Sri Lanka Institute of Information Technology

BSc Honors in Information Technology Specializing in Cyber Security

Weapons Systems and Cyber Security

- Improvement and Challenges –

Individual Assignment

IE2022 - Introduction to Cyber Security

Submitted by:

Student Registration Number	Student Name
IT21170270	Maduranga D.B.W.N

Main Topics

1. Abstraction

Military forces across the world employ a variety of weapon systems. Today, high-quality legacy systems that have been in operation for decades and are still in use coexist with contemporary weaponry. Hundreds of thousands of chips can be found inside a contemporary weapon system. These chips have intricate designs and may have billions of transistors, which results in a very complicated system of systems. Due to financial limitations or delays in obtaining new weapons, conventional weapons systems frequently have longer lifespans or superior performance. As a result, legacy state systems must cooperate not just from a communication standpoint, but also from a standpoint of overall system integration.

All these systems must be correctly integrated and able to cooperate for modern network-centric war scenarios to function. It contains a staggeringly intricate variety of sensors, communications, systems, and weaponry from several eras, opening a plethora of attack vectors and providing serious difficulties for the security of weapon systems. This article discusses the impact of weapons while also analyzing the individuals involved in today's warfare. a summary of how system ageing affects IT security and important cyber security factors. Essential supplies and contraindications are advised, and certain perilous circumstances are noted.

2. INTRODUCTION

Today's gun system is incredibly complicated, which makes it difficult to conduct normal security evaluations of utilities and raises the danger of harm. a cyberattack. According to other rumors, even though a gun's full functionality is frequently produced on the ground, or at the very least in close interaction with challenging circumstances, it is challenging to ensure the integrity of its additives. For instance, computer systems require integrated circuits (ICs).

Additionally, the link structure for the gun structure is typically bought from a variety of vendors, usually the highest bidder. The most essential items, such as monitoring the manufacture of parts or subsystem assemblies, are very difficult to acquire without paying large additional expenditures. As a result, the supply chain guard is frequently the subject of worrying queries.

It essentially entails moving manufacturing operations from high-cost international locales in the West to low-cost cities in Asia. The lack of academic employment initially caused anxiety, but it didn't take long for concerns about the security of buildings that had been carefully certified and had chips made by other manufacturers to surface. The US Department of Defense (DoD) started looking to solutions to strengthen the security of vulnerable defense structures in the early 2000s because of this. After Israeli aircraft destroyed a Syrian nuclear plant during Operation Orchard in 2007, it continued to expand. Some of the chips used for a utility breach are said to feature a flip port, and a back door to allow unwanted entry, as modern radar technology has improved its ability to identify jets. Concerns over potential death switches inside chips in nations' own military systems were substantially increased by the incident of 2007. [1]

The Department of Defense and the National Security Agency provided funding for Reliable Startup Program to "ensure service availability and mass production of devices with feature sizes as small as 32nm on a 300mm thin sheet. Reliable. Supplies through the program the chain was developed." Contains 52 potential trusted suppliers. The TFP provided programs with "National Security and Access to Semiconductors" and was completed in 2013.Electronic components from trusted sources the program can produce chips for a variety of sensitive systems, however, due to the complexity of contemporary military systems, interfering chips from untrusted sources are not permitted. But according to a 2011 research, 40% of military systems were impacted by fake electronics. [2] According to a report to congressional committees highlighted by the US Government Accountability Office (GAO) in February 2016 despite improvements since 2011, DoD efforts to combat supply chain risks and counterfeit parts remain challenging. [3]

The threat posed by the resurgence of proteases is widening and presents many risks. Because counterfeit components are often below legitimate manufacturing quality standards, there is a greater chance of a weapon system malfunctioning. Counterfeit coins further increase the chance of exposing backdoors and working circuits. A lot of studies have been done to develop and improve detection techniques that can create very ubiquitous attacks even below the transistor level. Malicious circuits may have new and even more destructive functions. One disturbing example is the recent evidence of hardware Trojan instantiation below the gate level of the Intel Ivy. Chip as reported by Becker et al. [4] Around 1300 doors are required for various manipulation strategies such as integrating all rear door hardware at the door level. Because the scientists changed the polarity of the dose in some areas, common tests, including fine-grained optical tests, could not detect changes in the wire layers. or comparison with gold chips.

When the process is known, Becker can reduce the entropy of a random number generator (RNG) from 128 bits to 32 bits, making an attack simpler. NIST guidelines based RNG testing procedures are unable to identify manipulation of produced random numbers. Backdoors have been employed in a few chips, including the Boeing 787 Dreamliner and the Microsemi ProASIC 3 used in military systems. [5] [6] These redundant circuits are frequently referred to as undocumented debugging features, which is equally enlightening. It doesn't matter, though, whether an almost undetectable hardware backdoor was intentionally added for high-security and military devices.

3. WEAPONS SYSTEMS

a) *Elderly weapons systems*

The cost to design, outfit and operate a weapon system is high. So these high value systems will last 30 to 40 years. Although this is a significant period, it is often longer due to logistical or budgetary issues. Reasons: The nation has faced economic downturns and budget cuts, leading to several procurement projects being canceled. Additionally, the method for buying military hardware could be changed. In this industry, delays of several years due to late specification changes or problems in the development process are not unusual. . For example, since the establishment of "Eurofighter Jagdflugzeug GmbH" in 1986, it has been 17 years.

The first production aircraft was delivered in 2003, and by 2012, the unit cost had increased from the initial budget of 33.32 million euros to 138.5 million euros. [7] Such delays can also significantly increase the life of the weapon system. As a result of these advances, even in the contemporary West, the age of a military's weapon systems can typically be decades. For example, the B-52 bomber, which first entered service in 1955, is much older than the average age of US Air Force aircraft, which is 27 years. [8] Therefore, the majority of the United States Air Force (USAF) is expected to accomplish this through lifestyle adjustments rather than equipment.

I'm going to explore the extent of our knowledge about the vulnerabilities of military and industrial control networks, explore recent incidents in which older systems were successfully breached, and identify how these systems can be protected from future cyber-attacks. I'll also talk about what's being done to protect these devices.

Experts have been warning for a while now that one major danger posed by computerized equipment is that they're vulnerable to hackers - either as they operate in cyberspace or as they operate in physical space with physical access. I'll look at ways that we might mitigate those vulnerabilities and make them less dangerous than they are today.

When a business has been in operation for a while, finding replacement parts can be challenging. Businesses may cease operations, change their production processes, or create brand new, incompatible items. Therefore, mid-life upgrade procedures are performed one or more times to retain availability throughout the life of the weapon system. To operate the system and replace obsolete items, more and more off the shelf (COTS) products should be deployed. [9] [10]

b) Modern weaponry systems

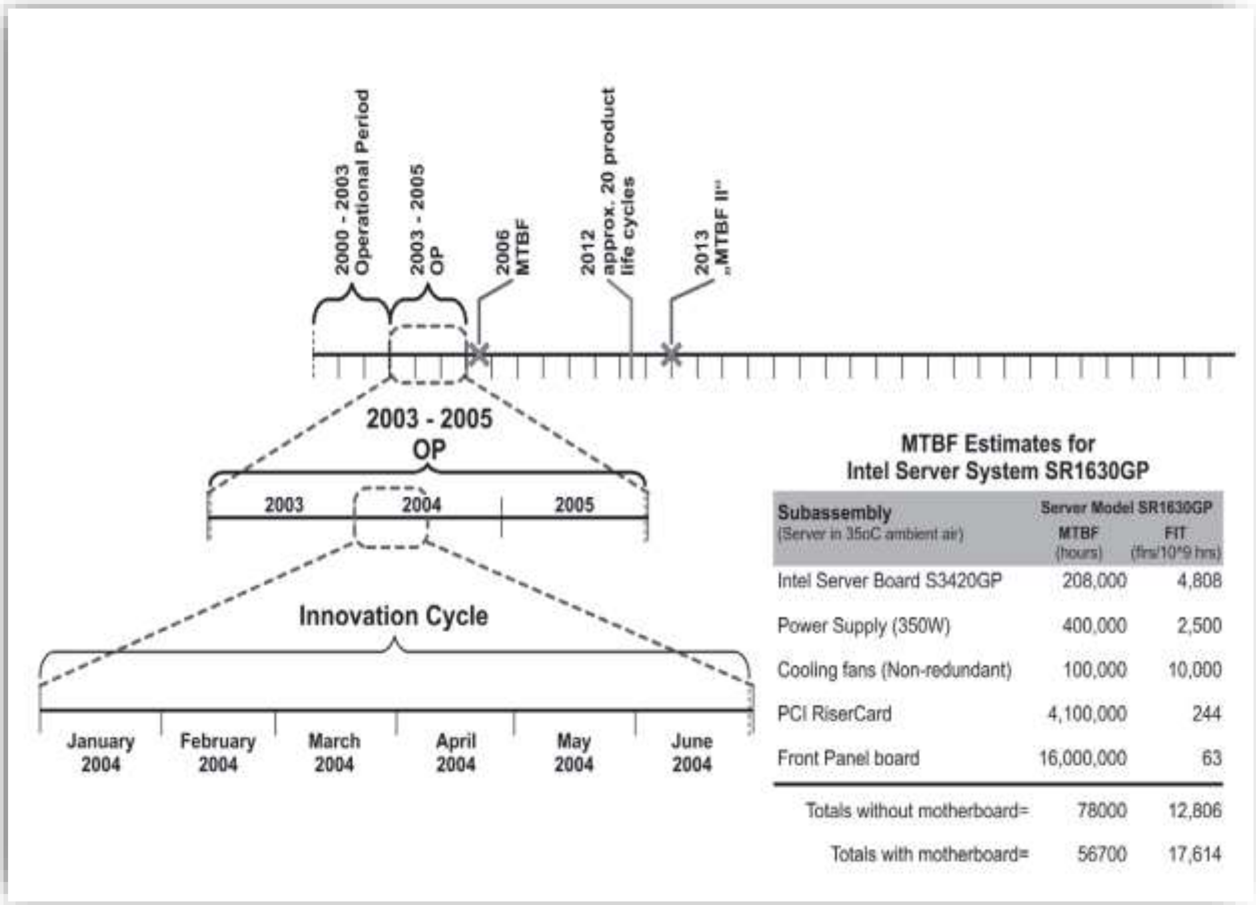
Modern weapons are very complex. They have huge networks, tens of thousands of chips and connected sensors and devices. Peace Dividends, as well as multiple economic and financial crises, have forced widespread budget cuts and reductions in overall defense spending, and the military served as a technology driver during the Cold War due to massive defense budgets for research and development. In contrast, the spectacular development of information and communication technology (ICT), the Internet and consumer electronics accelerated the growth of the industry into a multibillion-dollar sector. The commercial market is currently the driver of the technology, thanks to progressively shorter product and innovation cycles.

COTS products are commonly used in contemporary weapon systems to reduce costs and improve system performance. However, the increased use of COTS in high-value systems has created significant difficulties for maintaining weapon systems throughout their lifetime. Any Efforts to update an ICT component of a weapon system after deployment require costly recertification to obtain operational authorization. Due to the speed of technological development, new ICT and weapon systems are released every few years. ICT subsystems are often expensive as they require constant updates to keep them running for a long time.

It has been a major concern among government officials, military leaders, and corporate leaders alike. While we are not all in agreement as to who is behind these attacks or what their motives are, one thing that many people seem to agree on is that vulnerabilities do exist, and they can be exploited by a variety of actors.

These trade-offs consider the expected lifetime of IT components, their mean time between failure (MTBF) and harsh operating conditions such as a wide temperature range, material stress from strong acceleration or sea turbulence affecting ships. Components should be spent at least once every ten years. Updating a weapon system that has been in use for 30 to 60 years requires several projects. This increases the likelihood of introducing modified, synthetic, or low-quality elements and can cause compatibility issues. (See, for example, [11]).

FIGURE 1 :



MTBF Estimates for
Intel Server System SR1630GP

Subassembly (Server in 35oC ambient air)	Server Model SR1630GP	
	MTBF (hours)	FIT (fīrs/10^9 hrs)
Intel Server Board S3420GP	208,000	4,808
Power Supply (350W)	400,000	2,500
Cooling fans (Non-redundant)	100,000	10,000
PCI RiserCard	4,100,000	244
Front Panel board	16,000,000	63
Totals without motherboard=	78000	12,806
Totals with motherboard=	56700	17,614

c) Network centered military

Budget restrictions following the end of the Cold War mandated more effective use of finances. Costs related to developing, manufacturing, operating, and maintaining weapon systems are rising quickly as military budgets have been curtailed. The number of weapon systems available has maximized the use of scarce resources under these constraints. Not only that but also retain power supremacy with the largest number of units with structurally limited power but with the highest technical potential, the connectivity of all systems has responded to provide all necessary information at all levels properly. It is called Network-centered warfare (NCW).

Considering the twenty-first century battlefield, the US Navy was one of the first to consider how ICT could be used to improve the effectiveness of forces [12]. One of the main outcomes of their consideration is the improved integration of previously separate independent systems. This approach The NCW idea was eventually born out of integration. It is a practical theory.

The idea of the information age encourages network-based communication, improves situational awareness, and enhances the effectiveness and efficiency of military operations . [13]Through its network of scouts, commanders, control systems and weapons, NCW develops information excellence and consequently ensures full range military superiority and military operations.

NCW's mission is to enable rapid information access at all levels of the Armed Forces. This allows information to be shared between each component, which when combined can create a coherent and accurate image of the battlefield. Using this robust and adaptable grid power concept, units can fight in the absence of networked forces, smaller, more independent, and more effective armies avoid or reduce fraternal ties and accelerate the pace of warfare. [13] To remove the "fog and friction", the common understanding of all forces ends. The NCW concept allows the most efficient use of resources, but it also considerably increases the threat to the entire system: an attack on the weakest link in the NCW chain might have severe consequences for its owner, and in the worst situation, make the entire military formation unusable.

Even with hardened links, communication links will be the target of attacks since maintaining the network's secrecy, integrity, and availability is essential for employing NCW. Strong CND skills are enforced for every NCW-dependent actor by a strong CNA capability, which can treat even a weak enemy with love. As a result, thorough safety measures must be adopted, and there needs to be a quick ("real-time") response capability in the event of an attack or the discovery of network and system anomalies. These include equipment, as well as organizational and financial issues, education, and training

4. THREAT ANALIYSIS

The most important vulnerabilities are in issue because of the range of weapon systems used in modern warfare and the numerous attack pathways connected to them. Breaking the weakest link can have a significant influence on a mission overall in modern warfare because all systems are heavily integrated and vulnerable to NCW conditions. It is suggested that risk assessment be data-driven to facilitate security testing for cyber-physical systems. Schemes for defense and avoidance are created in response to perceived threats and related exploit vectors. Data streams are produced by cyber-physical systems by their very nature. Different procedures must be followed to determine vulnerability, both at the governance and cyber levels.

Data breach is the theft or unauthorized modification of data. If a hacker comes into your system and finds out your passcode, they will gain access to all the data contained in that system. Threat analysis is the identification and evaluation of potential hazards such as risks, vulnerabilities, threats, and risk mitigation strategies. Without threat analysis detection tools are unable to provide a complete picture which leads to potentially missing early warning signs of abnormal activity or malicious intent. Cyber security is an ever-changing field with new technology being developed daily and it can be difficult for companies without proper threat management capability (i.e., systems that are able to detect threats before they happen).

A.OLD VS NEW

One can draw the conclusion that older weapon systems are intrinsically less secure than more modern ones since they combine both antiquated and cutting-edge weapons. The lengthy design and procurement processes for new systems can result in their own issues with out-of-date software, as older systems frequently employ older software and can have problems with software updates and patches. Mid-life update projects improve older weapons systems, occasionally replacing all their ICT components. Therefore new, and old IT components can be found in both legacy and cutting-edge systems, and both must be treated equally when it comes to cyber hazards.

B. Base industrial and technological capabilities for defense

Another crucial element is the DTIB's (Defense Technology and Industrial Facilities) capabilities. To design, produce, and maintain the weapons and equipment required to meet national security goals, the DTIB consists of a few people, organizations, and technical experts. [14] A plan for the European DTIB has been developed by the European Defense Agency with the objectives of increasing its capacity, attracting greater investment, and promoting wider public use of the EU Public Procurement Regulation . [15]Although there are numerous skilled military firms in Europe, most components like electronic semiconductors are often produced in the Asia-Pacific region rather than in Europe. [16] Weapons systems are also not explicitly addressed in the European Union's DTIB plan, which greatly restricts the effectiveness of the European DTIB as well as that of other Western nations. Currently, there are few opportunities for basic computer component maintenance.

Another issue is that not all DIB agencies have access to the Cyber Threat Information Sharing Voluntary Program because it requires a DoD Common Access Card (CAC) and is not available to all DIB employees or enterprises. Some DIB campaigns may be missing Establishes informal contacts with members of the intelligence community who have access to critical information about cyber threats. To further enhance DIB's cyber security, advanced CSTs have been developed by cyber security companies, however these new tools are expensive. Many of these tools are covered in this article, along with how DIB companies can use them and how they fit into DCP2.

C. Supply chain

After losing most of it, North American manufacturers are gradually gaining market dominance. Electronics manufacturing in Europe continued to decline in the 1990s and into the first decade of this century, and China was also challenged by emerging manufacturers in other Asian countries. Asia-Pacific countries such as Malaysia and India . [17]As a result, the security of military systems is seriously threatened by the IT supply chain. Due to the complexity and widely dispersed chip design ecosystem, the construction process involves many businesses and individuals from specification to shipment [18].

Today, the specification, design, manufacturing, and testing phases of creating a trained chip involve a significant number of people, driven by streamlining of business procedures, cutting production costs, outsourcing, and globalization. Many companies are divided into different stages. Even the chip's component bits can now be bought or resold. Corporations and significant chip design participants are encouraged to increase the risk of fraudulent designs [18].

Despite the increasing use of cloud computing, there is a risk here. Kingdom, a US IT systems and cloud services provider, entered liquidation at the end of January 2013. (Robinson, 2013). The immediate impact resulted in loss of access to 2e2 clients. They faced financial demands from the liquidator if they needed to operate their data centers or maintain access to their hosting systems and data. Organizations are actively encouraged to replace their own locally based servers with cloud-based services to reduce IT costs. It is important to carefully consider how such measures affect cyber resilience, especially when hosted services are at risk.

The construction process can be changed to a greater or lesser extent at any time. [19] I ignore manipulation of standards, influencing the design process by inserting back doors, and other examples of this, such as disabling the debugging function. The SPARC M7 has 10 billion transistors, or 0.00013% of its ports. They are a largely invisible set of tests that successfully detect random design errors based on computational probabilities but fail to detect mismatches that a skilled designer has deliberately concealed . [18]

In addition to these options, markets dealing with counterfeit money are expanding. The market for semiconductors reached $169 billion in 2012. As it is a positive activity one can expect a higher increase. Weapons are in danger due to fake materials. Poorly maintained systems often fail to meet original requirements and increase the risk of circuit tampering. A record number of technology items were reportedly deployed by the US military and dozens of other federal organizations in 2012. [20] [21] This creates a variety of dangers for national security, such as fires, damaged missile airplane parts, cyber espionage, and more. See examples of specific supply chain risks and vulnerabilities that could result in DTIB. See [22].

D. Intentional hardware regeneration

The procurement procedure for specific weapon systems should be modified to consider the need to integrate short-term COTS hardware with high-value, long-lived weapon systems. As a result, semiconductor devices are not only constantly being replaced, but also come up with ideas for dealing with compatibility issues.

Identifying modified or modified chips is essential in system migration procedures and major problems with incompatibility with new hardware. From the time they were invented up until the last few years, all computer processors have gone through some level of degradation. This means that computers need to be replaced at least once every few years, and you'll want to replace your old processor with one that is as powerful as possible.

At present, it is estimated that about 70-75% of all systems in modern companies run a version of Microsoft Windows. This has been attributed to the consistent ease of use and widespread availability. It is not difficult for any development engineer to find and install a readymade OS with all the necessary software preinstalled. However, it can become quite hard to find and install new software without unwanted consequences for the company's security posture or general system stability. Furthermore, there might be features that are available in newer operating systems which can benefit your business even if you don't use them yourself. Depending on what type of computer you're using, you may also need to upgrade more than just your processor for it to keep up with the current trends and demands in computing.

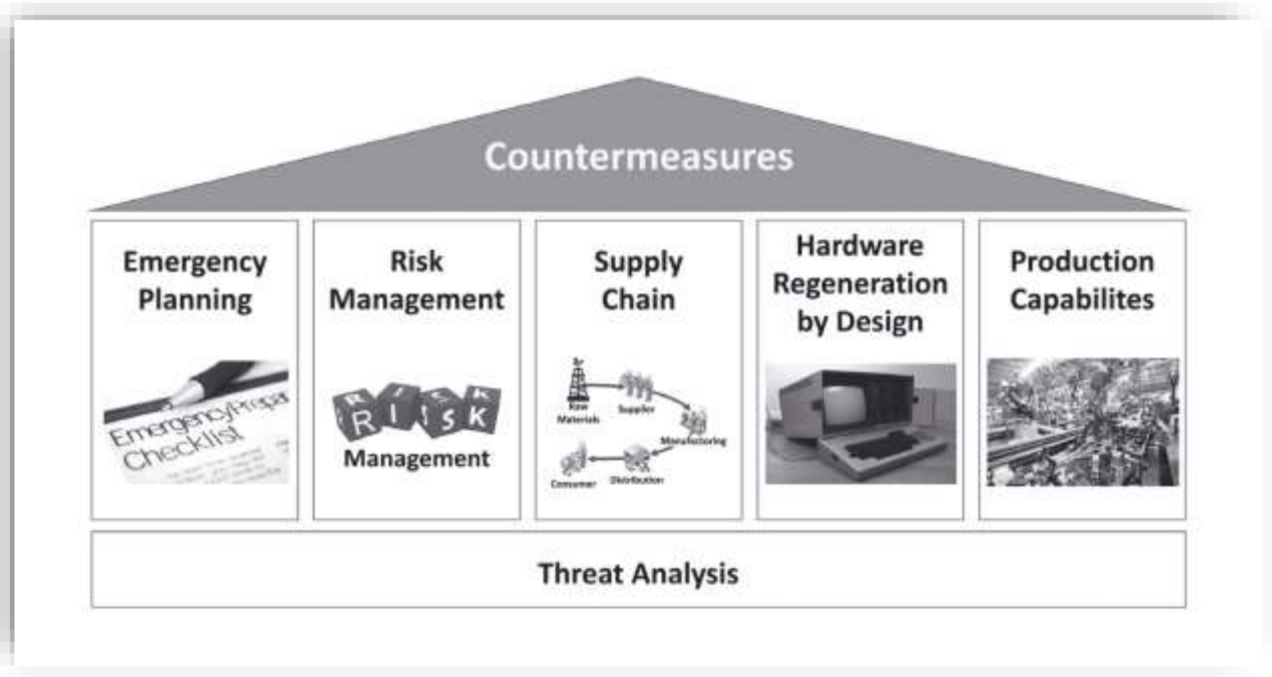
E. Capabilities for production

An analytical threat analysis report is a structured, systematic, and comprehensive description of how a potential adversary or serious incident could achieve its objectives. Threats can arise from non-state actors, or from state actors. Threats within the same country are usually perpetrated by that same state. A common way to categorize threats is to look at what assets the threat has available and what it may want to do with those assets; this categorization can help identify vulnerabilities in processes and systems that might be exploited by the threat to achieve its aims.

Additionally, test teams look for the quickest or most efficient way to access a system because they only have a certain amount of time with it. We spoke with DOD representatives and looked over inspection records. They don't pinpoint every vulnerability that a foe might use. Longer-term inspections often uncover more hypervulnerabilities than quick examinations, according to DOT&E. According to DOD officials with whom we spoke, the department has recently boosted the number of long-term assessments it does annually. Weapon system cybersecurity evaluations may also have some limitations. Assault kinds in which whole categories are represented Some cyber assessments do not yet address vulnerabilities.

European DTIB systems must be strengthened to provide all required weapon system components, including semiconductor electronics for increasingly sophisticated applications. This includes strengthening current blockchain- and cryptocurrency-related enterprises. DTIB simulates TFP by building its own production capabilities. Specialized chips for high-security systems and the new European Union plan the highlighted activities needed to improve safety are summarized in Figure 2: Reduce the worst side effects of weapons.

FIGURE 2


Countermeasures
Emergency Planning
EmergencyPrepar
Checklist
Risk Management
RISK
Management
Supply Chain
Raw Materials
Supplier
Manufacturing
Distribution
Consumer
Hardware Regeneration by Design
Production Capabilites
Threat Analysis

5. RESEARCH INQUIRY

Military supply of semiconductors in the US

To illustrate the growing problems associated with supply semiconductors in US military electronics, this section provides a case study illustrating the results that can be achieved by implementing the proposed countermeasures. The United States continues to lead the world in semiconductor research and development (R&D), and manufacturing sectors are increasingly moving to the Asia-Pacific region, a trend that is predicted to continue in the coming years. Brigadier General (retd) John Adams describes the incident as follows.

China's telecom sector has expanded rapidly, as the Chinese military funds the rapid proliferation of Chinese-made telecom equipment at below-market prices. The likelihood of switches or backdoors into critical communications infrastructure increases as the widespread use of Chinese military-funded equipment and the declining market share of prominent US telecommunications companies jeopardize the integrity of sensitive security-related communications. [22]

The U.S. Department of Defense is struggling to meet its increasing need for semiconductors, and the situation will likely worsen as the military's reliance on electronics continues to rise amid increasingly advanced technologies.

Today, over two-thirds of all modern military systems rely on electronic components. Semiconductors are used in everything from individual weapons systems, like Lockheed Martin's HELLFIRE missile, to complex command and control networks that allow US forces across the globe to communicate in near-real time with one another.

China's telecom sector has expanded rapidly, as the Chinese military funds the rapid proliferation of Chinese-made telecom equipment at below-market prices. The likelihood of switches or backdoors into critical communications infrastructure increases as the widespread use of Chinese military-funded equipment and the declining market share of prominent US telecommunications companies jeopardize the integrity of sensitive security-related communications. This assumes that substitute suppliers can be competitive in their absence. Today's market leading design tools From US based sellers only. They will also be a factor.

The ability to accelerate and strengthen China's growth the possibility of indoor casting or easy access Asian casting partners of note. In any case, our test Just one of our 32 product categories illustrates This qualifies the semiconductor market classification as: Only 5% of Chinese semiconductors are affected. demand. For eleven additional items which is 23% China's demand and the country's modest but growing suppliers Some could grow over time.

I. I shall prepare complete and effective contingency plans to provide all necessary guidance in the event of equipment failure. For example, if the communication system from manufacturer A fails (because of activating the kill switch), another device made by manufacturer B based on a more suitable architecture must access the support service. The operator shall, whenever possible, carry out all necessary activities as soon as possible using the information in the emergency plan to be included in it. [23]

II. Guidance should be provided through appropriate risk management that considers variables that may impact output or safety. For example, having a managed processor in a system that cannot use this function (such as an isolated system with no connectivity) has no limitations, and having the system online can be quite dangerous. [24]

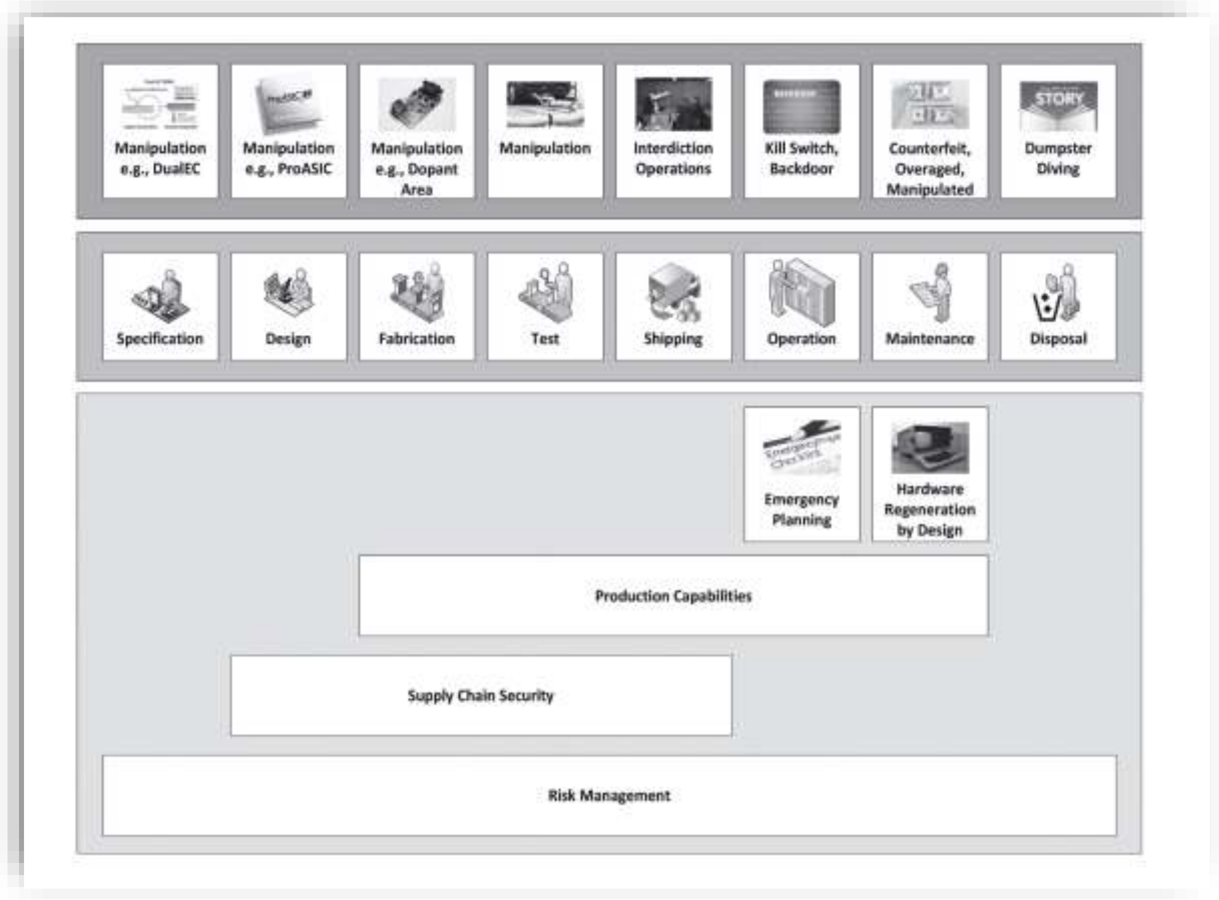
III. Replacement of unreliable components in threatened systems currently in use can also be done by increasing production capacity.

By taking all the necessary precautions, the risk of introducing a manipulated circuit can be reduced. This is done by increasing security and ensuring that the most critical and constrained systems can be manufactured. Reducing potential manipulation through the supply chain (see for example [25]).

Especially for new procurement initiatives, the need for periodic hardware upgrades should be incorporated into the design. For example, the specification and selection of components should be done using widespread, reliable, and open standards (such as IPv4/6), allowing components to be replaced with a minimum number of modifications. Even if the first supplier runs out of stock or discontinues the product line, at least. If genuine components can only be obtained from questionable sources, new comparable parts should also be used as there is a greater risk of counterfeit parts.

FIGURE 3 : EFFICIENT RISK MANAGEMENT

Provides a summary of the supply chain implications that can be expected when using all the contrasts.



6. CONCLUTION

Today's battlefield is a complex environment in which many highly complex weapon systems interact with each other, a mixture of generations and a variety of electronic equipment over the ages. Difference. As a result, there are unique cybersecurity needs, but as cases like Operation Orchard demonstrate, these sensitive systems are more vulnerable to intrusions. Due to the shift of manufacturing to low-cost countries and the globalization of chip production, current military systems are vulnerable to several attacks and maneuvers. Safe manufacturing capabilities in microelectronics can be developed. Look at the procurement process; It is very important to incorporate hardware regeneration concepts regularly.

As a result, risk and emergency management is crucial throughout the entire firm. Every unit Additionally, all levels of management must be capable of acting quickly in the event of an assault. During the hardware layer. specifically enhancing European DTIB capacities new ideas and methods for sensing systems are necessary for the semiconductor industry. There should be development of better supply chain security for electronic devices on international marketplaces. The US exhibits TFP, despite the high expense. It is possible to create safe microelectronics production facilities. By observing It's critical to streamline procurement procedures and hardware regeneration ideas.

REFERENCES

[1] S.Adee, "The hunt for the kill switch," *Spectrem , IEEE,* vol. 45, pp. 34-39, 2008.

[2] C. Ortiz, "Dod trusted foundry program," [Online]. Available: http://www.ndia.org/Divisions/Divisions/SystemsEngineering/Documents/..

[3] M. A. Mak, "'Counterfeit parts - DOD needs to improve reporting and oversight to reduce supply chain risk,' United States Government Accountability Office, Tech.," [Online]. Available: http://www.gao.gov/assets/680/675227.pdf..

[4] F. R. C. P. a. W. P. B. G. T. Becker, "'Stealthy dopant-level hardware Trojans,'," *Cryptographic Hardware and Embedded Systems-CHES 2013.,* p. 197–214, 2013.

[5] S. S. a. C. Woods, "Breakthrough silicon scanning discovers back door in military chip," 2012.

[6] C. Arthur., "Cyber-attack concerns raised over Boeing 787 chip's 'back door'.," [Online]. Available: http://www.theguardian.com/technology/2012/may/29/cyber-attack-concerns-being-chip..

[7] D. K. J. M. a. D. N. M. Freund, "Totalschaden mitAnsage.".

[8] D. L. Wood, "'2016 index of US. military strength,' The Heritage Foundation,," [Online]. Available: http://index.heritage.org/military/2016/resources/download/..

[9] S. Kosiak, "Options for Modernising US Defense Capital Stock.," *Buying Tomorrow's Military,* 2001.

[10] L. O. Association., "Aging weapons systems".

[11] D. Goldman, "Fake tech gear has infiltrated the US government.," [Online]. Available: http://security.blogs.cnn.com/2012/11/08/fake-tech-gear-has-infiltrated-the-u-s-government/..

[12] D. S. Alberts, "'Information Age Transformation: Getting to a 21st Century Military," *DTIC Document, Tech.,* 2002.

[13] C. Wilson, "background and oversight," *'Network centric operations,* 2007.

[14] W. Slocombe, "'Adjusting to a new security environment:," *The defense technology and industrial base challenge - background paper,' US Congress, Office of Technology Assessment,* 1991.

[15] EDA Steering Board, "'A strategy for the European defence technological and industrial base,'," *EuropeanDefence Agency,,* 2007.

[16] E. Publications, " Electronics .caPublications,," *'World electronic industries 2012-2017,,* 2017.

[17] E. S. Board, "'A strategy for the European defence technological and industrial base,'," *EuropeanDefence Agency,,* 2007.

[18] J. Villasenor, "'Compromised by design? securing the defense electronics supply chain,' Brookings Institution Report,," 2013.

[19] T. C. C. C. A. H. T. L. R. D. J. Bernstein, "'How to manipulate curve standards: a white paper for the black hat,' Cryptology ePrint Archive, Report," 2014.

[20] J. T. A. C. C. G. W. J. a. Y. Z. S. T. King, "'Designing and implementing malicious hardware.' LEET,," vol. 08, pp. 1-8, 2008.

[21] L. Dignan., "Counterfeit chips: A $169 billion tech supply chain headache.".

[22] J. Adams and P. Kurzer, "Supply chain vulnerabilities & national security risks across the US defense industrial base. Alliance for American Manufacturing," *Remaking American security:,* 2013.

[23]

[24] "'Directive 2004/108/ec of the European parliament and of the council of 15 December 2004 on the approximation of the laws of the member states relating to electromagnetic compatibility and repealing directive 89/336/eec,'," 2004.

[25] A. S. D. a. R. K. Ghadge, "present and future scope.' The International Journal of Logistics Management 23.3," *Supply chain risk management:,* pp. 313-339, 2012.

[26] J. Mick., "40 Percent of Defense Supply Chain Damaged by Chinese Parts," [Online]. Available: http://www.dailytech.com/US+GOA+40+Percent+of+Defense+Supply+Chain+Damaged+by+Chinese+Parts/article21937.html..