

Cyber-Nuclear C3 Stability of Pakistan: A Proposed Cyber Security Framework for Mitigating Cyber -Nuclear Threats



by

Muhammad Faisal Sultan

A thesis submitted to the faculty of Information Security Department, Military College of Signals, National University of Sciences and Technology, Rawalpindi in partial fulfillment of the requirements for the degree of MS in Information Security

July 2023

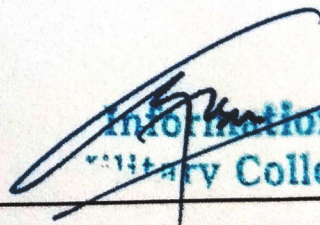
THESIS ACCEPTANCE CERTIFICATE

Certified that final copy of MS Thesis written by Mr. Muhammad Faisal Sultan, Registration No. 00000319164, of Military College of Signals has been vetted by undersigned, found complete in all respects as per NUST Statutes/Regulations/MS Policy, is free of plagiarism, errors, and mistakes and is accepted as partial fulfillment for award of MS degree. It is further certified that necessary amendments as pointed out by GEC members and local evaluators of the scholar have also been incorporated in the said thesis.

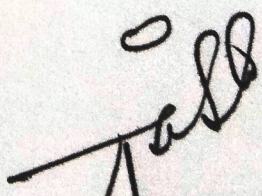
Signature: 

Name of Supervisor Dr. Imran Rashid

Date: 5/7/23

Signature (HOD): 
HoD
Information Security
Military College of Signals

Date: _____

Signature (Dean/Principal) 

Date: 18/7/23

Prof
Dean, MCS (NUST)
(Asif Masood, Pnd)

Declaration

I hereby declare that no portion of work presented in this thesis has been submitted in support of another award or qualification either at this institution or elsewhere.

Dedication

“In the name of Allah, the most Beneficent, the most Merciful”

I dedicate this thesis to my late mother, father, wife, and teachers who supported me
each step of the way.

Acknowledgments

I am extremely thankful to ALLAH Almighty for His bountiful blessings throughout this work. Indeed, this would not have been possible without His substantial guidance through every step, and for putting me across people who could drive me through this work in a superlative manner. Indeed, none be worthy of praise but the Almighty. In addition, my salutations be upon Prophet Hazrat Muhammad (PBUH) and his Holy Household for being a source of guidance for people.

I would like to express my special thanks to my supervisor Dr. Imran Rashid for his generous help throughout my thesis and for being available even for the pettiest of issues. The sense of belief that he instilled in me has helped me sail through this journey. My thanks for a meticulous evaluation of the thesis and guidance on improving it in the best way possible. I would like to make a special mention to my brother, who has always stood by me during tough times and was a great source of strength for me during this thesis. I am also thankful to my friend Mujeeb Ahmed, who encouraged me to complete my thesis, providing me with much needed motivation in times of stress.

Last, but not the least, I am highly thankful to my wife. She has always stood by my dreams and aspirations and has been a great source of encouragement for me. I would like to thank her for all the care, love, and support throughout my times of stress and excitement.

Abstract

Pakistan's nuclear program is believed to be advanced, with the country possessing an estimated arsenal of around 165 nuclear weapons. Pakistan's nuclear infrastructure includes hierarchical command & control structure along with an NC3 (Nuclear Command Control & Communication) system. Its nuclear command and control structure is believed to be centralized and tightly controlled by the National Command Authority. The country's Strategic Plans Division (SPD), the secretariat of NCA, is responsible for managing Pakistan's nuclear arsenal and has developed a comprehensive set of procedures and protocols for maintaining nuclear security. Pakistan has not declared its nuclear doctrine officially; however, it has professed to maintain a full spectrum deterrence. The asymmetry between the tactical military strength of Pakistan and other nuclear states has increased Pakistan's reliance on the nuclear variable. The cold start doctrine of India states that India will conduct surgical strikes within Pakistan while remaining under the nuclear threshold. Cyber-attacks on Pakistani NC3 infrastructure can be a part of the cold start doctrine. A typical NC3 infrastructure is highly networked as it binds all the components of NC3 through communication networks. The country's reliance on computer networks for Command Control and Communication could make it vulnerable to cyber-attacks that disrupt or degrade its C3 capabilities. Additionally, integrating cyber capabilities into conventional military operations can increase the risk of cyber escalation in a crisis. This research proposes a framework for the NC3 system of Pakistan by integrating SAFER (Security Assessment Framework for Embedded Device Risks) in NIST CSF (Cyber Security Framework) and integrating Cost Benefit Analysis of cyber security investments in the tier implementation part of NIST CSF.

Table of Contents

Introduction.....	1
1.1 Motivation & Problem Statement	2
1.2 Thesis Contributions	2
1.3 Thesis Organization.....	2
Literature Review.....	4
2.1 Cyber Threats to Nuclear Systems	4
2.2 Nature of Modern Cyber-Attacks and Attack Paths.....	8
2.3 NC3 Systems of Nuclear States	9
2.4 State Policies for Cyber Security	12
2.5 Vulnerabilities of NC3 Architecture	13
2.6 Frameworks and Controls by NIST	13
2.7 Automated Frameworks for Risk Prediction of Devices	14
2.8 Cost-Benefit Analysis in Cyber-Security	16
Research Methodology	17
3.1 Research Design.....	17
3.2 Selection of NIST Framework	17
3.3 Literature Review Methodology	18
Proposed Cyber Security Framework for Mitigating Cyber -Nuclear Threats to Pakistan	19
4.1 Importance of Cyber Security in NC3 System of Pakistan.....	19
4.2 Components of NC3 systems of Pakistan	19
4.2.1 Command & Control Systems	20
4.2.2 Communications systems.....	20
4.2.3 Industrial control systems	21
4.2.4 Early warning systems	22
4.2.5 Supply Chain.....	23

4.2.6	Launch systems	23
4.3	Types of Cyber Attacks and Cyber Operations.....	24
4.3.1	Types of Cyber Attacks	24
4.3.2	Cyber Operations	27
4.4	NIST Cyber Security Framework	30
4.4.1	Framework Core	31
4.4.2	Framework Implementation Tiers.....	32
4.4.3	Framework Profile	34
4.4.4	Stepwise creation of Cyber Security Program.....	34
4.5	Proposed framework	35
4.6	SAFER Framework.....	36
4.6.1	Device Identification.....	37
4.6.2	Firmware & Vulnerability Analysis.....	39
4.6.3	Risk Metrics	40
4.7	Cost Benefit Analysis based on Gordon Loeb Model.....	44
	Conclusion & Future Work.....	47
	References.....	49

List of Figures

Figure 1 Components of NC3 System	20
Figure 2 Cyber Kill Chain & Enterprise Attack Matrix for Identifying Attack Source .	27
Figure 3 NIST CSF Core Functions	31
Figure 4 Integration of Cost Benefit Analysis and Automated Vulnerability Assessment in NIST CSF	36
Figure 5 Overview of SAFER Framework	37
Figure 6 Assessed Devices of CERN by SAFER	44
Figure 7 Gordon Loeb Model	45

List of Tables

Table 1 Digital Database for Literature Review	18
Table 2 Functions of NIST Cyber Security Framework	32
Table 3 NIST CSF Implementation Tiers	33
Table 4 FDSRI Risk Matrix	43

Introduction

Pakistan formally announced its nuclear capability by conducting nuclear tests in 1998. Unlike India, which published its nuclear doctrine, Pakistan kept its doctrine a secret while emphasizing a robust Command & Control System. In this regard, the National Command Authority was set up, which dealt with everything Nuclear. Since then, Pakistan has expanded its nuclear arsenal. Pakistan has a nuclear stockpile of approximately 165 warheads. Warheads and their delivery systems are the front ends of strategic warfare. However, a comprehensive NC3 (Nuclear Command Control and Communication) system is required to i) ensure early warnings and detection of threats, ii) Provide the decision makers with authentic information for a suitable yet prompt response, iii) Relaying of the decision through authenticated channels to the strike forces, iv) employment of nuclear arsenal. Presently, Pakistan has declared its nuclear capability as a deterrent to any tactical/strategic warfare threat, i.e., the adversary will evaluate that the cost of an attack on the target country can be very high in terms of financial and human loss as the target country is a nuclear-capable state. That is why, although the exact nuclear capabilities of any state are unknown even then; their nuclear strength is displayed during national parades to deter the adversaries. Therefore, tactical warfare and strategic warfare are different as tactical warfare relies on the element of surprise and is mostly covert operations with reliance on weapons of first use. Strategic warfare is mostly overt operations where posture signaling is used to warn the enemies, and no-first-use weapons are used. Cyber-attacks are more like tactical warfare because their effectiveness relies on the secrecy of the attack, e.g., as soon as the target knows about the malware used for the attack, it can be removed very easily. The NC3 systems of nuclear states are in a transitional state. A combination of legacy systems and modern information and communication technologies are being employed in the NC3 architecture. This makes the NC3 systems also vulnerable to cyber-attacks. In a cyber-attack, attribution to an adversary and threat assessment (recon, espionage, war, etc.) are significant challenges. The target state must decide its reaction within a limited time. The uncertainty of the situation poses the risk of escalation and initiation of a nuclear war. China and the US are interested in maintaining a cyber-nuclear balance to mitigate the nuclear threat. Similarly,

it is essential that Pakistan being a nuclear state with a hostile nuclear-enabled neighbor in the East, optimizes its NC3 capabilities and simultaneously initiate a dialogue with India to devise a comprehensive regional cyber operations policy to mitigate subsequent nuclear escalation.

1.1 Motivation & Problem Statement

There is a visible asymmetry between the tactical capabilities of Pakistan and other nuclear states. India has openly announced its cold start doctrine through which it will undertake surgical strikes against Pakistan while remaining under the nuclear threshold. These surgical strikes can also include sophisticated cyber operations. Therefore, Pakistan needs to re-evaluate its nuclear use threshold and strengthen its NC3 to strike a balance between the military capabilities of the two countries. By proposing a comprehensive framework for mitigating cyber-nuclear threats, the NC3 system can be modernized to defend against modern cyber-operations.

1.2 Thesis Contributions

This thesis provides consolidated information about the nuclear posture, doctrine and NC3 systems of a nuclear state. The relationship of nuclear escalation with cyber-attacks on NC3 systems is explained in detail. It further discusses NIST Risk Management Framework, Cyber Security Framework and Security and Privacy Controls. Automated Vulnerability Assessment of Embedded devices is proposed to be integrated in NIST CSF, subsequent to which cost benefit analysis for investment in cyber security is proposed for integration in NIST CSF. As the information about NC3 systems of Nuclear States is classified, there was no official information about these systems. However, after conducting research from distributed sources, this research has been able to visualize the components of the NC3 system of a nuclear state and provides a meaningful insight into these systems.

1.3 Thesis Organization

The thesis is structured as follows

- Chapter 2 contains the literature reviewed in the thesis. Historical cyber-attacks that had negative effects on the nuclear stability of states were studied. Relationship between NC3 systems and cyber-security was determined and different security and risk frameworks were studied in this literature review.

- Chapter 3 provides the research methodology that was adopted to develop the thesis. Literature review methodology and digital databases for accessing contents are provided in this chapter.
- Chapter 4 proposes the framework for mitigating cyber-nuclear threats and achieving C3 stability. The chapter starts with emphasizing the importance of cyber-security in NC3 systems. Subsequently, the components of NC3 systems and their possible information systems are discussed. The types of attacks and increased sophistication in attacks in the form of APTs and cyber operations is discussed afterward. NIST Cyber Security Framework is then explained after which the detailed process of the SAFER framework and its integration in CSF is discussed. The final part of this chapter discusses the Gordon-Loeb model for integration in NIST CSF.
- Chapter 5 is the conclusion of the thesis. The thesis is summarized and some limitations of the research and future work are discussed in this chapter.

Literature Review

2.1 Cyber Threats to Nuclear Systems

A Cyber-Nuclear Weapons Study Group report provides four illustrative scenarios in which cyber threats to nuclear systems, their implications, and the plausibility of such attacks are discussed. These four scenarios highlight the vulnerable aspects of the NC3 systems and the potential consequence of a specific type of cyber-attack by exploiting those vulnerabilities. The first scenario involves false positives generated by early warning systems. Supposedly if NORAD USA receives a false positive alarm of a missile launch by Russia which is then relayed to the White House, the US high command would have a small bracket of time to make decisions, which can lead to the launch of nuclear missiles in the fear of “using it or losing it.” The second scenario involves a cyber-attack that disrupts communication between NC3 high command and nuclear systems, operators, and nuclear systems or international counterparts. For example, during the war, if Russian American dialogue channels are compromised, there will be no way for Russia to ask the USA if the USA is carrying out cyber-attacks. The plausibility of this kind of communication disruption is high, as it has happened in the past. In 2015 a DDoS (distributed denial of service) cyber-attack on Ukraine’s power grid cut off the telephone lines, and the information about power outage could not be relayed to its customers. In another incident, a malware named Slammer worm infected Ohio’s Davie Bessie nuclear power plant, and sensitive information about the core reactor could not be displayed for five hours. Scenario 3 discusses the event in which malware is introduced in the NC3 system of the target through its supply chain. An adversary, under the guise of a third-party organization can embed malware in an NC3 component. This kind of attack can undermine the confidence of the target state about its nuclear deterrence. The plausibility of this scenario is also high as this happened in the case of Operation Olympic Games when Stuxnet was introduced into the nuclear power plant of Iran and destroyed around 1000 centrifuges in the Natanz facility of Iran. Another scenario is discussed where the adversary seizes control of nuclear warheads. For example, the access control security of a storage site in the USA is compromised, and a warhead goes missing. A similar situation

surfaced in 2016 in the Incirlik air base. During the ongoing coup in Turkey, the base commander was detained under the suspicion of the coup, the electricity of the base was cut off, and U.S Airforce planes were grounded. This base housed U.S. forward-deployed nuclear warheads. It is deduced from the report that cyber-attacks are a real threat to the nuclear systems of states, and despite improvement in the cyber security mechanisms of states, a revision in the nuclear posture of states is required to minimize risks induced by cyber threats [1].

Analysis performed by Chatham House identifies the incidents of near-nuclear use and the factors that led to the tension escalation among nuclear-armed states [2]. It further highlights that the probability of nuclear use has risen again after a reduction post the cold war. This rise in probability can be attributed to an (i) increase in the number of weapon possessor states, (ii) Increased dependence of states on nuclear weapons for their safety and security, and (iii) Threat of nuclear terrorism.

Operation Olympic Games is discussed in [3], which was a cyber-attack on the critical infrastructure of an Iranian nuclear facility. It was the first incident where a virus popularly known as "Stuxnet" destroyed 10,000 centrifuges in an Iranian nuclear facility. This attack caused a delay in the development of Iran's nuclear program; however, it did not stop them from the development process. This study highlights that the US achieved tactical success by delaying Iran's nuclear program development and gaining a psychological advantage by displaying technical superiority in cyberspace. Furthermore, it avoided military engagement, which could have worsened the international situation. The number of resources that were used for a single operation indicates that planning and executing a sophisticated cyber-attack against an adversary is a resource-exhaustive exercise. Presently, it can be carried out by developed countries only.

“A Historical Study of Nuclear Connectivity” [4] details the false alarms generated by NORAD (North American Aerospace Defense Command). In November 1969, a tape from an exercise was mistakenly run on the operational computers at the Cheyenne Mountain complex. Consequently, missile launch warnings were relayed to NORAD’s strategic air defense centers and displayed in the Command-and-Control centers and NMC of the USA. As a result, the armed forces were sent on alert for the next ten minutes. A review board was formed to investigate the matter, which recommended that hardware and software testing of systems should not be done on operational computers. A few

months later, another false alarm of a missile attack was generated but was successfully identified as a false positive. Post-event investigation attributed the false alarm to a faulty microchip in a computer. As a result, this chip and circuit boards were redesigned to avoid future untoward incidents. This paper further explains the efforts by the US government to harden specific components of USA NC3 against an EMP attack which could render the communication unusable. In this regard, TACAMO (Take charge and move out), command centers, dedicated phone lines, High Altitude Nuclear Detection (HAND) sensors, and Defense Satellite Communication System (DSCS) were hardened [4].

Satellites are vital to the NC3 architecture as they relay sensor information to ground stations and command centers. The various kinetic and non-kinetic threats faced by satellites are discussed in [5]. Cyber threats are categorized as non-kinetic threats to a satellite. Data theft, unauthorized access, and unavailability of satellite systems are some of the risks caused by a cyber-attack on a satellite. It further states some incidents where non-state actors hacked satellites through an offensive cyber operation. Dangers caused by cyber operations are considered a real threat to the satellite systems of an NC3. The primary advantage of a cyber-attack is the difficulty of attribution, i.e., in case of an attack, it will be difficult for the target to identify and punish the attacker, weakening the deterrence of the target state.

“Cyber Nuclear Nexus” [6] concludes that with the increasing digitization of NC3 systems, the entanglement of nuclear forces and cyberspace is more probable. Furthermore, cyber-attacks not directly targeted on nuclear systems can also indirectly cause nuclear escalation. It is, therefore important to lay down certain norms of cyberspace to reduce nuclear escalation risks.

A research paper that includes strategic experts from US and China funded by the Carnegie Endowment Fund focuses on the China-US C3 Stability [7]. The first part of the paper details the plausible nuclear escalation scenarios and provides a framework for their analysis. Four broad categories of scenarios are discussed, which include (i) Cyber Espionage: Gathering data about the core and within the core of a target state’s NC3 infrastructure (ii) Cyber espionage activities in systems that are used for strategic as well as tactical purposes or other systems that provide support or relate to NC3 (iii). Cyber-attacks targeting dual-use NC3 systems, which encompass both conventional and strategic capabilities, or supplementary systems associated with NC3, are conducted

without any intention to impact their nuclear functionality; and (iv) Situations that involve significant concerns regarding the intentions of the opposing state, coupled with apprehensions regarding the vulnerability of one's NC3 to cyber-attacks from adversaries. These scenarios can have four consequences, nuclear conflict, accidental use of nuclear weapons, crisis escalation, or long-term impacts such as a heightened arms race. The paper also stresses the diverging threat perceptions of the US and China. The US sees the expansion of Chinese tactical and strategic forces as a threat to its allies. At the same time, China perceives the US as much superior in the Cyber domain and sees that the U.S. might pre-empt a cyber-attack to blunt the Chinese deterrent. This distrust between the two nations is an obstacle to establishing confidence-building measures and defining no go areas in a cyber-operation by the two states. The second part of the paper discusses the steps that can be undertaken to enhance strategic stability and reduce cyber-nuclear threats. The authors suggest assured decision-making procedures. Domestic & Foreign Policy oversight, technical, operational, intelligence and legal oversight must be carried out to ensure confident decision-making at a state level about cyber operations. Improving the resilience of the two state's NC3 will also help stabilize the nuclear environment as presently, China understands the cyber superiority of the US and is apprehensive of a US cyber-attack to blunt the Chinese deterrent. Modernization of China's NC3 will help create a more stable environment. Furthermore, a commitment by both sides to not intrude on the core NC3 architecture of either state might also reduce the nuclear use risk. However, the NC3 architecture of both countries is complex, compartmentalized, and intentionally kept secret. It would be difficult to specify precisely out-of-bound equipment or system. However, a broad-based description of core NC3 can be provided to other states for mutual commitment.

USA's Nuclear Matters Handbook defines NC3 as follows: "U.S. command, control, and communications are necessary to ensure the authorized employment and termination of nuclear weapons operations, to secure against accidental, inadvertent, or unauthorized access, and to prevent the loss of control, theft, or unauthorized use of US nuclear weapons [8]. NC3 ensures the President's ability to exercise authority. The US is the only nuclear state which has publicly documented the structure of its NC3 systems; this document gives an insight to the NC3 system of the USA, which can be used as a benchmark by other nuclear states.

2.2 Nature of Modern Cyber-Attacks and Attack Paths

The attack path for Operation Olympic Games is described in [9]. In 2009, a highly sophisticated malware called Stuxnet was launched with the aim to disrupt Iran's uranium nuclear project. The malware was delivered to the Iranian nuclear facility through USB drives. Once inside the system, it exploited zero-day vulnerabilities in Windows Explorer and Windows Print Spooler System; the malware spread to the hosts connected to a printer. Subsequently, Privilege escalation was performed by utilizing vulnerabilities in the Windows Keyboard files and the task scheduler to gain complete control of the systems. After installation in the system, Stuxnet sent the Internal IP, Public IP, Installed OS, and information regarding the presence of Step7 Siemens software to its Command & Control Centre. In case of detection of Step7, the malware was executed, else it was altered to remain passive and keep replicating on other systems. Stuxnet was a complex and layered piece of malware that targeted programmable logical controllers, causing damage to Iran's centrifuges and slowing down their nuclear weapon production. Despite being discovered in 2010, the malware continued its operations until 2012. Stuxnet demonstrated the unprecedented power of digital code to affect the physical world [9].

Solarwinds attack was a software supply chain attack, which infected more than 18,000 customers and 40 public entities with malware. The attack path for Solar Winds is described in [10]. The attackers spoofed the identity of access accounts and inserted functions in the source code of a library file of ORION (Network Monitoring & Management Platform). Subsequently, Solarwinds signed the DLL and distributed it in the update process thereby infecting its customers with the malware. During the recon phase, a profile of possible target developers was created through social engineering. The DLL backdoor known as Sunburst or Solorigate was created and then executed by Solarwinds. The malware was wrapped in an updated version of Orion's network management software and delivered to the target developer by spearphishing. As soon as the target would install the update executable, the malware was installed which opened a backdoor in the victim's server for the attacker to access the services. Sunburst then sent the Windows Domain name to C2 server. In this way, the source code was controlled for installation of sunburst, which created backdoors that would be distributed to all customers in form of updates. Solarwinds signed this update and distributed it.

Analysis of the Cyber Attack on the Ukrainian Power Grid details the technical attributes of the cyber operation [11]. In 2015, Ukrainian energy companies reported severe outages to their customers which was attributed to the illegal intrusion of an adversary in the company's computer and SCADA systems. Initially, two substations of the energy company were disconnected which spread to additional services later on. It was reported that three energy companies were attacked in this manner causing discontinuation of services to 225,000 customers. Ukrainian authorities claimed that the incident was a cyber-security attack conducted by Russian agencies. The recon activities for this attack are unknown; however, considering simultaneous, coordinated and sophisticated attack on three energy companies, it can be safely supposed that the adversary had obtained sufficient knowledge about the internal mechanisms of the companies and their respective control systems. Black Energy 3 Malware was embedded in Microsoft Office during the weaponization phase. The malicious files were then delivered to the network of electric companies through phishing mail. Once the users opened these documents, a pop-up appeared advising the user to enable macros. This enabled the attacker to exploit the Office Macro Vulnerability and install Blackenergy 3 on the target system. Throughout the attack path, already available vulnerabilities were exploited. Once installed, the malware was used for credential harvesting and gaining access to systems and enabled the attacker to blend into the system under the guise of a valid user. This enabled the attacker to identify VPNs connecting the enterprise network to the Control Systems. The attackers extended their attack to the control systems through remote administration tools on operator systems. Finally, a modified form of malicious software, "KillDisk" was installed across the control systems. Resultantly, operators were locked out of their systems. Afterward, HMI (Human Machine Interface) in SCADA environment were used to open the breakers causing the power outage. Simultaneously, malicious firmware was installed in the serial to ethernet gateway devices that discontinued remote connectivity of the operator with control systems. A telephonic DoS attack was also initiated; as a result, customers could not report the outage to their respective companies.

2.3 NC3 Systems of Nuclear States

NC3 architecture of China is discussed in [12]. China maintains a "No first use policy" for its nuclear weapons. It states that early warning threat detection and relaying of the same to higher command is the priority of the Chinese NC3, whereas survivability of the systems is the second priority. Early NC3 system of China relied on radio frequency

communication, however, with the advent of technology, fiber optic and satellite communication has been introduced in the NC3 system. The strategic setup of China (second artillery) comprises of a dedicated fiber optic system. China has been using an automated command and control system since early 2000 i.e., relaying of command-and-control messages over authentic communication channels, remote monitoring, tracking of missile launches through live audio and video, intelligence gathering, weather tracking and order issuing. The brigade headquarters of the second artillery have a dedicated computer network for command and control. Early warning setup of China consists of ground-based radars. Presently, China has three phased array ground-based radars. It does not have a space based early warning detection system. Moreover, China has also developed a ground based nuclear detection network through seismic waves, electromagnetic pulse etc. The nuclear warheads of China are stored in various parts in spatially apart locations to ensure negative controls over the warheads and are only assembled during exercises or wartime. China also possesses use control devices for its warheads. Chinese nuclear forces have a three-tier alert system. In the first-tier state, warheads and missiles are separate and stored in spatially apart location. In the 2nd tier the artillery starts preparing for the launch orders whereas the forces are ready for launch orders in the 3rd tier. There has been some discussion on launch on warning alert but that denies the China no first-use policy [12].

NAPS Net special report on Russian NC3 [13] describes the nuclear posture of Russia and the composition of its NC3 system. It states that both US and USSR accumulated nuclear weapons during the cold war up to the extent that 90 % of the nuclear weapons of the world were possessed by these two states. Both the countries signed several agreements for nuclear arms reduction to reduce reliance on nuclear weapons. However, after the dissolution of Soviet Union as the Russian economy saw a decline, its conventional military strength also deteriorated. There was a visible asymmetry between the conventional military strengths of USA and Russia which forced the latter state to increase its reliance on nuclear warheads. National Defense Command & Control Centre (NDCCC) provides management over all spheres of Russian armed forces. This includes Nuclear Strategic Forces command & control centers, Combat Command & Control Centers. Use of nuclear weapons is managed by the Nuclear Strategic Forces command & control centers under supervision of senior political leadership of Russia. Russia has a nuclear triad, which includes Strategic Rocket Forces, Airforce Strategic Aviation and

Navy Nuclear Ballistic Missiles Submarines. Combat Management Automated System (CMAS) of Russia is named “Kazbek.” The portable component of this system is known as “Cheget” or “Nuclear briefcase.” The President, Minister of Defense and Chief of General Staff have these briefcases. Launch codes are transmitted from these briefcases to Command Posts of SRFs. Permission is granted only on reception of message from at least two briefcases. With improvement in the CMAS system, inflight targeting of Ballistic Missiles will also be possible. A duplicate Command & Control center named “Perimeter” based on Artificial Intelligence has also been developed by Russia to ensure a nuclear strike even if its SRF and weapons are destroyed.” The Russian NC3 includes a Ballistic Missile & Early Warning System (BMEWS). The task of BMEWS is to provide continuous, timely, and reliable information to political and military leadership on the current situation of missiles throughout near-earth space and any changes in that situation that might pose a threat to the Russian state. This BMEWS consists of ground-based VHF/UHF Radars along the periphery of the country, satellite-based infrared detection systems in the space surveillance system, and the Ballistic missile defense system. Russians claim that their NC3 architecture is impervious to a cyber-attack as they have isolated networks for nuclear command & control; however, BMEWS components such as radars and satellites can still be accessed by a third party for data theft, generation of false alarms, etc.

UK and U.S. provide the nuclear capability of NATO as per [14]. Like any other nuclear-enabled state, NATO also has an elaborate NC3 system in place. This paper stresses that NC3 systems require the adoption of suitable measures to prevent cyber-attacks. The five themes across which cyber security is required are software & network protection, data (integrity) protection, hardware protection, access/security control and cybersecurity awareness/security by design. This paper also emphasizes taking into consideration the risks that come with procuring military equipment from adversary states such as Russia [14].

Pakistan conducted its nuclear tests in 1998. While India stressed defining its nuclear doctrine, Pakistan opted to keep its doctrine secret while designing an elaborate system for nuclear command and control. In this regard, the National Command Authority was formed in the year 2000 with SPD (Strategic Plans Division) as its secretariat [15]. NCA is the highest body for policymaking and development of all nuclear programs of Pakistan. Furthermore, it also controls the use of all strategic weapons of Pakistan.

Chairman of NCA is the Prime Minister while the Chairman Joint Chiefs of Staff Committee is the deputy chairman of DCC (Development Control Committee) and Foreign Minister is the Deputy Chairman of ECC (Employment Control Committee). ECC provides policy guidelines for the development of nuclear programs and reviews the threat assessment and appropriate response. DCC, on the other hand, implements the policy devised by ECC and directly oversees the development of nuclear programs. Strategic Plans Division is the secretariat of NCA.

Nuclear posture of Pakistan is defined as a full spectrum deterrence in the form of long-range strategic missiles and short-range TNWs (Tactical nuclear weapons) [16]. This posture of Pakistan is in reaction to the cold start doctrine of India, where 4 to 5 brigades will conduct a quick operation in Pakistan while remaining below the nuclear threshold. NASR is one such TNW to counter the cold start doctrine. As tactical nuclear weapons are battlefield ready, they have also raised concerns in the U.S. that such weapons increase the risk of accidental usage and are a security hazard. However, Dr. Samar Mubarakmand has aptly replied to the concerns by explaining that nuclear warheads are assembled only during the time of war and are stored in various locations separately during peacetime [16].

2.4 State Policies for Cyber Security

USA has developed several policies and initiatives aimed at strengthening the nation's cybersecurity. CNSS Policy No. 22 [17] is a high-level policy that outlines the information assurance risk management requirements for US government departments that use, maintain, operate, or develop National Security Systems. The policy mandates the development of an IA risk management system that establishes an acceptable risk threshold within the organization and provides information assurance to receiving organizations.

PECA was passed by the parliament of Pakistan in 2016 for dealing with the uprising threats of cybercrimes in Pakistan. It states that the cyber activities such as spamming, spoofing, un-authorized access to critical infrastructure, un-authorized interception of communication, child pornography, online stocking/harassment are offences punishable by law. This act states that responsibility for investigation of cyber-crimes rests with FIA (Federal Investigation Agency) [18].

National Cyber Security Policy 2021 has been formulated by MOITT (Ministry of IT & Telecom), Pakistan [19]. It states that a CGPC (Cyber Governance Policy Committee) has been formed to oversee and formulate a strategy to better deal with the cyber security threats. This committee will be responsible for the formulation and approval of cyber security policies and acts. More importantly, this document lays down some guidelines for protection of information systems in government departments. Some of these recommendations are i) Establishment of data centers federally and provincially ii) Defining a data protection framework including data classification, iii) Establishment of a vulnerability and patch management program, iv) Allocation of funds for implementation of cyber security measures, v) Formulation of a security clearance and vetting mechanism for recruitment of new staff and monitoring of existing staff in government organizations. vi) Setting up a mechanism for security clearance and vetting of suppliers for the protection of the government supply chain. Furthermore, it recommends formulating governance rules, regulations, and risk management frameworks. However, a lot of work needs to be done as cyber security in Pakistan government organizations is in its nascent stages.

2.5 Vulnerabilities of NC3 Architecture

Nautilus Institute for Safety and Security lists down some of the vulnerabilities of the NC3 architecture that can be exploited and become a risk. It further suggests some measures like cyber and physical security best practices, redundant supplies, communication, sensors, and systems to mitigate these risks. Moreover, creating a network monitoring cell and adopting cybersecurity best practices are suggested. It further compares the operational and Strategic factors of the “Nuclear Domain” and “Cyber Domain” [20].

2.6 Frameworks and Controls by NIST

In 2013, NIST Cyber Security Framework was introduced because of a directive from the US presidency and was subsequently updated in 2018 [21]. Currently, NIST is in the process of updating the CSF and NIST CSF version 2 is expected to be released in 2024. The primary goal of the framework was to develop effective strategies for safeguarding data and information against potential threats and breaches. The framework was designed to meet the specific data protection needs of the US government and other nations. While

the framework incorporates the fundamental requirements for data protection, each country can tailor it to their unique needs.

Risk Management Framework for Information Systems and Organizations NIST SP 800-37 was created in December 2018 and describes the Risk Management Framework that lays down basic guidelines for managing security and privacy risks and implementation of this framework on information systems and entire organization [22]. The objective of this framework is to i) Promote development of secure software ii) To integrate SCRM (Supply Chain Risk Management) concepts in RMF (Risk Management Framework) iii) To demonstrate integration of NIST CSF (Cyber Security Framework) with RMF. The risk management approach is applied at Organization, mission/business process and systems level in this framework.

Security controls that are referenced in NIST Cyber Security Framework and NIST RMF are listed in NIST SP-800-53 [23]. This document provides a collection of security and privacy controls to safeguard the assets of organizations and individuals from various threats such as human errors, natural calamities, and foreign intelligence agencies. These controls are flexible and can be customized to suit the needs of the organization. They cover a range of requirements based on the organization's mission and business objectives, as well as legal requirements and industry standards. Furthermore, the controls provide both functionality and assurance in terms of security and privacy. This approach aims to ensure that IT products and systems are dependable and trustworthy.

Methodology for assessment of NIST Security and Privacy Controls is available in NIST SP-800-53-A [24]. This publication offers a method and set of processes for evaluating security and privacy controls used by systems and organizations within a risk management framework. The evaluation processes align with the security and privacy controls in NIST Special Publication 800-53, Revision 5, and can be adjusted to fit an organization's risk tolerance. Additionally, the publication includes information on creating effective assessment plans and analyzing assessment results.

2.7 Automated Frameworks for Risk Prediction of Devices

[25] Presents and shares evaluation of SAFER framework (Security Assessment Framework for Embedded Device Risk). Considering large number of networked devices within the organization, accurate asset identification, vulnerability assessment and risk estimation is a skill extensive process. SAFER automates this process by providing

automatic asset identification through CCD (Clock Characteristics Detection) which collects TCP time stamps and WPD (Web Pattern Detection) which accesses http-based pages of devices. XPATH is used to narrow down the content where WPD should be applied in a webpage. Identification results from both methods are then passed through a fusion process based on probabilistic logic framework called subjective logic to enhance the probability of correct identification. Subsequently, device brand, models and firmware used within the organization are identified. SAFER then retrieves unprocessed firmware images by crawling official manufacturers websites. Firmware decompression or unpacking is implemented by FACT (Firmware Analysis and Comparison Tool). 16 YARA (Yet Another Recursive Acronym) rules are applied on unpacked firmware for identification of software libraries. Vulnerability analysis of software libraries is conducted by using CVE search to retrieve publicly available vulnerabilities. SAFER's local vulnerability database is updated on an hourly basis. Vulnerabilities for device model software are identified from MITRE, which is the vulnerability numbering authority. Additional vulnerabilities in unpacked firmware, such as pre-defined passwords or sensitive cryptographic keys are detected by SAFER through its binary analysis plugin, which uses regular expression. Subsequent to the vulnerability enrichment, risk rating of vulnerable assets is performed based on Risk Metrics. CDSRI (Current Device Security Risk Indicator) & FDSRI (Future Device Security Risk Indicator) are two indicators used for this purpose. As the name suggests, CDSRI provides the existing risk rating of devices, whereas FDSRI provides the future risk rating of devices. CDSRI uses CVSS 3.0 and calculates the maximum vulnerability score of an unpatched vulnerability (Impact of vulnerability ranges from 0~to 10 in CVSS 3.0). The assumption is that attackers will exploit the most severe and unpatched vulnerability to save time and cost. FDSRI uses VT (Vulnerability Trends) based on the predictive model ARIMA to predict the vulnerability level of a device based on historic vulnerabilities. PT (Patch Trends) based on Prophet predictive model provides the median capability of vendors to patch new vulnerabilities based on data where vulnerabilities were first discovered and how long it took the vendor to patch them. VT is categorized into low, medium, or high and PT is categorized as Fast, Medium, or Slow. FDSRI combinations of VT and PT assess which device will be high risk in the future. This framework provides a less invasive identification technique, secondly, instead of analyzing large base of software code for vulnerabilities, it uses public vulnerability databases to assess the frequency of vulnerabilities in the firmware and the time vendors take to patch them. This

enables it to assess risk for close source software also. The underlying assumption of this framework is that adversary exploits the vulnerability once it is publicly published; therefore, this framework is not applicable to Zero-Day vulnerabilities. SAFER identifies the vulnerabilities in the firmware and advises the organization to update their device to a safe version of the firmware.

Research at [26] argues that SAFER conducted its device identification process on 38 devices only and based on this small data set, the framework predicted current and future risks with approximately 100 % success. This research tries to implement the SAFER framework on a large data set of devices to validate the accuracy claims of SAFER framework. To achieve this, SAFER framework was evaluated on 838 device models with 6123 different firmware versions. SAFER achieved correct FDSRI prediction for 793 devices i.e., 93 % accuracy.

ReVeal framework was proposed in [27] for automated vulnerability prediction. This framework performs vulnerability predictions on Linux Debian Kernel & Chromium relying on the vast amount of publicly available data related to both code bases.

In a study conducted by [28], an extensive analysis was performed on the Linux Kernel using over 570,000 commits spanning from 2005 to 2016. The researchers noted that the most effective methods for predicting future vulnerabilities relied on utilizing header files and function calls.

2.8 Cost-Benefit Analysis in Cyber-Security

The Economics of Cyber Security [29] discusses the amount of investment that is being done for protection of information systems annually. It argues that despite heavy investments in the cyber security sector of USA (15 billion USD per year), economic impact of cyber security breaches is very large. It further states that 75% of cyber-attacks are low sophistication attacks. Therefore, there is a need to rationalize the investments in the cyber security sector. It recommends practicing the implementation of baseline controls for protection of devices and conducting a cost-benefit analysis prior to further investment in cyber-security.

Research Methodology

3.1 Research Design

A thorough literature review was conducted to determine the Nuclear Posture of States, nature of a typical NC3 infrastructure, scenarios and incidents that could cause nuclear escalation. It was found that due to classified nature of NC3 infrastructure, cybersecurity frameworks of nuclear states are not found publicly. However, each nuclear state recognizes the importance of cyber security measures and has laid down certain procedures and guidelines to secure its systems against potential cyber threats. Furthermore, NC3 systems are highly layered as they consist of weapons, industrial control systems, early warning systems, command centers, supply chain of information systems. The literature review is therefore divided into three parts. In the first part, incidents of near nuclear use, scenarios in which nuclear escalation is possible and modern case studies such as Stuxnet and Solar Winds are discussed. It was found during the research that President Trump had issued a notification to implement NIST (National Institute of Standards & Technology) Cyber Security Framework in organizations whereas implementation of NIST RMF is already mandatory for Federal Organizations of USA. Similarly, CNSSP No. 22 also advises to implement NIST frameworks. Therefore, NIST Risk Management Frameworks, NIST Cyber Security Framework and NIST Controls for Security & Privacy were studied in the 2nd part of literature review. In parallel cyber security legislation, (PECA) and National Cyber Security of Pakistan were also studied. The third part of literature review covers the automated vulnerability assessment frameworks, including SAFER and the economics of security investments.

3.2 Selection of NIST Framework

As discussed in the previous section, NIST Risk Management Framework and NIST Cyber Security Framework were studied during the literature review. It was deduced from the nature of NC3 systems of state and the elaborate cyber operations they are exposed to that a high-level framework for addressing cyber security concerns is required. Therefore, a comparison of NIST RMF and NIST CSF was done. RMF is used for providing guidelines for creating a Risk Management Framework that addresses security

as well as privacy controls. It also integrated NIST Cybersecurity Framework in it. RMF is implemented at organization, business and systems level separately. Both the frameworks are very useful and can be used in combination i.e. for Risk Management & Security Management. As we are proposing an initial security framework for the NC3 structure of Pakistan, NIST CSF owing to its simplicity is proposed for a higher-level security framework. In future, RMF can also be used as the Risk Management Framework.

3.3 Literature Review Methodology

Digital databases were searched for relevant papers, report, and articles. The list of this database is shown in Table 1. The abstract and conclusion of research papers retrieved from the databases was studied for relevance with the thesis. Three main schemes for filtering the accessed data were used. First, research papers consisting of nuclear posture of states, their doctrine and NC3 systems were gathered. In the second phase, multiple NIST publications were studied and NIST RMF, CSF and NIST Controls were selected for literature review. In the third phase, papers related to automation frameworks for vulnerability analysis were studied. Papers that were found closely relevant were then studied in detail.

Digital Database	URL
Google Scholar	https://scholar.google.com
IEEE Explore	https://ieeexplore.ieee.org
Science Direct	https://www.sciencedirect.com/
National Institute of Standards & Technology	https://NIST.gov
NAUTILUS Institute for Safety & Security	https://nautilus.org/

Table 1 Digital Database for Literature Review

Proposed Cyber Security Framework for Mitigating Cyber -Nuclear Threats to Pakistan

4.1 Importance of Cyber Security in NC3 System of Pakistan

Pakistan became a nuclear power in 1998 officially after India tested its nuclear warheads in Pokhran. Since then, the nuclear warheads of Pakistan are being used as a nuclear deterrent and a no first use policy is in place. There is a visible asymmetry in the tactical capabilities of Pakistan and Indian forces; however, the nuclear variable balances the equation between the two countries. It is therefore important for Pakistan that its nuclear systems are always available for use when required and never activated when not required. This has been ensured by the establishment of an NC3 architecture under the umbrella of NCA which provides a hierarchical command structure for initiation and termination of mission plans through its secretariat SPD. It is therefore important for Pakistani NC3 to ensure Confidentiality, Integrity and Availability of its NC3 architecture to maintain the ambiguity cloud around its nuclear capabilities, maintain tight controls over the execution of nuclear missions and retain the deterrence capabilities of the system, respectively.

4.2 Components of NC3 systems of Pakistan

Prior to proposing a framework for mitigating cyber-nuclear threats to Pakistan. It is important to have an overview of the components in the NC3 system. Due to the classified nature of NC3 systems, there is no public information regarding the information systems used in the NC3 systems of Pakistan and subsequent cyber security measures adopted by the relevant authorities. We have therefore relied on a black box approach to formulate the components of NC3 system based on the limited literature available. Figure 1 shows the components of NC3 extracted from Nuclear Matters Hand Book, USA [8]. The C2 (Command & Control) Centre controls or takes feedback from all the components from shooters to transport to sensors, which are bound to the C2 Centre through communication networks. This is a high-level diagram of the NC3 components; by researching separately for each component, a detailed picture of NC3 systems was

formed. Broadly, NC3 system consists of Industrial Control Systems, Pay Load Delivery Systems, Early warning Systems, Command Centers & Strategic Forces and the communication systems used to interconnect all the above components of NC3.

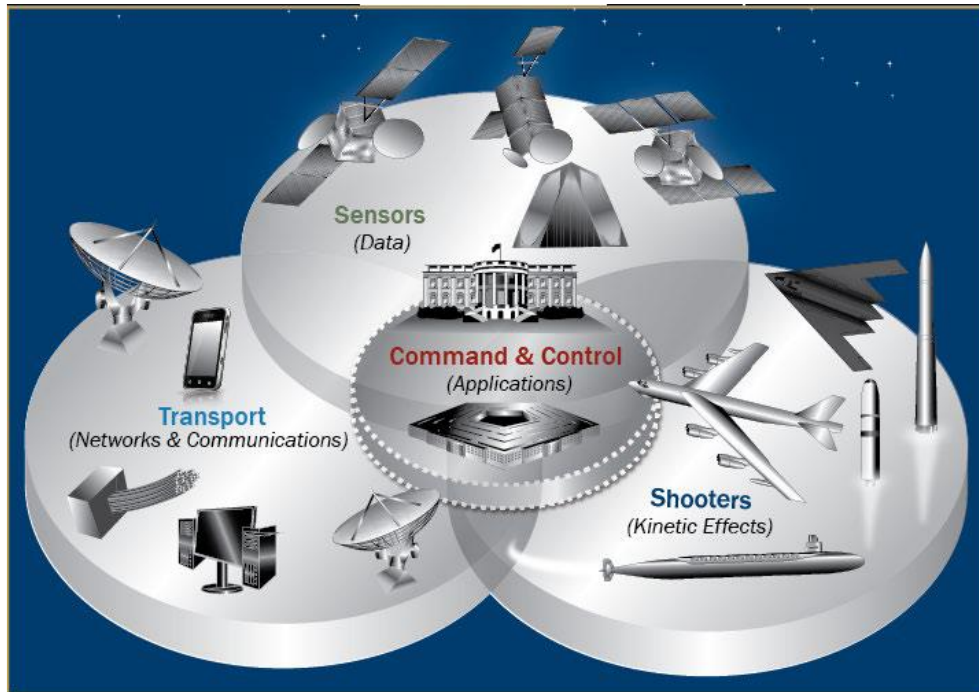


Figure 1 Components of NC3 System

4.2.1 Command & Control Systems

These are systems used to manage and control missile launch systems and other critical assets. These systems often include advanced computer networks and software applications that provide military and political leaders with real-time information about potential threats and other critical information and enable them to monitor and control nuclear forces in real-time. These systems often include advanced displays and visualization technology to provide decision-makers with a clear and concise picture of the situation on the ground.

4.2.2 Communications systems

These are systems used to transmit and receive information between decision makers and military forces. These systems often include secure communication channels, such as optical fiber, satellite links, transmission systems, access network (switches, routers, firewalls) and encryption technology to ensure that critical information is protected from unauthorized access.

4.2.3 Industrial control systems

NC3 (Nuclear Command, Control, and Communication) systems involve a range of industrial control systems that are designed to monitor, control, and communicate information about nuclear weapons and related activities. These systems typically require elevated levels of security and reliability to ensure the safe and effective use of nuclear weapons. The information systems used in NC3 (Nuclear Command, Control, and Communication) include a range of equipment that is used to monitor and control nuclear weapons and related activities. Some of the key information systems used in industrial control systems of NC3 include:

Supervisory Control and Data Acquisition (SCADA) systems are used to monitor and control industrial processes and equipment, such as nuclear reactors or missile launch systems. SCADA systems typically include software and hardware components, including sensors, controllers, and communication devices. SCADA server is referred to as MTU (Master Terminal Unit) in academic literature, the master Terminal Unit serves as the central device within SCADA architecture. It functions as the host for all supervisory, control functions, and data object models pertaining to the process assets.

Distributed Control Systems (DCS) are used to control and monitor complex industrial processes and equipment, such as nuclear power plants or missile launch facilities. DCS systems typically include advanced control algorithms and communication networks to enable real-time monitoring and control.

Programmable Logic Controllers (PLCs) are electronic devices used to control and monitor industrial processes. PLCs are often used in NC3 systems to control various processes, such as the operation of nuclear reactors or missile launch systems. PLCs have advanced capabilities in controlling intricate processes within both DCS (Distributed Control Systems) and SCADA (Supervisory Control and Data Acquisition) systems. PLCs possess the ability to handle complex logic for controlling process functions and communication, originating from the control server. In practical applications, PLCs are commonly linked to devices at lower levels, such as sensors and actuators

Human Machine Interface (HMI) provide operators with visual displays and control interfaces for industrial processes. HMI device is a software that is either hosted on computers or specialized hardware. It is utilized for monitoring processes, adjusting

control settings, and providing manual control overrides. HMIs can function as clients of SCADA servers or be directly connected to the control network.

Control servers and communication equipment are used to manage and control data communication and exchange within the NC3 system. They may include servers, routers, switches, and other networking equipment.

Reactor Protection Systems continuously monitors various parameters and signals within the reactor and its associated systems. If it detects any abnormal conditions that could jeopardize the safe operation of the reactor, it initiates an automatic shutdown sequence known as a reactor trip or scram. The RPS acts as a failsafe mechanism, independent of human intervention, to ensure the reactor's safety.

4.2.4 Early warning systems

EWS (Early Warning Systems) are a critical component of NC3 (Nuclear Command, Control, and Communication) architectures, providing information about potential threats and enabling timely and informed decision-making. The equipment used for early warning systems in NC3 architecture can vary depending on the specific system and its intended purpose, but includes the following types of equipment.

Sensors are used to detect and measure several types of signals, such as radio, radar, or infrared. For example, Ballistic Missile Early Warning Systems (BMEWS) use radar technology to detect incoming ballistic missiles.

Data processing systems are used to analyze and process data from sensors to identify potential threats. These systems often use advanced algorithms and artificial intelligence to analyze enormous amounts of data in real-time and provide actionable insights.

Communications equipment is used to transmit and receive data between early warning systems and decision-makers. For example, satellite communication systems are often used to provide real-time updates to military or political leaders.

Control centers are centralized facilities where operators can monitor and control early warning systems. These centers often use advanced displays, such as video walls or 3D graphics, to provide operators with real-time information about potential threats.

The equipment used for early warning systems in NC3 architecture is designed to provide accurate, reliable, and timely information about potential threats to enable effective decision-making in the event of a nuclear attack or other crisis.

4.2.5 Supply Chain

The supply chain of NC3 (Nuclear Command, Control, and Communication) systems typically involves the procurement, management, and delivery of a wide range of equipment and materials, including electronics, software, and other types of components. To support these activities, a variety of information systems are used throughout the supply chain of NC3 systems, including:

Procurement and inventory management systems manage the procurement of equipment and materials, as well as the storage and distribution of these items. These systems may include inventory tracking, purchase order management, and other types of procurement and supply chain management software.

Manufacturing and production systems manage the manufacturing and production of components and systems used in NC3 operations. These systems may include computer-aided design software, computer numerical control (CNC) machines, and other types of manufacturing equipment and software.

Logistics and transportation systems manage the transportation and delivery of equipment and materials throughout the supply chain. These systems may include transportation management software, warehouse management software, and other types of logistics and supply chain management software.

Quality control and testing systems ensure the quality and reliability of components and systems used in NC3 operations. These systems may include testing and inspection equipment, as well as quality control and quality assurance software.

4.2.6 Launch systems

These systems are used to launch nuclear weapons in the event of an order to do so. Launch systems may include missile launchers, launch control centers, and other types of hardware and software that enable the launch of nuclear weapons. These systems involve complex and highly secure information systems that are designed to support the launch of nuclear weapons. These information systems typically include:

Launch control systems manage the launch of nuclear weapons. They may include hardware and software components that enable military personnel to enter launch codes, authorize the launch of nuclear weapons, and monitor the launch process.

Communication systems communicate information about the launch process between the launch control center and the launch vehicle.

Positioning and navigation systems ensure that the launch vehicle is positioned correctly and follows the desired trajectory. Positioning and navigation systems may include GPS and other types of navigation technology.

Data processing and analysis systems process and analyze data related to the launch process. These systems may include software that can quickly analyze data and provide insights into the status of the launch process.

The information systems used in launch systems of NC3 are designed to ensure that nuclear weapons can be launched quickly and efficiently, while also maintaining a high level of security and reliability. These systems must be highly secure, resilient, and capable of operating in a variety of challenging environments.

4.3 Types of Cyber Attacks and Cyber Operations

4.3.1 Types of Cyber Attacks

Cryptanalysis is a cybersecurity technique, which is used to break an encryption algorithm without the encryption key. It is also used to find loopholes in digital signatures and hashes. There are certain ways in which cryptanalysis works. Cipher text only, plain text only, chosen plain text or plaint text pair.

DDoS (Distributed Denial of Service) attacks are executed using networks comprising internet-connected machines. These networks are comprised of computers and other devices, including IoT devices, that have been infected with malware. This malware enables remote control of these devices by the attacker. Individual devices within the network are commonly referred to as bots or zombies, while a collection of bots forms a botnet. Once a botnet is established, the attacker can issue remote instructions to each bot, directing them to initiate an attack. When the botnet targets a victim's server or network, each bot within the network sends requests to the target's IP address. This flood of requests can potentially overwhelm the server or network, leading to a denial-of-service situation where normal traffic is disrupted. Due to the fact that each bot in the

botnet is a legitimate internet device, distinguishing between the attack traffic and regular traffic can be challenging. This further complicates the process of mitigating the impact of the attack on the victim's server or network.

Ransomware refers to a type of malicious software utilized by threat actors to exploit computer systems or networks. Once infected, ransomware restricts access to the system or encrypts its data. To regain access or decrypt the data, the cybercriminals demand a ransom payment from the victims. To prevent ransomware infections, it is advisable to maintain vigilance and utilize security software. When affected by malware attacks, victims typically have three options; paying the ransom, attempting to remove the malware, or initiating a device restart. Extortion Trojans often employ various attack vectors, including the Remote Desktop Protocol, phishing emails, and software vulnerabilities. Consequently, both individuals and companies can become targets of ransomware attacks

Cyber Influence Operations involve using various means of communication and interaction to influence target audiences with the objective of changing their opinions and behaviors. When the goal is to control the responses of a group, it is referred to as perception management. In the military context, a term closely related to cyber influence is influencing maneuver [30]. It involves using cyber operations to penetrate an enemy's decision cycle, thereby influencing or even directing their actions. This maneuvering tactic aims to attain and maintain information superiority and dominance, while preserving freedom of maneuver in cyberspace. Influencing maneuver can be employed through direct or indirect operations. A direct example could involve compromising command and control systems and subtly manipulating data to undermine a commander's confidence in the systems and slow down decision-making abilities. Indirect actions might include providing compromised and manipulated data to the media to elicit a desired reaction from the enemy.

A **Spear Phishing Attack** refers to an effort to obtain sensitive information or gain access to a computer system by sending deceptive messages that appear legitimate. Spear phishing is a targeted form of phishing, where specific individuals or groups are focused on, often using information known to be of interest to the targets, such as current events or financial documents. These deceptive messages are typically delivered through email and aim to persuade the recipient into opening a malicious link or attachment, thereby

exposing them to harmful software. The primary objective of spear phishing is to obtain sensitive information like usernames, passwords, and personal details. Clicking on a phishing email link may lead to a malicious website, downloading unwanted content onto the user's computer. Opening an attachment can trigger the execution of malicious software, potentially compromising the security of the affected system. Once a connection is established, the attacker can initiate actions that jeopardize the integrity of the user's computer, the network it is connected to and the stored data. In the past, phishing emails were relatively easy to spot due to factors like unfamiliar senders, spelling mistakes, and poor grammar. However, modern phishing scams have become more sophisticated, with masked identities, tailored messages, and genuine-looking email content. Indicators of a phishing scam may include generic greetings, urgent requests for action that you didn't initiate, solicitation of personal information, or even unfounded threats.

The term "*Advanced Persistent Threat*" (*APT*) is commonly employed to describe a comprehensive attack campaign where an intruder or group of intruders infiltrate a network with the intention of maintaining an unauthorized and prolonged presence for the purpose of extracting extremely sensitive data. The primary objective of an APT attack is to establish persistent access to the system, which is accomplished through a sequential progression of five stages by hackers. These five stages are (i) gaining access to the network by exploiting a vulnerability, (ii) introduction of malware to establish backdoors and tunnels in the network to move undetected, (iii) strengthening the access by gaining administrator rights to the system. (iv) lateral movement in the system to access other secure servers (v) understanding the complete system from inside and exploiting it further on long term to harvest more information.

In a military context, *Traffic Analysis* is an essential aspect of intelligence, providing valuable information about the intentions and activities of the target. Continuous monitoring of target traffic can provide certain patterns with which attackers can extract useful information. For example, frequent communication pattern between two nodes implies some ongoing planning activity, lack of communication may imply lack of activity or recent completion of a mission plan, frequent communication from a central location to distributed locations might imply that the central location is a Command Center. Heavy traffic payloads during specific times may give insights on when an important activity is underway.

4.3.2 Cyber Operations

The nature of Cyber Attacks has changed in the present times as shown in the modern case studies in literature review. These cyber-attacks are not a simple DDoS attack or a spear phishing attack. Rather, states face elaborate and complex cyber operations today, which include multiple tactics and techniques to intrude in the target system, gain escalated privileges and remain in the system while evading detection to achieve the final goal of adversary. To understand the nature of these attacks, Cyber Kill Chain by Lockheed Martin and Enterprise Matrix by MITRE ATT&CK provide a complete path to execute an attack.

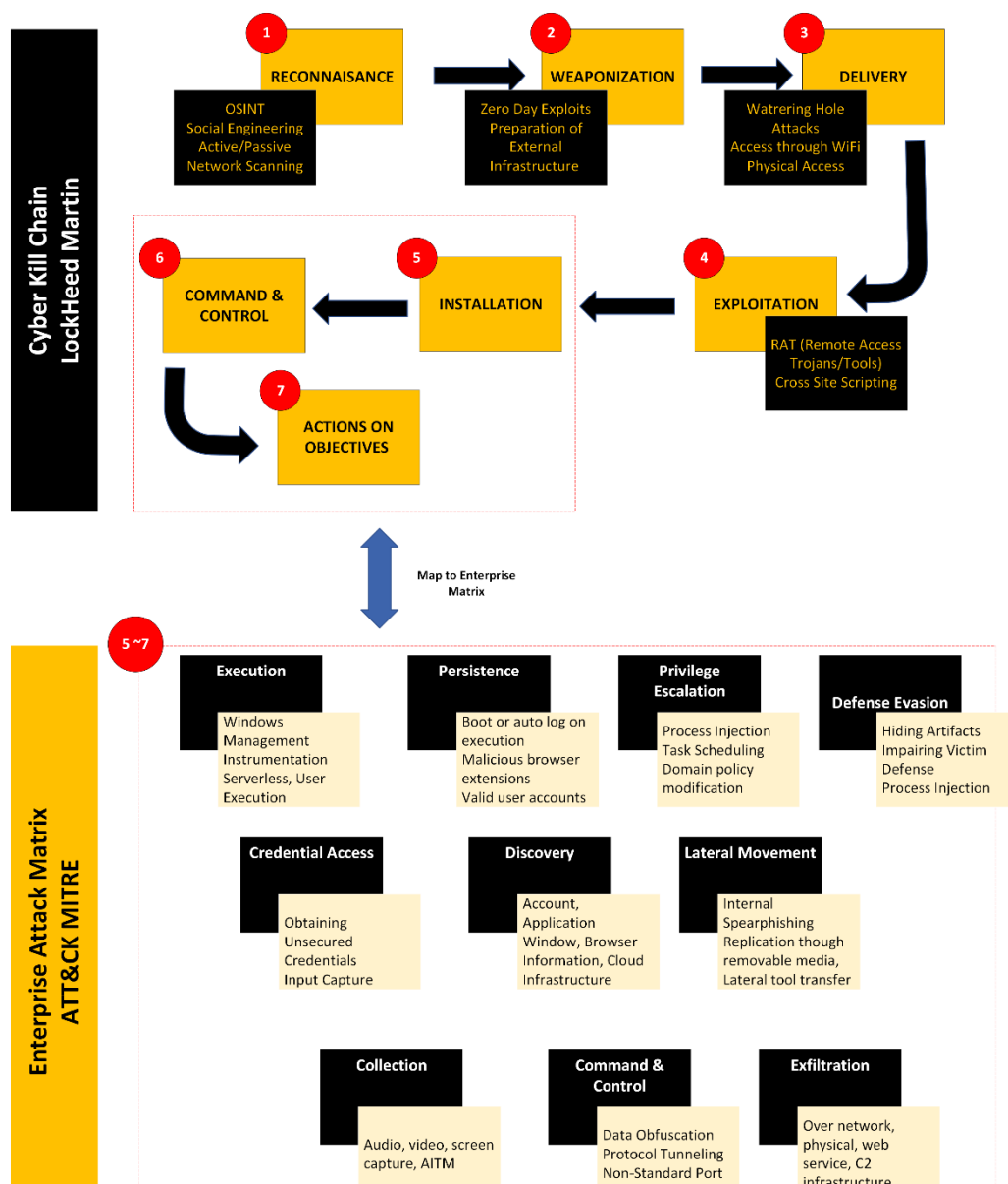


Figure 2 Cyber Kill Chain & Enterprise Attack Matrix for Identifying Attack Source

Reconnaissance is the first step of a cyber-attack; cyber attackers actively search for vulnerabilities to get inside the target system. This process involves gathering login credentials and other potentially valuable information that could be exploited in phishing attempts. Common attack techniques include OSINT Analysis (OpenSource Intelligence), Social Engineering, Active and Passive Network Scanning.

During the **Weaponization** phase, the focus is on constructing a deployable payload by utilizing an exploit within the target system, along with a backdoor that ensures continuous access over an extended period. Techniques for weaponization include research on zero-day exploits, evaluating standard payloads and preparation of external infrastructure such as cloud service in case of data exfiltration.

Delivery is the third step in the Cyber Kill Chain. Following the weaponization phase, the attackers transmit the prepared package to the victim, often employing deceptive techniques like embedding a malicious link within a seemingly legitimate email. Phishing is the most common technique used during this stage; some other techniques include Watering Hole Attacks, access through Wi-Fi networks or physical access.

Once the weaponized payload is successfully delivered, the initial breach occurs when the attacker executes code on the victim's system in the **Exploitation** phase. The installation of a backdoor enables the attackers to maintain persistent access, even if the initial vulnerability that was exploited is patched. Some common examples of exploitation tools are RAT (Remote Access Trojans/Tools) & Cross Site Scripting.

The Installation, Command & Control and Actions on Objective phase of Cyber Kill Chain is explained with the help of MITRE ATT&CK tactics and techniques mentioned in its Enterprise Matrix. **Execution** encompasses methods that lead to the execution of code controlled by an adversary, either on a local or remote system. This tactic is frequently employed alongside initial access to execute code once access is gained, as well as during lateral movement to extend access to remote systems within a network. Methods include, Windows Management Instrumentations, Serverless Execution, User Execution, Using RunDll32, Service Execution etc.

Persistence refers to any method of accessing, manipulating, or modifying system configurations that allows an attacker to maintain a long-term presence within the targeted infrastructure. Adversaries frequently require a means to sustain access to systems even in the face of disruptions such as system restarts, credential loss, or other

failures that would necessitate the restart of a remote access tool or the utilization of an alternate backdoor in order to regain access through persistence. Persistence techniques include obtaining valid user accounts, installation of malicious browser extensions, boot or auto logon execution, Registry Run Key, Hooking.

Privilege Escalation: Once the code is executed, the adversary tries to gain further access in the target's infrastructure (systems or network) as some attack tools might require higher levels of privilege at various stages of an operation. Adversaries may initially gain access to a system with limited privileges and then exploit vulnerabilities in order to obtain local administrator level privileges. Additionally, an adversary may leverage a user account with administrator-like access. The escalation of privilege can also involve user accounts with permissions to access particular systems or perform specific functions that are crucial for adversaries to accomplish their objectives. Privilege escalation methods include Task Scheduling, Domain Policy Modification, Access Token Manipulation and Process Injection etc.

Defense Evasion comprises of tactics employed by an adversary to elude detection or bypass other defensive measures. Defense evasion is a collection of characteristics that the adversary incorporates throughout all stages of their operation. Some defense evasion techniques include Hiding artifacts associated with the cyber-attack, impairing victim defense mechanisms, process injection, packing, obfuscation.

Credential Access are methods used to gain access to system, domain or service credentials employed within an enterprise setting. Adversaries will often seek to acquire valid credentials from users or administrator profiles (such as local system administrators or domain users with administrative privileges) for use within the network. By doing so, adversaries can spoof the identity of the compromised profiles, obtaining all associated permissions on both the system and the network, which makes their detection more challenging for defenders. With significant access within a network, adversaries can also establish additional profiles for future use within the compromised infrastructure. Credential Access methods include OS Credentials Dumping, brute force, obtaining unsecured credentials, Input Capture etc.

Discovery involves tactics utilized by the adversary to gather information about the system and internal network. Upon gaining access to a new system, adversaries must familiarize themselves with the extent of their control and the advantages offered by

operating from that system, aligning with their current objectives or overarching intrusion goals. Discovery methods include Account Discovery, Application Window Discovery, Browser information Discovery & Cloud Infrastructure Discovery etc.

Lateral Movement encompasses methods that empower an attacker to infiltrate and exert control over remote systems within a network. It may or may not involve the execution of tools on those remote systems. These techniques enable adversaries to gather information from a system without requiring additional tools, such as a remote access tool, thus facilitating their progression across the network. Methods include Replication through removable media, internal Spearphishing, Lateral Tool Transfer etc.

Collection entails methods employed to identify and procure information, including classified files, from a targeted network before proceeding with data exfiltration. This category also encompasses the exploration of system or network locations where the adversary may search for data to extract. Collection methods include Audio, Video & Screen Capture, Adversary in the middle, etc.

At the **Command & Control** stage, the adversary establishes a communication channel that allows the attacker to control the compromised system remotely. Typical tactics used here are Data Obfuscation, Protocol Tunneling, Non-Standard Port, Multilayer Encryption etc.

In the **Actions on Objective** stage, the attackers proceed to execute their objectives remotely, which may involve taking control of the system or extracting sensitive data. Exfiltration methods include Exfiltration over Network Medium, Physical Medium, Web Service, Command & Control channel, Alternative Protocol etc.

4.4 NIST Cyber Security Framework

In 2013, NIST CSF was introduced subsequent to a directive from the US presidency and was updated in 2018. Currently, NIST is in the process of updating the CSF and NIST CSF version 2 is expected to be released in 2024. The primary goal of the framework was to develop effective strategies for safeguarding data and information against potential threats and breaches. The framework was designed to meet the specific data protection needs of the US government and other nations. Therefore, NIST CSF will be used as the frame of reference for our framework. As can be seen from the literature review, cyber-attacks on NC3 systems are generally APT based elaborate cyber ops, which need a high-

level strategy for risk management. Therefore, use of NIST CSF is recommended for use in the Pakistani NC3 system. The cyber security framework comprises of three parts, framework core, framework implementation tiers and framework profiles.

4.4.1 Framework Core

Framework core consists of five functions that are Identify, Detect, Protect, Respond and Recover with each function having its own categories, sub categories and informative references. These functions are activities that should be performed for achieving specific outcomes. This framework further provides some references in the form of controls that can be applied for achieving these outcomes. Application of every category or sub-category specified in the core framework is not necessary for a company. Each organization should implement these outcomes based on their own cybersecurity environment. The core framework structure as described in NIST CSF is shown in Figure 3. The goals that can be achieved from each activity or function are explained in Table 2.

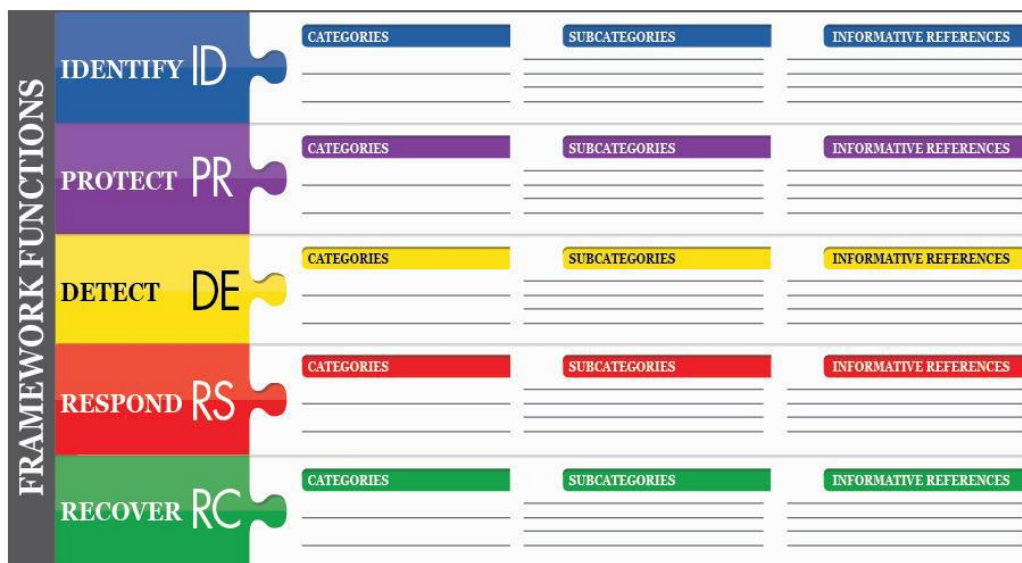


Figure 3 NIST CSF Core Functions

The purpose of each function, its goal and relevant outcome are shown in Table 2. It should be noted that NIST CSF does not mandate implementation of every category, it suggests including categories in the organizational security framework depending on the security environment of the organization.

Functions	Goal	Outcome Categories
Identify	Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.	<ul style="list-style-type: none"> a. Asset Management b. Business Environment c. Governance d. Risk Assessment e. Risk Management Strategy
Protect	Develop and implement appropriate safeguards to ensure delivery of critical services.	<ul style="list-style-type: none"> a. Identity Management and Access Control b. Awareness and Training; c. Data Security d. Information Protection Processes and Procedures e. Maintenance
Detect	Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.	<ul style="list-style-type: none"> a. Anomalies and Events b. Security Continuous Monitoring c. Detection Processes.
Respond	Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.	<ul style="list-style-type: none"> a. Response Planning b. Communications c. Analysis d. Mitigation Improvements
Recover	Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.	<ul style="list-style-type: none"> a. Recovery Planning b. Improvements c. Communications

Table 2 Functions of NIST Cyber Security Framework

4.4.2 Framework Implementation Tiers

This framework consists of four implementation tiers from Tier 1 to Tier 4, the former being the lowest and latter the highest in cyber security risk awareness and implementation. The organization is categorized in a specific tier depending on its current risk management practices, information sharing practices and legal requirements. Tier recommendation provides direction to the organization for management of cyber security risks, creation of Target profile and formulation of a realistic gap analysis. The purpose of Tier Selection is to assist organizations in highlighting the organizational zones, which are high priority and need additional resources. NIST CSF encourages organizations to move from a lower to higher tier, but it also recommends performing a cost-benefit

analysis prior to raising the implantation levels. Description for each Tier is shown in Table 3.

Processes	Tier 1	Tier 2	Tier 3	Tier 4
Risk Management	Not Formalized	Approved without an organization wide policy	Approved and expressed as policy	Adaptive process of Risk management
Integrated Risk Management Program	Limited awareness of cyber security program. Irregular implementation of risk management. Absence of cybersecurity mechanisms for information sharing.	Cyber security risk aware. No organization wide approach to manage cyber-security risks. Informal mechanism for information sharing. No reoccurring cyber risk assessment.	Organization wide approach to manage cyber security risks. Risk informed policies are implemented and reviewed. Continuous monitoring of cyber-security risk.	Cyber security risk dealt like other risks e.g., financial risk. Cyber security risk management is the part of organization's culture
External Participation	Organization does not understand its role in the larger eco system w.r.t to its dependents or dependencies. No information sharing or collaboration with other entities about threat intelligence and best practices. Unaware of cyber supply chain risks.	Organization understands its role in the larger eco system w.r.t to either its dependencies or dependents, but not both. The organization collaborates with and receives some information from other entities and generates some of its own info but does not share information. Aware of cyber supply chain risks but not consistent in risk mitigation	Organization understands its role, dependents and dependencies in the larger eco system and may contribute to community's broader understanding of risk. Collaborates with and receives information from other entities regularly and shares information with other entities. Aware of cyber supply chain risks and acts on those risks by mechanisms such as agreements to communicate baseline requirements.	Does continuous analysis of risk with the evolution of threat landscape. Information is shared internally and externally. Uses real time information to understand and act upon cyber supply chain risk.

Table 3 NIST CSF Implementation Tiers

4.4.3 Framework Profile

Profiling of an organization means the formulation of state of the organization based on outcome categories it has achieved. The current profile of an organization is the number of outcome categories it has achieved and the Target profile is the desired state of the organization. The comparison between the current profile and target profile of the organization gives a realistic gap analysis of the cyber security state of the organization.

4.4.4 Stepwise creation of Cyber Security Program

Prioritize and Scope

Clarity in the business mission or objective of the organization and the objective of framework implementation is very important for setting priorities for framework implementation. Moreover, scope definition i.e., departments, people, information systems on which this framework will be applied is also required as it will enable the organization to focus its efforts towards those specific entities.

Orient

Assets, systems, legal regularities and respective threats and vulnerabilities are identified.

Create a current profile

Current profile of the organization is created by noting the categories and subcategories of the framework core which have been implemented or partially implemented.

Conduct a risk assessment

A risk assessment is carried out considering the operational environment of the organization by identifying emerging risks and using cyber threat information. This risk assessment enables the organization to understand the likelihood of a vulnerability being exploited and the possible impact of that cyber security event on the organization.

Create a target profile

A desired state of organization is prepared in light of categories and sub categories of framework core. The organization chooses these categories and sub categories as per its scope and business mission.

Determine, analyze and prioritize gaps

The comparison between current profile and target profile provides a realistic analysis of gaps in the present cyber security state of the organization.

Implement action plan

The results from risk assessment, organization profiling and gap analysis can be used as input for identifying the Implementation Tier for the organization and selection of suitable categories, sub-categories and cyber security controls.

4.5 Proposed framework

The proposed framework will integrate some additional capabilities in NIST CSF. CSF provides a high-level approach to mitigate risks to an organization. Based on the framework core, it lists down functions such as asset management, their subcategories. It provides informative references from CIS, COBIT, ISO and NIST to implement controls relevant to the sub-categories. Similarly, in the tier implementation of the framework, CSF helps organizations to categorize themselves in a certain tier from T1, T2, T3 and T4. After profiling, CSF provides a stepwise procedure for implementation of the framework. However, it leaves the method adopted for risk assessment to specific organizations. It was discussed in the Components of NC3 systems that they contain many information systems, as new vulnerabilities keep arising by the day, the manual process of vulnerability analysis and risk assessment is a cumbersome process and difficult to keep up with. Therefore, it is recommended to automate the vulnerability assessment process while implementing CSF. Multiple risk assessment frameworks for cyber-security are available which can be categorized into CVSS (Common Vulnerability Scoring System) based frameworks, Extended CVSS based frameworks, Graph based frameworks and Game Theory based Frameworks [31]. [25] is CVSS based IoT vulnerability analysis framework called SAFER. This framework provides a mechanism for device & firmware identification, less invasive mechanisms like CCD based on TCP time stamps and Web Pattern Detection are used to identify the brand, model and firmware of devices in an organization. Both of these mechanisms independently identify devices. Subsequently, a fusion mechanism based on “subjective logic” is applied on the output of both methods to optimize the identification results. SAFER was implemented for identification of 572 devices out of which it identified 531 devices (92.55% accuracy). Individually, WPD achieved a result of 77 % correct identification, whereas after the

fusion process the correct identification process increased to 92.55%. This framework predicts CDSRI (Current Device Risk Indicator) i.e., the current vulnerability of the device and FDSRI (Future Device Risk Indicator). It is therefore recommended to integrate this vulnerability assessment framework in the NIST CSF for predicting current vulnerability analysis and prediction of future trends.

Secondly, it is recommended to add a cost benefit analysis of the organization for quantifying the right amount of security investment based on the expected and potential loss of information. Based on this cost-benefit analysis it can be determined whether an investment for moving to a higher implementation tier should be made or not. In this regard [32] proposes Gordon-Loeb model for cyber security investments. It is recommended to use this model in our framework for cost benefit analysis and a subsequent tier selection of our organization. The integration of automated vulnerability assessment and cost-benefit analysis is depicted in Figure 4.

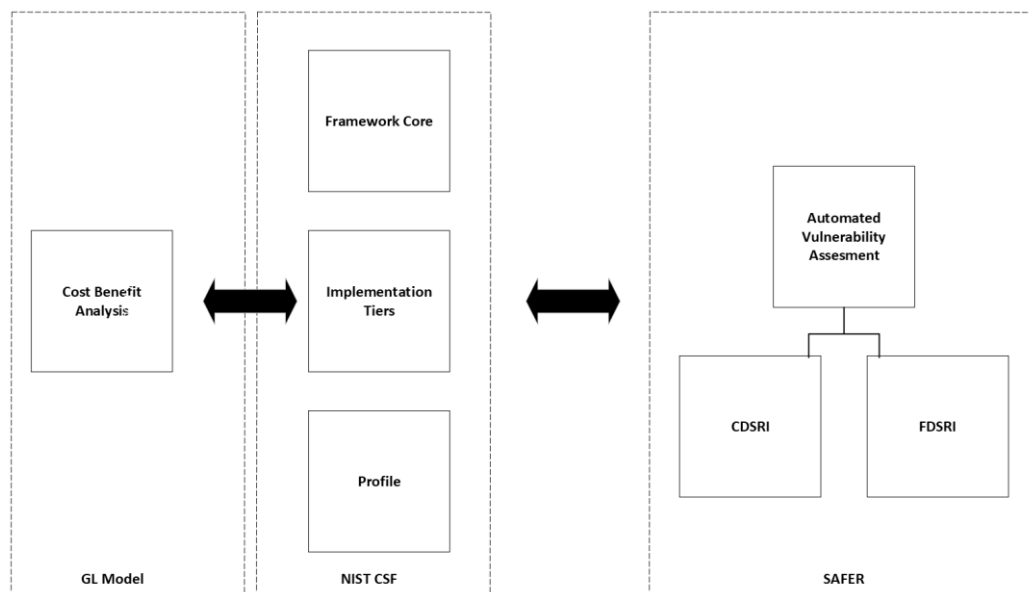


Figure 4 Integration of Cost Benefit Analysis and Automated Vulnerability Assessment in NIST CSF

4.6 SAFER Framework

SAFER (Security Assessment Framework for Embedded Device Risk) was developed by CERN for automated risk analysis of IoT devices. Considering the huge number of information systems involved in the NC3 systems, we should use SAFER for the risk assessment process. Steps involved for vulnerability assessment are depicted in Figure 5.

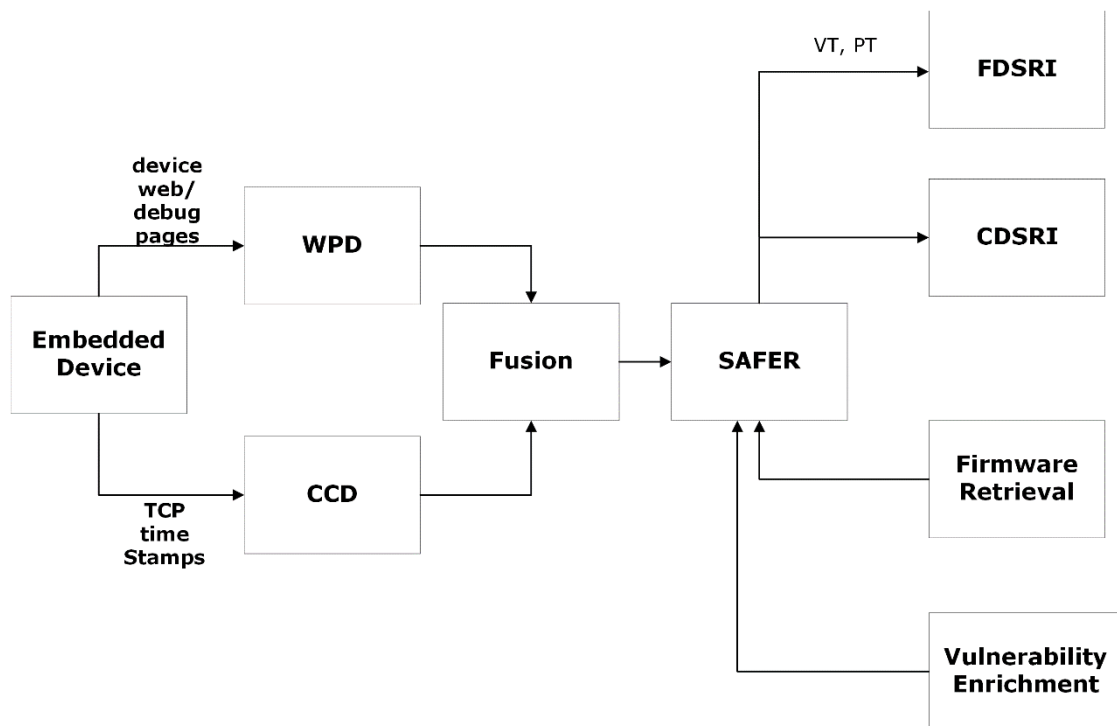


Figure 5 Overview of SAFER Framework

4.6.1 Device Identification

The device identification stage is divided into three parts. In the first phase, devices are identified through CCD (Clock Characteristics Detection), whereas WPD (Web Pattern Detection) is used in the second phase as a separate mechanism for device identification. The results from both methods are then combined through subjective logic to perform a data fusion which is the third phase of device identification.

CCD (Clock Characteristics Detection)

CCD examines the inner clock of an embedded information system over the network using information within IP packets. This information can be obtained with ease and scanning for it does not disturb the routine functions of the network as all networked information systems use TCP for their functionality. One scan of CCD provides 576 timestamps obtained in a span of forty-eight hours. The set of these time stamps are then fed to a machine learning algorithm which is trained to recognize known device models. Not going into the details of machine learning, random forest classifier matches the CCD data of the test device to a repository of previously identified models and outputs the likelihood of match. The devices with top three probabilities are retained for vulnerability analysis. Initially to train random forest on a larger data set, multiple CCD scans should be performed. Identification through CCD scanning is based on the assumption that clock

characteristics of IoT devices are very similar with minor variations. Information systems that are more complex than IoT devices have different OS and hardware characteristics where TCP timestamps can be used for clock-based fingerprinting.

Opinion Configuration for CCD

Equation 1 describes the probability of correctly identifying a device model in relation to probability of classifying all device models.

$$b(x) = \left(\frac{p(x).D + \frac{k}{2}}{D + k.n} \right) \quad (1)$$

$$U = 1 - \sum_{i=1}^n b_i \quad (2)$$

WPD (Web Pattern Detection)

Web Pattern Detection uses the information in the configuration page of devices to discern device model and firmware. The information patterns to look for in a web page are pre-defined during the setup of SAFER. WPD makes some http-based queries for information gathering. In the first step, the default page or user web page of the embedded device is accessed. The obtained pages then undergo analysis by pre-defined patterns to collect relevant data about the subject device. In case the information retrieved is limited, as if only manufacture's name could be resolved. WPD moves to the second query, which accesses http-based debug page of a manufacturer to retrieve the specific device model. WPD is based on the assumption that several IoT device models have similar firmware and subsequently similar user interface, hence enabling pattern identification. SAFER looks for the following hints in its web template detection. (i)String Patterns: WPD gathers text patterns (strings) from web pages which are related to a device model or device type. For instance, in the case of a telepresence system, strings such as "camera" or "encoder" would be detected in the string detection process. Web page's context for string detection is narrowed down using "XPath" for avoiding errors by random string detection. (ii)Embedded Libraries: Some devices include a variety of external libraries to enhance the functionality and design of web pages. Web Pattern Detection analyzes these libraries to help it specify the device model. (iii) Hashes of images: Most of the times, device manufactures embed useful textual information of devices within a picture on the device web page, WPD matches the hashes of these pictures to detect device model (iv) APIs: Some devices, such as IP based CCTV cameras provide applications that can scan

the network for their device. Network traffic for such an application was analyzed and a standard vulnerable API was found. WPD reads the model and firmware version directly by mimicking a network exploration through the use of this API.

Opinion Configuration for WPD:

Matching previously set patterns of WPD to a device's web page forms an opinion configuration. Under optimal conditions, the identification process will successfully determine device model, brand and firmware.

$$f_{w_{detected}} = \begin{cases} 0.0 & \text{Not Detected} \\ 0.4 & \text{Detected} \end{cases} \quad (3)$$

$$b(x) = \left(Amount_{TextPatterns} \cdot \frac{1}{6} + Amount_{hashes} \cdot 0.3 \right) + \left(Amount_{ConfigPatterns} \cdot \frac{1}{6} + Amount_{configPatterns} \cdot 0.1 \right) + f_{w_{detected}} \quad (4)$$

$$b(x) = \min\{b(x), 1.0\} \quad (5)$$

Equation (4) is the belief equation. The weight of hashes is set to 0.3 due to the observation developed by SAFER that text images within hashes rarely matched the actual text patterns. In other words, the first part of equation 3 depicts that amount of belief in matching from text patterns is twice as compared to matching with hashes. $Amount_{TextPatterns}$ and $Amount_{ConfigPatterns}$ are multiplied by 1/6 as SAFER limits WPD to detect not more that 6 patterns in web pages. It is argued that if WPD matches a web pattern on a configuration page, considering the detailed technical or administrative information of the device it can be safely assumed that this detection is correct. This confidence in pattern detection through configuration pages is shown in the second part of equation (2) where $Amount_{configPatterns} \cdot 0.1$ is again added.

Fusion Process

Opinion Configurations of CCD and WPD are fed as input to the fusion process using subjective logic operator CBF (Common Belief Function). This operator allocates a belief level to each device that has been identified, resulting in the generation of a ranked list of the probable candidates for device models.

4.6.2 Firmware & Vulnerability Analysis

SAFER automates the risk assessment process by obtaining firmware images from vendor websites, carrying out an automated firmware analysis and finally deducing

vulnerabilities of the device model and firmware contained software. SAFER then computes existing and future risk faced by a device based on this information.

There is no central public repository for *firmware image retrievals*. SAFER has developed its own repository which now consists of 825 firmware images of various device models. This repository has been developed by SAFER by gathering unprocessed firmware from official manufacturer websites. After a specific firmware is retrieved, it is then decompressed or unpacked using FACT (Firmware Analysis & Comparison Tool). Additional third-party software detection capabilities have been added to FACT. 16 YARA rules are applied on the firmware for software library identification. There is no public information on which YARA rules to apply for software library identification. SAFER therefore, manually analyzed the firmware for software libraries and specified these 16 rules based on their experience. To develop a firmware repository for NC3 infrastructure of Pakistan, it is suggested to contractually bind the vendors to provide firmware of purchased devices for subsequent analysis and vulnerability enrichment.

Publicly available *vulnerabilities of the software libraries* are then collected by SAFER. CVE-Search, a publicly available solution is used in this regard, which automatically retrieves known vulnerabilities of all software libraries. All vulnerabilities for identified firmware and software libraries are collected. It offers a dedicated repository for vulnerabilities by fetching CVE information from reputable external databases like NVD (National Vulnerability Database), NIST.

Vulnerabilities of device models are publicly listed on MITRE. SAFER retrieves these vulnerabilities through CPE (Common Platform Enumeration) queries on its local database.

Additionally, SAFER identifies the *vulnerabilities of decompressed firmware*. SAFER's firmware module comprises of a binary plugin which uses simple text search to detect pre-defined passwords and sensitive cryptographic keys. Attackers can acquire the firmware and use these cryptographic keys to infiltrate devices of similar model.

4.6.3 Risk Metrics

Two Risk metrics are calculated, one for Current Risk that is associated with the present use of device, known as CDSRI (Current Device Security Risk Indicator). The second metric known as FDSRI (Future Device Security Risk Indicator) predicts the possibility of a presently safe device turning into a risky device in the future or vice versa.

CDSRI (Current Device Security Risk Indicator)

For the calculation of CDSRI, SAFER takes into account all CVSS values of unpatched vulnerability. CVSS 3.0 is used for this purpose and the vulnerabilities are classified as per equation 6.

$$\left\{ \begin{array}{l} \text{None} \\ \text{Low} \\ \text{Medium} \\ \text{High} \\ \text{Critical} \end{array} \right. \begin{array}{l} \max_{CVSS} = 0 \\ 0.1 \leq \max_{CVSS} \leq 3.9 \\ 4 \leq \max_{CVSS} \leq 6.9 \\ 7 \leq \max_{CVSS} \leq 8.9 \\ 9 \leq \max_{CVSS} \leq 10 \end{array} \quad (6)$$

FDSRI (Future Device Security Risk Indicator)

FDSRI is calculated using two prediction variables known as VT (Vulnerability Trend) & PT (Patch Trend). VT is dependent on occurrence frequency of vulnerabilities and potential severity of these vulnerabilities. SAFER has applied various forecasting models on VT data and it deduces that ARIMA model (Auto Regression Integrated Moving Average) is the best option for VT prediction. ARIMA predicts future vulnerabilities v_{future} based on past CVSS vulnerabilities score v_{past} .

$$X^{vulnerabilities} = v_{past} \cup v_{future} \quad (7)$$

$$vt_{CVSS} = median(X^{vulnerabilities}) \quad (8)$$

$$V_t = \left\{ \begin{array}{l} \text{Low} \\ \text{Medium} \\ \text{High} \end{array} \right. \begin{array}{l} 0 \leq \max_{CVSS} \leq 3.9 \\ 4 \leq \max_{CVSS} \leq 6.9 \\ 7 \leq \max_{CVSS} \leq 10 \end{array} \quad (9)$$

Vulnerability thresholds from CVSS 2.0 are used in equation 9 for simplicity purpose. In order to select the prediction model out of ARIMA, Simple Moving Average and Facebook Prophet, the MAD (Mean Absolute Deviation) of the three models was calculated. For this purpose, data set O was divided into O_{test} & O_{train} . Each model was first trained on O_{train} , based on it these models predicted \hat{Y} . These \hat{Y} were then compared with O_{test} to calculate MAD for each model. MAD is defined in equation 11.

$$x_i = |o_i - \hat{y}_i| \quad \text{where } \hat{y}_i \in \hat{Y}_i \text{ \& } o_i \in O_i \quad (10)$$

$$MAD = median(|x_i - \tilde{X}|) \quad \text{where } x_i \in X \quad (11)$$

Where $X = U \{x_i\}$ and $\tilde{X} = \text{median}(X)$.

Based on the training data it was found that median deviation for ARIMA model was the lowest. Considering the small variation in CVSS value (0-10) it was decided that ARIMA model is the best choice for VT prediction.

The second metric PT takes into account the official release time of a vulnerability and at what point of time was this vulnerability patched by the vendor, based on which a time interval in which a vendor will patch future vulnerabilities is predicted. Creation date of CVEs is extracted from CVE identifiers in firmware images and included libraries. This information is then compared with the release notes of the manufactures to determine the date the respective vulnerability was patched. SAFER considers a vulnerability is patched if one of two conditions is met (i) A software version not exposed to the identified vulnerability is used by the manufacturer (ii) Entire software is removed. Some manufacturers do not list patched vulnerabilities in their release notes, in that case, SAFER retrieves vulnerabilities of all firmware versions and software libraries of the detected device. Subsequently, an analysis of successive firmware images is conducted by SAFER to look for version modification in the vulnerable library. The absence of a vulnerable library in the subsequent firmware version is considered an indication by SAFER that the vulnerability has been patched. In case of re-appearance of a newer version of vulnerable library software in a future firmware image, SAFER will again check for vulnerability patching in the subsequent firmware image. Based on the past patching time intervals known as pt_{past} SAFER uses the Facebook Prophet model to forecast future patch intervals known as pt_{future} . The set of all past and future patch intervals is therefore $X^{patch\ time\ spans}$ as shown in equation 12. The median of all these patch intervals is pt_{median} (eq 13) and the Patch Trend (PT) is classified in equation 14. c3, c2 and c3 are classifications given to the attackers by the SAFER framework i.e. c1 are security professionals, c2 are advanced security experts and c3 are script kiddies. As per a study conducted by RAND Corporation [33], security professionals need 22 days to formulate an exploit once a vulnerability is released publicly. For calculating time required by script kiddies to exploit a vulnerability, the time interval from vulnerability release to upload of an exploit code on Metasploit was determined. It was observed that script kiddies take a median time of 414 days to exploit a vulnerability subsequent to its public release.

$$X^{patch\ time\ spans} = pt_{past} \cup pt_{future} \quad (12)$$

$$pt_{median} = median(X^{patch\ time\ spans}) \quad (13)$$

$$Patch\ trend = \begin{cases} Fast & 0 \leq pt_{median} \leq c1 \\ Medium & c1 \leq pt_{median} \leq c3 \\ Slow & pt_{median} \geq c3 \end{cases} \quad (14)$$

Based on the Patch Trend and Vulnerability Trend values, this framework now calculates the FDSRI. In this regard a risk matrix is formed which contains pt and vt.

		Patch Trend		
Vulnerability		Fast	Medium	Slow
Trend	Low	Low	Low	Medium
	Medium	Low	Medium	High
	High	Medium	High	Critical

Table 4 FDSRI Risk Matrix

Table 4 shows that a device with medium patching trends and low vulnerability trends has a low FDSRI. The basis of this argument is that the device will be exposed to c2 (advanced security experts) as per the patching trend, but the low vt means that the attack surface for the attacker will be low risk vulnerabilities. Hence, an organization is at a low risk, same is implied as low FDSRI. The worst-case scenario is described in Table 4 where high-risk vulnerabilities combined with slow patching intervals indicate a critical FDSRI. In other words, there are chances that a high-risk vulnerability will be exposed for a very long time due to slow patching intervals giving ample amount of time to even script kiddies.

Type	CDSRI	Models	VT	Models	PT	Models	FDSRI	Models
CCTV	Low	4	Low	4	Slow	0	Low	4
	Medium	0	Medium	0	Medium	0	Medium	0
	High	0	High	0	Fast	4	High	0
	Critical	0					Critical	0
IP-2-X	Low	1	Low	2	Slow	0	Low	2
	Medium	0	Medium	0	Medium	0	Medium	0
	High	0	High	0	Fast	2	High	0
	Critical	1					Critical	0
IPMI	Low	4	Low	8	Slow	0	Low	8
	Medium	0	Medium	0	Medium	0	Medium	0
	High	0	High	0	Fast	8	High	0
	Critical	4					Critical	0
NAS	Low	3	Low	3	Slow	0	Low	3
	Medium	0	Medium	0	Medium	0	Medium	0
	High	0	High	0	Fast	3	High	0
	Critical	0					Critical	0
Printer	Low	3	Low	15	Slow	0	Low	15
	Medium	0	Medium	0	Medium	15	Medium	0
	High	0	High	0	Fast	0	High	0
	Critical	12					Critical	0
Telepresence	Low	2	Low	4	Slow	0	Low	6
	Medium	0	Medium	2	Medium	1	Medium	0
	High	0	High	0	Fast	5	High	0
	Critical	4					Critical	0

Figure 6 Assessed Devices of CERN by SAFER

Figure 6 depicts the results generated by implementation of SAFER framework by [25] for evaluation purposes. It shows that SAFER was able to predict existing and future risk of 38 IoT device models, which amount to 240 physical IoT devices. The figure shows that 21 out of 38 device models have a critical CDSRI.

4.7 Cost Benefit Analysis based on Gordon Loeb Model

NIST Cyber Security Framework [21] provides implementation Tiers for organizations in order to support decision making processes for risk management and setting the priorities of the organization. It encourages the organization to move from a lower Tier to a higher Tier but for doing so, it advises the organization to conduct a cost-benefit analysis i.e. analysis regarding the cost of risk reduction as compared to the benefits achieved from the risk reduction. However, it does not specify any methodology for the implementation of this analysis. It is therefore recommended to integrate Gordon Loeb Model [32] in the NIST CSF Implementation Tiers for cost-benefit analysis.

Expected benefits $EBC(z)$ from an investment 'z' is shown in equation 15 where 'L is the potential monetary loss or value associated to an information', $s(z, v)$ is the security breach function which represents reduction in vulnerability after an investment 'z' and

v is the vulnerability of an information system over a period of one year. The GL model states that the benefits incurred in risk reduction due to additional investments increase at a decreasing rate. $ENBC(z)$ is the expected net benefit of an investment z as shown in equation 16. The optimal level of investment $z^*(v)$ for a vulnerability v is presented by GL method in equation 17.

$$EBC(z) = [v - s(z, v)]L \quad (15)$$

$$ENBC(z) = [v - s(z, v)]L - z \quad (16)$$

$$z^*(v) \leq \left(\frac{1}{e}\right)vL \quad (17)$$

As the value of e is 2.7182, GL method states in equation 16 that optimal investment for risk reduction should be less than or equal to 37 % of the expected loss vL . The same phenomenon is depicted in Figure 7 below.

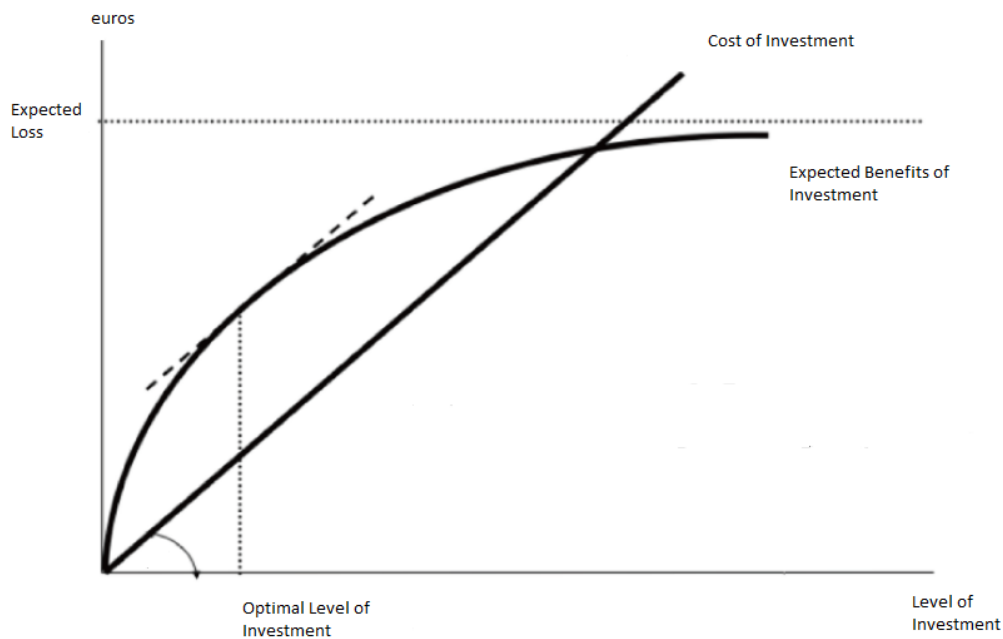


Figure 7 Gordon Loeb Model

Implementation of GL method for cost analysis is divided in 4 steps. (i) Estimating value of information being protected (ii) Estimate the probability that a vulnerability v will be exploited. (iii) Combine the first two steps for deriving expected loss. (iv) Allocate investments to the information to be protected on the basis of cost-benefit analysis.

For moving from one tier to the next tier, the GL model proposes that an organization should only move from a lower tier to a higher tier if benefit from the reduction in loss is greater than the investment required to move from lower tier to higher tier. The same is shown in equation 18 below where $z_{T_{i+1}}$ is the investment required to move to higher tier T_{i+1} .

$$\left[s(z_{T_i}, v) - s(z_{T_{i+1}}, v) \right] L \geq z_{T_{i+1}} - z_{T_i} \quad (18)$$

Implementation of this economic model therefore can provide direction to our organization whether to invest in the tier improvement process or not. However, it was discussed in equation 17 that optimal investment $z^*(v)$ is 37 percent of the expected loss. If an organization has already invested $z^*(v)$ it means it has achieved the optimal NIST tier $T(z^*)$. Therefore, to move to higher CSF implementation tier, equation 18 is amended as follows.

$$\left[s(z^*, v) - s(z_{T+(z^*)}, v) \right] L + B \geq z_{T+(z^*)} - z^* \quad (19)$$

Equation 19 above means that an organization which is at the optimal tier level will need some additional incentive B in addition to benefit in cost reduction because it was discussed earlier that risk reduction increases at a decreasing rate. Therefore, an additional incentive in the form of business profit is added in equation 19. It should be noted that we are integrating this method to the NC3 system of Pakistan for which monetary benefit is not a concern. However, B can also be termed as the saving incurred due to loss reduction. For example, nuclear states such as Pakistan have invested heavily in their NC3 systems; a cyber-attack which consequently results in the destruction of an NC3 component such as Natanz facility Iran would have a financial impact on the state in addition to affecting its deterrence capability. Therefore, this B can be treated as benefits from cost saving in case of a cyber-attack.

Conclusion & Future Work

This research conducted a detailed study of nuclear posture, doctrine, and NC3 System (Nuclear Command Control & Communication). Hypothetical scenarios and real-time historic events were studied to understand the risk of nuclear escalation in case of a cyber-attack on the NC3 systems of states. It was observed that the nature of cyber-attacks contrasts with the strategic operations of NC3. Nuclear states tend to show off their nuclear capabilities to deter the adversary from a misadventure. On the contrary, cyber operations are covert in nature, as the success of the cyber operation is dependent on stealth. Therefore, when a cyber-operation is conducted on an NC3 system, the target state cannot assess the cyber-attack's severity, intention, and source. This is considered the major cause for nuclear escalation in a cyber-attack. Secondly, it was observed that modern cyber-security attacks are sophisticated attacks, as shown through the study of the Cyber Kill Chain and ATT&CK Enterprise attack matrix. Therefore, it was proposed that a Cyber Security Framework for risk mitigation should be based on NIST Cyber Security Framework, which provides guidelines and best practices for organizations to improve their security postures. We discussed in Components of NC3 that a typical NC3 system has various components, and each component has various information systems. We inferred from this that there would be many embedded devices in the NC3 system, and vulnerability assessment for each device is cumbersome and a task too difficult to keep up with because of the high frequency of new vulnerabilities. As a result, it was proposed to integrate an automated vulnerability assessment component into our framework. SAFER Framework was considered the most suitable vulnerability analysis framework for the following reasons (i) This framework achieves high device identification accuracy by combining results from two different methods for identification (ii) Not limited to detecting vulnerabilities for specific programming languages, closed source software, and large code base. The SAFER framework will output the CDSRI (Current Device Security Risk Indicator) and FDSRI (Future Device Security Risk Indicator) level of a device i.e. the existing risk linked with using an embedded device and the future risk of using the device. It was further recommended that procurement rules for buying off-the-shelf equipment from vendors should contractually

bind the vendors to provide requisite firmware along with the required equipment. It was found that countries tend to invest more in their cyber-security programs than what is required to minimize the attack surface. For this purpose, the GL (Gordon-Loeb) method is proposed to assist the Pakistani state in its investment activities in the cyber-security sector. This method will help the organizations to do a cost-benefit analysis and quantify an optimum amount of investment to minimize their expected loss. It also suggests a criterion through which companies can decide whether to move to a higher Tier of NIST CSF. Two takeaways from the integration of GL methods in NIST CSF are that increased investments in security provide additional benefits to the organization in the form of a reduction in potential loss. However, after a certain point, the increase in this benefit is either diminishing or there is no additional benefit. Secondly, the optimal investment in security should be at most 37 % of the expected loss value.

There are certain limitations in this research work. First, NC3 systems of states are classified systems; therefore, accurate information about the types of information systems being used could not be formulated. However, we have specified some components of the NC3 systems through which typical information systems used in a typical NC3 infrastructure can be visualized. The SAFER framework, which is proposed to be integrated into NIST CSF, provides current and future vulnerability predictions of embedded devices based on publicly available vulnerabilities. However, non-IoT devices like Workstations or Servers, which have more complex Operating Systems, cannot be assessed using this framework. Secondly, the GL model describes the optimal investment as 37 % of expected loss, it does not provide a method to quantify the expected loss. This can be a good direction for future work in cost benefit analysis of security systems, to derive a methodology for quantification of expected and potential losses in a security system.

References

- [1] W. A. Owens, K. W. Dam, and H. S. Lin, *Technology, policy, law, and ethics regarding U.S. acquisition and use of cyberattack capabilities*. National Academies Press, 2009. doi: 10.17226/12651.
- [2] P. M. Lewis, H. (Research F. in nuclear weapons policy) Williams, B. Pélopidas, and S. Aghlani, *Too close for comfort : cases of near nuclear use and options for policy*.
- [3] M. Kamiński, “Operation ‘Olympic Games.’ Cyber-sabotage as a tool of American intelligence aimed at counteracting the development of Iran’s nuclear programme,” *Security and Defence Quarterly*, vol. 29, no. 2, pp. 63–71, Jun. 2020, doi: 10.35467/sdq/121974.
- [4] U.S. Joint Chiefs of Staff. “A Historical Study of Strategic Connectivity, 1950-1981.” Special Historical Study Washington, DC: Joint Chiefs of Staff, Joint Secretariat, Historical Division, July 1982.
- [5] S. Egeli, “Space-to-Space Warfare and Proximity Operations: The Impact on Nuclear Command, Control, and Communications and Strategic Stability,” *Journal for Peace and Nuclear Disarmament*, vol. 4, no. 1, pp. 116–140, 2021, doi: 10.1080/25751654.2021.1942681.
- [6] W. Wilfred, K. Andraz, and K. Eleanor, “The Cyber-Nuclear Nexus: Interactions and Risks,” Nov. 2021. doi: 10.37559/WMD/21/NRR/03.
- [7] A. E. Levite *et al.*, “China-U.S. Cyber-Nuclear C3 Stability,” 2021. Carnegie Endowment for Peace.
- [8] Office of the Deputy Assistant Secretary of Defense for Nuclear Matters. “Nuclear Command and Control System.” *Nuclear Matters Handbook*, pp.14-15, 2020.
- [9] A. Alshamrani, S. Myneni, A. Chowdhary, and D. Huang, “A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities,” *IEEE Communications Surveys and Tutorials*, vol. 21, no. 2, pp. 1851–1877, Apr. 2019, doi: 10.1109/COMST.2019.2891891.
- [10] J. Martínez and J. M. Durán, “Software supply chain attacks, a threat to global cybersecurity: SolarWinds’ case study,” *International Journal of Safety and*

Security Engineering, vol. 11, no. 5, pp. 537–545, Oct. 2021, doi: 10.18280/IJSSE.110505.

- [11] "Analysis of the cyber attack on the Ukrainian power grid." Electricity Information Sharing and Analysis Center (E-ISAC) 388, 2016: 1-29.
- [12] S. Cunningham, "Nuclear Command, Control, and Communications Systems of The People's Republic of China," *Tech4GS Special Reports*, 2019. [Online]. Available: <https://www.tech4gs.org/nc3-systems-and-strategic-stability-a-global-overview.html>
- [13] L. Ryabikhin, "Russia;s NC3 and Early Warning Systems", *NAPSNet Special Reports*, 2019. [Online]. Available: <https://nautilus.org/napsnet/napsnet-special-reports/russias-nc3-and-early-warning-systems/>
- [14] Y. Afina, B. Unal, and | Chatham House, "Ensuring Cyber Resilience in NATO's Command, Control and Communication Systems," 2020.
- [15] F. H. Khan, "Nuclear Command, Control and Communications (NC3): The Case of Pakistan," *Tech4GS Special Reports*, September 26, 2019, [Online]. Available:<https://www.tech4gs.org/nc3-systems-and-strategic-stability-a-globaloverview.html>
- [16] H. M. Kristensen and M. Korda, "Pakistani nuclear weapons, 2021," *Bulletin of the Atomic Scientists*, vol. 77, no. 5, pp. 265–278, 2021, doi: 10.1080/00963402.2021.1964258.
- [17] CNSS, "Policy on Information Assurance Risk Management for National Security Systems," 2012. [Online]. Available: <http://www.cnss.gov>.
- [18] Majlis-eShura (Parliament)"BILL to make provisions for prevention of electronic crimes." 2016
- [19] "Government of Pakistan National Cyber Security Policy 2021."
- [20] J. R. Lindsay, "Cyber Operations and Nuclear Weapons *NAPSNet Special Reports*, 2019,"[Online]. Available: <https://nautilus.org/napsnet/napsnet-special-reports/cyber-operations-and-nuclear-weapons/>

- [21] “Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1,” Gaithersburg, MD, Apr. 2018. doi: 10.6028/NIST.CSWP.04162018.
- [22] “Risk management framework for information systems and organizations:,” Gaithersburg, MD, Dec. 2018. doi: 10.6028/NIST.SP.800-37r2.
- [23] “Security and Privacy Controls for Information Systems and Organizations,” Gaithersburg, MD, Sep. 2020. doi: 10.6028/NIST.SP.800-53r5.
- [24] “Assessing Security and Privacy Controls in Information Systems and Organizations,” Gaithersburg, MD, Jan. 2022. doi: 10.6028/NIST.SP.800-53Ar5.
- [25] P. Oser, R. W. Van Der Heijden, S. Lüders, and F. Kargl, “Risk Prediction of IoT Devices Based on Vulnerability Analysis,” *ACM Transactions on Privacy and Security*, vol. 25, no. 2, May 2022, doi: 10.1145/3510360.
- [26] P. Oser, F. Engelmann, S. Lüders, and F. Kargl, “Evaluating the Future Device Security Risk Indicator for Hundreds of IoT Devices,” In: *Lenzini, G., Meng, W. (eds) Security and Trust Management. STM 2022. Lecture Notes in Computer Science*, vol 13867. Springer, Cham. https://doi.org/10.1007/978-3-031-29504-1_3 Sep. 2022, [Online]. Available: <http://arxiv.org/abs/2209.03826>
- [27] S. Chakraborty, R. Krishna, Y. Ding and B. Ray, "Deep Learning Based Vulnerability Detection: Are We There Yet?," in *IEEE Transactions on Software Engineering*, vol. 48, no. 9, pp. 3280-3296, 1 Sept. 2022, doi: 10.1109/TSE.2021.3087402
- [28] M. Jimenez, M. Papadakis, and Y. Le Traon, “Vulnerability prediction models: A case study on the Linux Kernel,” in *Proceedings - 2016 IEEE 16th International Working Conference on Source Code Analysis and Manipulation, SCAM 2016*, Institute of Electrical and Electronics Engineers Inc., Dec. 2016, pp. 1–10. doi: 10.1109/SCAM.2016.15.
- [29] “THE ECONOMICS OF CYBERSECURITY: A PRACTICAL FRAMEWORK FOR CYBERSECURITY INVESTMENT,” 2013.
- [30] “S. D. Applegate, "The principle of maneuver in cyber operations," 2012 4th International Conference on Cyber Conflict (CYCON 2012), Tallinn, Estonia, 2012, pp. 1-13.”

- [31] S. A. Baho and J. Abawajy, “Analysis of Consumer IoT Device Vulnerability Quantification Frameworks,” *Electronics (Switzerland)*, vol. 12, no. 5, Mar. 2023, doi: 10.3390/electronics12051176.
- [32] L. A. Gordon, M. P. Loeb, and L. Zhou, “Integrating cost-benefit analysis into the NIST cybersecurity framework via the gordon-loeb model,” *J Cybersecur*, vol. 6, no. 1, 2020, doi: 10.1093/CYBSEC/TYAA005.
- [33] L. Ablon, A. Bogart, and Institute for Civil Justice (U.S.), *Zero days, thousands of nights : the life and times of zero-day vulnerabilities and their exploits*.