exploiter with a convenient channel that may be used to introduce malicious exploits into products. On the other hand, delivery of hardware exploits to intended targets may be more reliable if the targets receive their equipment from suppliers who are considered trustworthy. Attempts to screen out counterfeits requires expensive equipment. An US survey estimated that as many as 1 in 10 IT products purchased were counterfeit; a recent study of defence electronics reported that detected counterfeiting nearly doubled. The extent of malicious hardware implants is unknown.

1.3 Critical Information Infrastructure (CII)

Critical Infrastructures [2](CIs) have become dependent on ICT technologies (such as networking, telecommunications, cloud, sensor and SCADA technologies), thereby rendering Critical Information Infrastructures (CIIs) a vital element of their functioning. Likewise, attacks in the Industrial Control Systems (ICSs) (e.g. supervisory control, SCADA, distributed control systems and programmable logic controllers) may cause disruption or damage of CIIs and even worse they may cause loss of life, steal data/material and destruction of weapon systems. Thus countries who are dependent on import for supply of IT devices and networking equipment will remain victims of supply chain poisoning. These countries cannot trust these devices especially when they are being used for sensitive applications. The national security could be jeopardised in case of non-functioning of these devices as well as breach of sensitive data being processed through these devices.

1.4 Motivation for study:

The reasons of how and why the supply chain poisoning happens have been introduced, the most important thing is how to overcome this supply chain attacks and protect the national security and maintain confidentiality, reliability and integrity of

the defence systems and its data. The primary objective of this paper is to understand the various sources of supply chain poisoning, study the mitigation strategies adopted by organisations and countries around the world and propose a mitigation plan framework.

2. LITERATURE REVIEW

2.1 Vectors of Supply Chain Attack:

There are various modes of supply chain attacks/ poisoning, some of the methods are discussed.

2.1.1 Government Policies and Regulation:

The U.S. is allegedly the main player involved in surveillance followed by China. The U.S. cites the reason behind surveillance and intelligence gathering, as to identify the terrorists and keep an eye on their activities. Simultaneously, they could look into the activities of others breaching their privacy. The U.S. has gone for a program called "Prism"(Fig. 1) after the twin tower attack in 2001 by roping in almost all companies involved in providing various services through Internet, to share data of all the people using these services. In order to establish defenses against cyber-attacks, the government's plan to maintain built-in access (backdoors) to data held by U.S. technology companies, these backdoors will not be harmful to privacy, would not fatally compromise encryption and would not ruin international markets for U.S. technology products as per director of NSA. Like U.S. the proposed new regulations from the Chinese government would require technology firms to create backdoors and provide source code to the Chinese government before technology sales within China would be authorised. Beijing's far-reaching counter-terrorism law would require technology firms to hand over encryption keys as well as installing "backdoors" into systems, thus granting Chinese authorities access in the process. These policies of both U.S. and China clearly indicate that the IT devices being produced in their countries are not trustworthy and the users of these devices will remain under constant surveillance by these states. The US has been accused of putting backdoors in Cisco routers, Windows 95, Windows XP, Android OS, Juniper devices apart from tempering with the firmware of CD ROM drives. The fact is that the NSA has routinely been intercepting US-based networking hardware bound for countries abroad. It would be safe to assume that companies like Cisco, Juniper, Brocade, Dell, HP and many more are part of NSA surveillance program. The US on other hand accuses China for bugging their networking equipment coming from Huawei, a Chinese firm. China has been accused of and on, for installing backdoors in the Smartphone produced in their countries. The researchers at Kaspersky lab discovered that a group of operators code named "Equation Group"[1] possibly connected to the U.S. National Security Agency (NSA) has infected computers including India with malware.

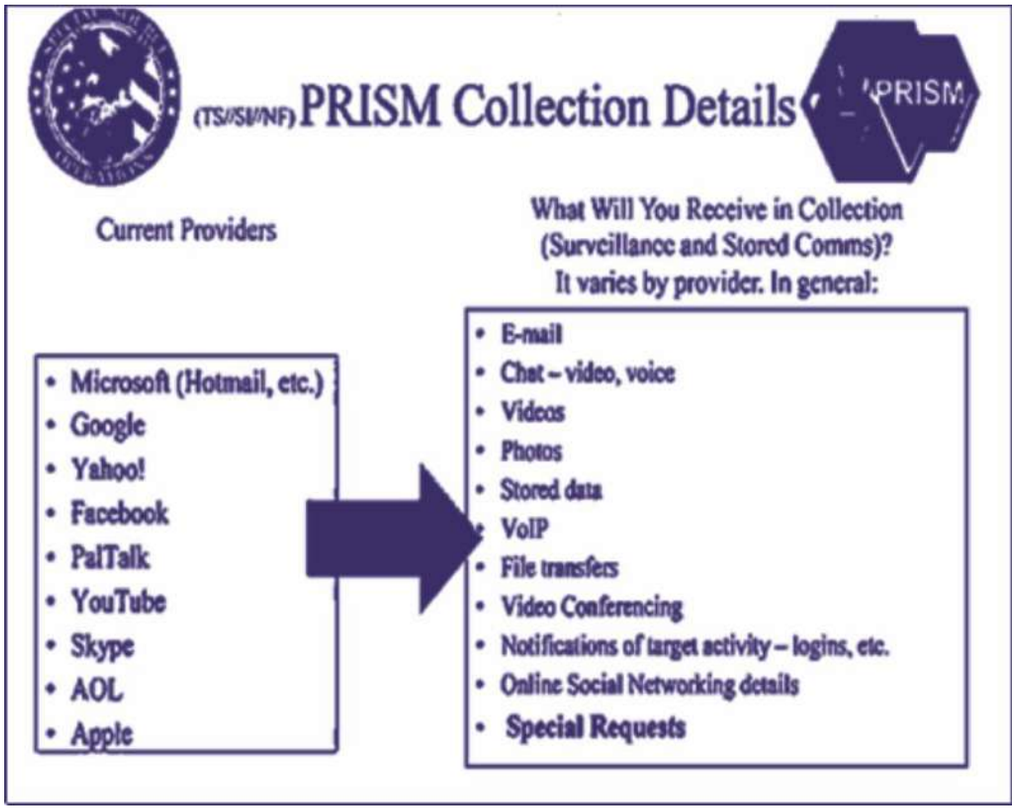

Fig.1. NSA PRISM Spy Program Given Direct Access To Servers At Apple, Google, Microsoft And 6 Others [3]

2.1.2 Global Supply Chainsin IT.

As connectivity and bandwidth has increased, the supply chains have become global, meaning the items are sourced from places which are economical and efficient, transported to multiple sub-assemblies assembly point then further to the main equipment assembly locations. IT supply chain integrity has been identified as a top three security-related concerns. Supply chain integrity is the process of managing an organisation's internal capabilities, as well as its partners and suppliers, to ensure all elements of an integrated solution are of high assurance. The need for integrity in the IT supply chain is necessary, whether the solution is developed in-house or purchased from a third party. These issues are not of concern only to defence and intelligence agencies but have implications for businesses, governments and individuals moving forward in a world where the integrity of the IT supply chain is no longer guaranteed completely, compromise can be carried out at any layer of IT stack. Hardware vendors are increasingly outsourcing manufacturing as well as design to OEM suppliers and contractors who could be located anywhere in the world. Today most of hardware systems are a conglomeration of components and subsystems provided by individual suppliers as shown in Fig 2.

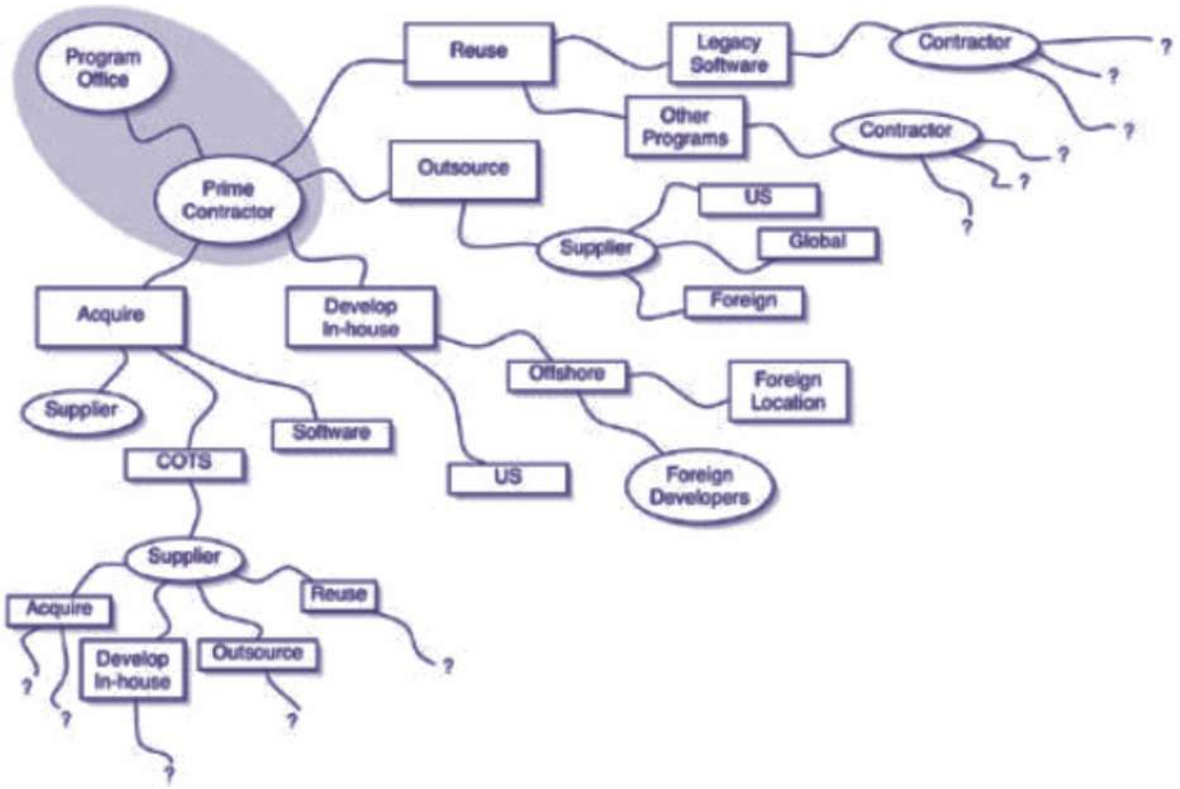

Fig.2. Supply Chain Complexities[4]

As a result, many organisations face significant risk due to the high probability that the global IT infrastructure, including their own systems, relies on tampered or tainted ICT components that could either stop working unexpectedly or compromise the data that is delivered, processed, and stored by the IT infrastructure. If there is a complete reliance on global supply chain system for the national networks and critical sectors there are very high chances of risk exposure on above mentioned threats. These risks include threats posed by actors such as foreign intelligence services or counterfeiters who may exploit vulnerabilities supply chain and thus compromise the confidentiality, integrity, or availability of an end system and the information it contains. With information and security arrangements shared across a supply chain, the cyber-security of any one organisation within the chain is potentially only as strong as that of the weakest member of the supply chain. A determined aggressor, notably advanced persistent threats (APTs), [5] will make use of this by identifying the organisation with the weakest cyber-security within the supply chain, and using these vulnerabilities present in their systems to gain access to other members of the supply chain.

2.1.3. Software Supply Chain: As per Symantec year report of 2017 released in March 2018, There was at least one large software update supply chain attack reported every month in 2017.**[6]**The actual number may even be higher considering some smaller cases may not have been publicly reported. An extension of the recent living-off-the-land trend, this type of attack occurs when sophisticated attackers manipulate software supply chains to infiltrate even the well-guarded networks. A software update supply chain attack in IT security can be defined as follows: “Implanting a piece of malware into an otherwise legitimate software package at its usual distribution

location; this can occur during production at the software vendor, at a third party storage location, or through redirection." The typical attack scenario involves the attacker replacing a legitimate software update with a malicious version in order to distribute it quickly and surreptitiously to intended targets. Any user applying the software update will automatically have their computer infected and will give the attacker a foothold on their network. It is not only desktop computers, the same applies to IoT devices and industrial controller components. The various attack methods are shown at Fig. 3.

Fig 3 Software update supply Chain attack Methods[6]

2.1.4 Recent examples of software supply chain attacks.

A recent example[5]of this is the installation of adware known "Superfish" in Lenovo notebooks. Superfish software tends to install a self-signed root HTTPS certificate that can intercept encrypted traffic for every website a user visits. When a user visits an HTTPS site, the site certificate is signed and controlled by Superfish and falsely represents itself as the official website certificate. Even worse, the private encryption key accompanying the Superfish-signed Transport Layer Security certificate appears to be the same for every Lenovo machine. Attackers may be able to use the key to certify imposter HTTPS websites that masquerade as Bank of America or any other secure destination on the Internet.

A cyber espionage group named Dragonfly was able to attack the pharmaceutical sector by setting up trojans in legitimate software. Because of this plantation of trojans in the supply chain, the Dragonfly group was able to control the now malicious software by replacing legitimate files with malicious files in the software. This malicious software in result, when downloaded from the supplier's website, provided remote access functionalities that could be used to take complete control over the system where the software was installed, or it could have been used to make the remote system act like a bot.

Another example of cyber-attack risks in the supply chain is that of shylock banking trojans. Attackers use the website builders to compromise legitimate web sites by redirecting their requests to a malicious domain. As soon the request lands onto the malicious domain, malware gets downloaded onto the system and thus attacks like man in the browser was performed. This attack is so severe that it even avoids detection and protects itself from analysis.

Another great deal of cyber risks involved in a supply chain is involvement of third parties, which are often used to store confidential data. Similarly, an attack was observed on large data aggregators where a small botnet was transferring data from the internal systems to a botnet controller on the Internet through the encrypted channel. This attack has resulted in theft of a data aggregator that licenses information to use in credit decisions.

Depending on the software package chosen, supply chain attacks may allow for semi-targeted infections. For example, attackers may target a specific sector by leveraging software that is primarily used in that sector. Trojanized software updates may also allow attackers to penetrate air-gapped networks, as sys-admins will often copy the software update to the separated network or install it from a USB stick.[6]The Petya incident in June 2017 was an example of how the supply chain can be abused to rapidly deploy malware to a targeted region. In the Petya (Ransom Petya) case, Ukrainian accounting software was misused to distribute the payload. It's therefore not surprising that more than 96 percent of the companies that downloaded the malicious update were located in Ukraine

Given the increase in supply chain attacks in 2017 and the success of a number of campaigns, it's likely that attackers will continue to leverage this attack method. Already in 2018 we have seen some attacks where this method was used: one targeted forum software, and another aimed at Mac users. While supply chain attacks are difficult to protect against, there are some steps that can be taken including testing new updates, even seemingly legitimate ones, in small test environments or sandboxes first, in order to detect any suspicious behavior.

2.1.5. Embedded systems as part of every system.

As more and more weapon systems are being interconnected and coming with state of art avionics systems, they are consisting of computer on a chip with connectivity. Internet of Things are there to stay in the defence equipment. Be it an aircraft or a radar or a drone, the network, computers and connectivity is a given thing due to the embedded and real time systems which make the OODA loop much shorter in the operations arena. Today most of the systems including vehicles have GPS, data connectivity for ease of management and better utilization in the battlefield. But along with it they are now new attack surface. Still there is monopoly of suppliers in most of the embedded systems thus the scope for manipulating the supply chain remains a viable option for the adversary.

2.2. Countering Cyber Threats In Supply Chain

Governments and industries have rolled out different compliance requirements, testing frameworks and adopted new methods to counter cyber threats. Some of the initiatives are discussed.

2.2.1. Initiatives by US DOD

In June 2018, the U.S. Department of Defense(DoD) introduced a new security initiative called "Deliver Uncompromised."[7] The program aims to improve the DoD's ability to deliver mission-critical weapons, equipment, and communications systems, free from either unintended or malicious defect. This initiative recognizes the shortcoming of existing procurement methods and recommends addition of security as a fourth foundational pillar to the traditional golden triangle of sourcing: price, delivery, and performance. The DoD program reflects the harsh reality that smart or Internet of Things (IoT)-connected devices – like computer networks, weapons systems, and aeronautical flight controls – are prime targets for intellectual property theft, data poaching, and/or tampering. Traditionally ascribed to a breakdown in IT security, these breaches are more frequently arising from exposures throughout the electronic component supply chain, which have grown exponentially as the IoT increases the attack surface and boosts the potential payoff for cyber attackers. Today, hackers need only breach one vulnerable third party to gain access to hundreds or thousands of connected organizations. These policies of US DoD has forced the giants like Lockheed Martin[8] to go in for partnerships. Lockheed Martin has contracted Guardtime Federal as a key supplier to integrate a variety of cyber-related elements into systems engineering processes, supply chain risk management and software development efforts. Since 2015, Lockheed Martin and Guardtime Federal have conducted demonstrations of data integrity technologies to address the threat of manipulation in networked and weapon system embedded cyber physical systems. With this effort, Lockheed Martin becomes the first U.S. defense contractor to incorporate block chain technology into its developmental processes, enabling more efficient and assured offerings to the federal government. Using Guardtime Federal's Black Lantern appliances and the nationally distributed Guardtime Federal Core blockchain infrastructure, Lockheed Martin plans to realize more efficient and secure software development and supply chain risk management.

2.2.2. Adopting Block Chain technology:

Blockchain provides: A verified, immutable record of actions across distributed systems with robust security capabilities. If desired, the actual contents of a blockchain can be encrypted – providing secrecy as well as integrity. These capabilities can be used in many ways. They can range from robust methods to gather sensor data to building more secure command and control systems that work even in the presence of system failure, degraded communications, and compromised or hostile nodes inside your perimeter. In many cases, the "control" part of an embedded system is a series of commands to directly attached actuators. Some of these systems, such as flight controls, may be performance-sensitive – actually, latency-sensitive. Consider the case of an autonomous drone. Critical commands issued to the drone would include a destination and whether or not to release a payload when it reaches the destination. One major concern about command and control systems is the ability to function in the presence of disrupted and degraded communications systems. A key strength of blockchain is that it is extremely tolerant of retransmission: A user can send (and receive) a block a thousand times and end up with a single command or transaction, not a thousand of them. There can be multiple partial transmissions of a block that then get reconstructed into a single verifiable block; blocks can come in out of order, as the blockchain enables the blocks to get assembled in the proper order no matter what order you receive them in. Fake shipping manifests , altered invoices, tampered tracking data, and new age supply chain security issues like cargo theft by fictitious pickups (where goods are stolen by tech savvy thieves using falsified digital shipping records that let them make a legitimate pickup) – these are some growing concerns for digitized supply chains right now. Blockchain applications in supply chain data management could change all that. The accuracy and security of information logs in a modern supply chain is essential, especially when it comes to identifying who is liable. The complications (and sometimes lack) of effective information sharing and trust in supply chains is what's fueling interest in supply chain blockchain technology and its potential to improve data sharing and visibility in the logistics and supply chain industry.

2.2.3. Compliance Requirements for Cyber Security in Supply Chain

Various compliance regulations such as PCI DSS clearly articulate in their requirements[5] about how to manage risks in the supply chain, whether that includes an internal process or involvement of third party service providers, merchants etc. For example, PCI DSS 3.0 includes requirements like penetration testing, application development lifecycle security, and threat modeling – all facts to the point that supply chain risks are an escalating concern.

Huawei has also developed[11]an ISO 28000 standard supplier management system. This supplier management system is helpful in identifying and controlling the security risks during

the end-to-end process from the point of incoming of the materials to delivery of the product. Huawei monitors and regularly checks the quality and efficiency of the qualified contractors and suppliers, and also checks the integrity of the materials provided by third party, production and delivery process. Huawei evaluates the performance of each point of SCM and establishes a traceable system throughout the supply chain of the products and services.

NIST Framework is a tool that analyzes the possible risks and prepares an appropriate path towards a risk free environment for any organization. In general, it lays out a method of risk analysis framed by standards and best practices, so any organization can use it. Using the present standards and best practices of the organization, it analyzes the risks. It also provides guidance to organization and to help it to determine and implement the best path forward by mapping the risk elements to whatever standards are applicable to the requirement for that sector or industry.

Open Trusted Technology Provider Standard (O-TTPS):- O-TTPS has been recognized by ISO (International Standards Organization) and International Electro technical Commission (IEC) as ISO/IEC 20243:2015 recently. This tool address the risks related to supply chain security, third-party providers, vendors and product integrity for any organization. O-TTPS provides a set of predictive requirements and appropriate recommendations to follow the best practices throughout the product lifecycle. Over and above these compliances various countries have come out in different mitigation methodology which has multiple compliance requirements.

2.2.4. Effective vendor management[12]:

Create Contractual Obligations by making the vendors responsible for notification within a timeline and parameters[13]. The firm has to ensure establishing data handling requirements, require product integrity, ensure language mandates communication back to the supplier are only for updates (not data collection). Thus making the suppliers demand the same of their suppliers. Evaluation of technology and capabilities through security Assessments and Source code and binary validation (quality, vulnerability, and FOSS). Information Sharing by of the threat information that can protect both.

2.2.5. Black Box Testing to Check for any Unusual Processes and Connections [1]:

Any new product has to be evaluated for any connections which it may make through Ethernet or wireless networks by the use of sniffers and other packages. Any observations should be investigated in detail.

2.2.6. Physical Inspection of Hardware by a Team of Specialists[1]:

Physical inspection of the Hardware should be carried out in detail to check for presence of any implants etc. which may be inserted with malicious intentions.

2.3 Literature Survey Summary:

There are multiple vectors of supply chain attacks in cyber domain, various countries and organisations are adopting different strategies to mitigate supply chain attacks. However none of the literature gives an assurance that following a set of steps or by adopting some mitigation strategies, supply chain poisoning can be avoided or mitigated. Almost all the literature which brings out the supply chain attacks are as a post attack study or a part of investigation of the attack which was executed. This gap is what is being attempted to be filled by designing and proposing a framework for mitigation for Indian defence.

3. METHODOLOGY

3.1 Research design.

The study and analysis was carried out based on the extensive literature survey and extensive interaction with personnel engaged in the field for procurement, testing, installation and usage of various defence equipment which have electronic components, embedded chips and computing hardware. The personnel chosen were of different seniorities and from different field of responsibilities.

3.1.1 Sample Data Collection.

All the literature survey were compilation of attacks, mitigation and policies, thus there was no readymade questionnaire available for the research. The subject is still in the nascent stage of research, therefore following set of questions were framed and used for interviewing the sample audience mentioned at para 3.1 :

(a) Awareness of the personnel regarding supply chain poisoning.

(b) Whether there has been formal awareness to personnel about the vectors of supply chain attacks?

(c) How to detect supply chain attacks?

(d) How to mitigate supply chain attacks?

(e) What are the infrastructure and expertise to test new equipment's for anomalies?

(f) Have they come across supply chain attacks if yes what did they do to mitigate?

(g) Do they have strong clauses on supply chain poisoning in procurement and tender documents?

(h) Have they undergone any workshops or training regarding cyber risks in supply chain?

(i) What are the existing government guidelines on the subject?

3.2 Findings.

The summary of the interactions using the questionnaire given at para 3.1.1 were the following :

(a) The awareness on supply chain poisoning is lacking overall.

(b) The personnel who have some awareness on the supply chain poisoning were not sure how to counter the threats.

(c) Only a certificate from the supplier is obtained saying that the products are not having any cyber threats.

(d) There is no agency equipped with tools and expertise to carry out third party evaluation for supply chain threats.

Subsequent to the analysis it was observed that there is no single solution which exist for counter supply chain threats in cyber-attacks. Moreover the case studies covered at para 2.1.4 was all studies post cyber-attack and none of them pointed out that supply chain poisoning was averted by adopting a particular set of guidelines or tests. The study also brought out the supply chain poisoning is continuously evolving since the technology is also evolving in a faster pace.

3.2.1 Indian Scenario.

India has an adverse scenario in this field since almost 100% of the electronics and computer equipment and its spare parts are imported. The defence industry is also not robust due to which the latest technology products be it avionics or radar or communication systems are all imported. These equipment has computers, programs and embedded chips which are vulnerable to future attacks, which are already compromised, which are delivered at a lower efficiency. India does not have any testing agencies to carry out the detailed testing for supply chain poisoning but they rely only on certificates given as part of the procurement procedure[14]. India is also signatory to EAL certification i.e. the Evaluation Assurance Level for the product[15]. Some product which has been tested by a friendly country is accepted at that assurance level. Still the Assurance level of 7 is a dream which are the requirements for defence product. The different government agencies have developing their own testing procedure/framework for each procurement and there is no standardisation of this procedure. There is an urgent need to build this gap and to work on a framework for mitigation of supply chain poisoning.

3.3 Proposed Framework for Supply Chain Cyber Risk Mitigation:

Based on the study carried out the Cyber Security Risks to Supply Chain is an ongoing or continuously evolving field. There is a requirement to check and act after every plan and action. i.e. continuous change as per the market and technology trends along with risk exposure. It is proposed to adapt the Deming Wheel of PDCA for countering cyber threats. This gives a framework to continuously check for new threats, technologies, detection and countering cyber threats in the supply chain of defence equipment.

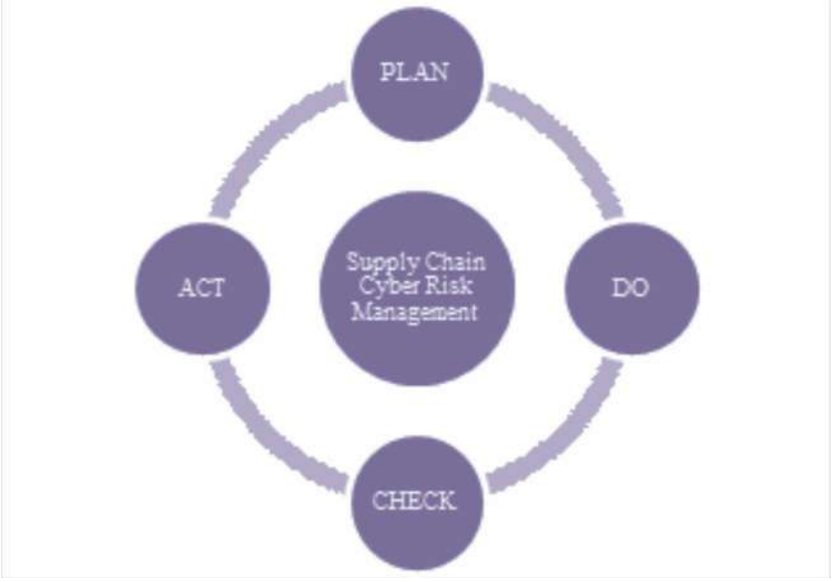

Fig.3. Proposed framework for mitigation of cyber security risks in supply chain

3.3.1 Plan

Follow the compliance requirements as per the standards and as per country policy. Implement Assurance level based requirement specification. Indigenous development of products. Plan to implement new technologies like block chain. For every new product procured, indigenisation should be the parallel activity.

3.3.2. Do.

Engage with vendors, make them fully accountable and responsible. Have a chain of custody type of accounting for all

products. Innovative procurement policies to add cyber security as an important tool in procurement policies. Educate inside the organization. Implement compliance based inductions of systems, including isolations from internet and reduce the threat exposure. Before import evaluate the indigenous product on offer and approach them for upgrade or modification first.

3.3.3. Check.

Auditing, testing and inspection. The organization should have robust monitoring capability to detect early breaches and leakages including malfunctioning. Keep a watch on Indian market for identifying the indigenous alternative.

3.3.4 Act.

Alter, change and modify the plan to improve the cyber security posture thereby building robust supply chain. Reducing the vulnerabilities. The supply chain poisoning is ever evolving thus there is a need for corrective and introduction of new parameters/methods for securing the loopholes.

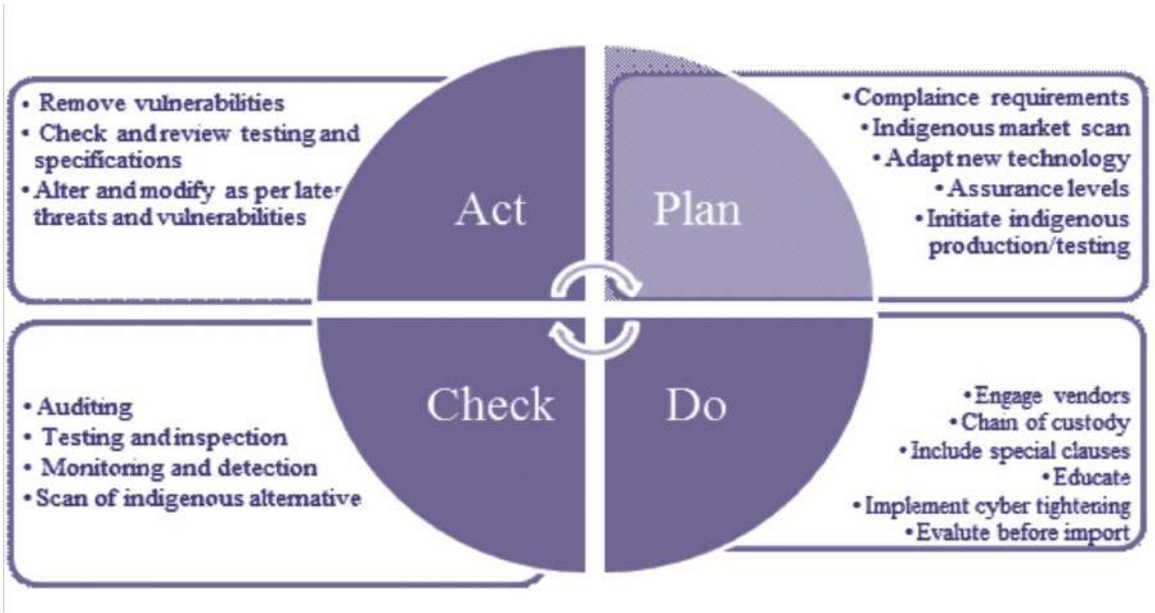

Fig 4 Proposed framework for mitigation of Supply Chain Poisoning

4. RESULTS AND DISCUSSIONS

Supply Chain cyber threats is a reality and earlier the nation / organizations recognize the importance of countering threats, the defence equipment will become trust worthy and reliable. There is a requirement to develop the indigenous industry in the latest technology to develop supply chain poisoning proof products for the Indian industry. Till that time it is recommended that the Indian industry adapt a robust framework like the one suggested in this paper**.** The main theme of the framework is that there is no one stop solution for supply chain poisoning and there is a requirement of evolving framework which is self-learning so that the cyber risks in defence equipment are countered.

5. CONCLUSION

Cyber security risks in supply chain has been evolving and risks exists in every step of the supply chain. Adapting new technologies like blockchain, collaborating with experts, educating and engaging with vendors and implementing standards and guidelines issued by various organization and the countries will go a long way in mitigating supply chain poisoning. Countering supply chain poisoning is an ongoing process and one has to be vigilant to monitor the technology leaps and be updated on the latest breaches. Implementing strong mitigation process like the one proposed will go a long way in countering supply chain poisoning.

REFERENCES

1. *M. G. G. Lamba, D. Vatsa and V. Sood, "An Approach To Handle Supply Chain Poisoning," VSRD International Journal of Technical & Non-Technical Research, Vol. VIII Issue III, pp. 96-103, March 2017.*
2. *N. P. a. S. Papastergiou, "Current efforts in ports and supply chains risk assessment," in 10th International Conference for Internet Technology and Secured Transactions (ICITST),, London, 2015.*
3. *B. Hein, "NSA PRISM Spy Program Given Direct Access To Servers At Apple, Google, Microsoft And 6 Others,"6 june 2013. [Online]. Available: https://www.cultofmac.com/230345/nsa-prism-spy-program-allegedly-given-direct-access-to-servers-at-apple-google-microsoft-and-6-others/.*
4. *"Software Development Security: Risk Management Perspective," GAO, 2005.*
5. *S. Ninja, "Cyber Security Risks in Supply Chain Management part 1,"[Online]. Available: https://resources.infosecinstitute.com/cyber-security-risks-in-supply-chain-management-part-2/#article.*
6. *Symantec, "Internet Security Threat Report Vol 23," Symantec, 2018.*
7. *P. Gallagher, "No room for compromise in supply chain*

security: New DoD initiative establishes benchmark for strategic ICT sourcing,"3 September 2018. [Online]. Available: http://mil-embedded.com/articles/no-benchmark-strategic-ict-sourcing/.

8. *Lockheed Martin Contracts Guardtime Federal for Innovative Cyber Technology,"27 April 2017. [Online]. Available: https://news.lockheedmartin.com/2017-04-27-Lockheed-Martin-Contracts-Guardtime-Federal-for-Innovative-Cyber-Technology.*
9. *R. H. Russell Doty, "Blockchain for embedded systems," [Online]. Available: http://mil-embedded.com/guest-blogs/blockchain-for-embedded-systems/.*
10. *P. Sainathan, "Blockchain - A Solution for Supply Chain Cyber Security?," 23 July 2018. [Online]. Available: https://blog.roambee.com/supply-chain-technology/blockchain-a-solution-for-supply-chain-cyber-security.*
11. *O. Pal, B. Alam and V. Srivastava, "Cyber Security Risks and Challenges in Supply Chain,"International Journal of Advanced Research in Computer Science, vol. 8, no. 5, pp. 662-666, 2017.*
12. *K. Patrick, " Practical ways to alleviate cyber risk," 07 August 2017. [Online]. Available: https://www.supplychaindive.com/news/cyber-risk-security-threat-Maersk-blockchain/448583/.*
13. *J. C. Douglas, "Combating Cyber Risk in the Supply Chain," Raytheon Cyber, April 2015. [Online]. Available: http://docplayer.net/13543959-Combating-cyber-risk-in-the-supply-chain.html.*
14. *Indian Govt MoD, "Defence Procurement Procedure,"in , 2016, p. 138 para 38.*
15. *"Indian Govt,"04 November 2018. [Online]. Available: http://www.commoncriteria-india.gov.in/overview.php.*
16. *F. E. M. a. R. D. Arnold, "Supply chain risk mitigation for IT electronics," in IEEE International Conference on Technologies for Homeland Security (HST), , Waltham, MA, 2010.*

AUTHORS

J Angel Reuben, BE, MS, MSc, MTech, DIAT, Pune, angelreuben@gmail.com

Dr Nilesh Ware, BE, MTech, PhD, DIAT, Pune, nilesh.ware01@gmail.com