Gap Analysis of Cyber Security Framework and Practices in Military

Kamal Thapa[1], Dr Pramod Parajuli[2]

[1]PG Scholar, Lord Buddha Education Foundation, Kathmandu, Nepal
[2] PGD Manager, Lord Buddha Education Foundation, Kathmandu, Nepal

Abstract

The effectiveness of gap analysis in cyber security frameworks, particularly in military contexts is focused on strengthening governance, risk mitigation, resilience improvement, and early threat detection in enhancing cyber security practices within military operations. It emphasizes the role of robust governance structures, policies, and procedures in establishing a solid foundation for effective cyber security measures. Addressing identified gaps through framework analysis enables proactive risk mitigation and resilience building, crucial for adapting to evolving cyber threats. Additionally, strategic planning based on current capabilities enhances preparedness, while training perspectives and resource allocation play pivotal roles in swiftly identifying and containing cyber threats. The significance of a comprehensive and proactive approach to cyber security within military operations to mitigate threats and enhance overall resilience provides the organizations to adapt and respond effectively to evolving threats.

Keywords: *Cyber Security, Cyber Operations, NIST Framework, Vulnerabilities, Cyber Threats, Military Cyber Security, Cyberspace, Technological Advancement, Cyberwarfare, Cyber Incident, Risk Assessment.*

1. Introduction

In the contemporary landscape of military operations, cybersecurity has emerged as an indispensable component, crucial for upholding national security and preserving the integrity of defense systems. The interconnected nature of the modern world has ushered in unprecedented challenges in cyberspace, ranging from state-sponsored cyber-espionage to intricate cyber-attacks, expanding the scope of warfare beyond conventional boundaries. As advanced technologies like artificial intelligence, the Internet of Things (IoT), and cloud computing are integrated into military operations, they enhance capabilities while concurrently amplifying vulnerabilities to cyber threats. Adversaries, including hostile nation-states and non-state actors, exploit these vulnerabilities to infiltrate military networks, disrupt communications, and compromise critical infrastructure. Recognizing the gravity of these threats, nations worldwide have prioritized the development of robust cyber defense strategies to safeguard their interests in the digital age, highlighting the imperative for a comprehensive and adaptive approach to cybersecurity within the military domain.

The rapid evolution of new cyber threats poses a challenge to counteracting attacks on information systems. Fragmented ownership and regulatory control of Information and Communication Technology (ICT) infrastructure present a major global challenge in cybersecurity efforts (Scott J. Shackelford, 2015).

2. Problem Statement

Continuous technological advancement poses significant challenges in the military domain, particularly regarding cybersecurity and vulnerabilities. Defining the problem is essential, involving a thorough examination of underlying causes and relevant actors' inclinations and capabilities. Pinpointing relationships and interactions among these actors clarifies how operational variables may hinder or enable technological transformation. The problem statement guides strategic leveraging of

cyber operational environment inertia to address critical issues in the cyber threat landscape. In the face of a constantly changing, intricate, and unpredictable global cyber security landscape marked by contested norms in cyberspace and ongoing disorder, the military encounters persistent challenges in executing Cyber Operations (CO) and other military operations (Muhammer Karaman, 2016). The cybersecurity landscape is currently fragmented, with varying effectiveness across different frameworks, leading to challenges for organizations in securing their systems and data. To overcome these obstacles, there's a pressing need for a more cohesive and comprehensive approach to cybersecurity. A unified framework that encompasses best practices, standards, and adaptable strategies can provide organizations with a standardized and robust foundation to enhance their cybersecurity posture (Smith, 2019).

The military's cyber security landscape grapples with challenges including fragmented framework integration, uncertain training effectiveness, vulnerability exploitation risks, and insufficient incident response capabilities. Addressing these issues is crucial for fortifying cyber defense and ensuring resilience against evolving threats.

3. Research Questions

The rise of cyber threats has paved the way for a reevaluation of security paradigms. Given the intricacies of the cybersecurity landscape, a nuanced analysis becomes imperative. Hence, its focus to explore the military's contribution to national cybersecurity, acknowledging the complexity of the subject. The central inquiry revolves around unraveling various facets of the military's involvement in this crucial domain (ZUKIC, 2020).

On this basis, the following research questions are generated for overarching goal to contribute valuable insights into optimizing the integration of cyber security measures within military operations, ultimately fortifying national defense against contemporary and emerging cyber threats.

RQ1. How effectively are existing cyber security frameworks integrated within the military structure, and what gaps exist in this integration process?

The following supporting questions are generated for the clear views and ideas for the overall cyber security framework and gap analysis within the military practices.

RQ2. How current military cyber security frameworks address the evolving and sophisticated nature of cyber threats with the identification of key vulnerabilities within the military's cyber security practices, and how can they be exploited by potential adversaries?

RQ3. How adequate are the training programs provided to military personnel in preparing them to identify, prevent, and respond to cyber threats?

RQ4. In what ways does the military demonstrate adaptability to the rapidly evolving cyber threat landscape, and what adjustments are needed in current frameworks to enhance this adaptability?

RQ5. How well are cutting-edge cyber security technologies integrated into military systems, and what challenges exist in the practical implementation of these technologies?

RQ6. To what extent do current military cyber security practices comply with established standards and regulations, and what gaps exist in achieving compliance?

4. Objective of the Research

Research aims to provide a structured approach to addressing the specified research questions, guiding the investigation into the gap analysis of cyber security framework and practice in the military.

5. Significance

Understanding the integration and effectiveness of cybersecurity frameworks in the military is relevant due to the increasing digitization of military operations. Cyber threats can compromise national security, making it crucial to assess the efficacy of existing frameworks in safeguarding sensitive information (UK Ministry of Defence, 2022). With continuous technological advancements, staying relevant in cybersecurity practices is essential. Assessing the alignment of military cybersecurity with evolving technologies ensures that defense systems remain robust and adaptive in the face of emerging threats (Masterson, 2019). In an era of global interconnectedness, the relevance of military cybersecurity extends beyond national borders. Evaluating the integration of frameworks becomes crucial for international collaborations and maintaining the cybersecurity integrity of alliances (Rane, 2023).

The significance of cybersecurity in the military lies in its direct impact on national security. Cyberattacks can disrupt military operations, compromise classified information, and potentially lead to strategic vulnerabilities (The White House, Washington, 2023). Strategic Decision-Making: Effective cybersecurity frameworks enable secure data-driven decision-making within military structures. Significantly, a well-protected information environment ensures the integrity of strategic plans and enhances the military's overall operational efficiency. Public Trust: Military operations often involve public trust and confidence. The significance of cybersecurity in this context is paramount as breaches can erode trust, impact public perception, and compromise the credibility of military institutions. Global Stability: Given the interconnected nature of global affairs, the significance of military cybersecurity extends to contributing to global stability. Ensuring the resilience of military systems contributes to a secure international environment, fostering cooperation among nations.

6. Literature Review

Cyberspace serves as a crucial domain for national and international security, trade, and public activities, encompassing diverse ICT infrastructure. Despite its essential role, the continuous evolution of cyberspace introduces new risks from various state and non-state actors, posing threats to individuals, businesses, and national infrastructure. Cybersecurity efforts span government strategies, institutional adherence to standards, and individual vigilance, with a focus on preventing disruptive cyber activities and ensuring public safety and national security (Muhammer Karaman H. C., 2016).

In modern military operations, particularly concerning the Indian Armed Forces' cyber preparedness emphasizes the level of significance in the new arena of warfare. With technological advancements, cyber tactics exploiting vulnerabilities have become integral to warfare, ushering in a new arena of conflict. The integration of the Internet of Military Things (IoMT) into military operations enhances battlefield readiness but also poses significant cybersecurity challenges due to interconnected nodal points vulnerable to cyberattacks. The Indian Military and government recognize the importance of IoMT, employing technologies like drones for surveillance and defensive/offensive missions to address evolving threats in cyberspace (Poornima, 2023).

The UK Ministry of Defence's "Cyber Primer" underscores the critical role of cyberspace in national security and military operations. It defines cyberspace as a domain with unique characteristics, enabling instantaneous and global actions with anonymity. Unlike physical domains, cyberspace operates without environmental constraints or limitations on time and resources. The primer categorizes cyberspace into six interconnected layers and three effect dimensions, highlighting its complexity and significance in contemporary warfare (Ministry of Defense , 2022).

Cyberspace encompasses physical assets and human operators vital to military operations beyond just the internet and IT systems. The Department of Defense defines it as a global domain within the

information environment, comprising interconnected networks and resident data, equating its importance to conventional domains. Military-relevant cyberspace activities include intelligence, information, crime, and military operations, requiring equal attention from military leaders (G. Alexander Crowther, 2018).

Cyber Security Framework Selection: Comparison of NIST and ISO 27001 discusses cybersecurity frameworks encompassing international standards and best practices for safeguarding information and IT infrastructure. These frameworks serve as foundations for enhancing network security, aiding in threat analysis, monitoring, and response during cyber-attacks, contributing to robust safety in both government and private sectors. Despite differences, all frameworks aim to standardize threat defense, manage cybersecurity protocols, and implement efficient measures, offering companies diverse options for informed decision-making based on suitability and effectiveness.

NIST Cybersecurity Framework (CSF) 2.0 offers guidance for managing cybersecurity risks across industries and organizations, providing a taxonomy of outcomes applicable irrespective of size or sector. These outcomes assist in understanding, evaluating, prioritizing, and communicating cybersecurity efforts within organizations (National Institute of Standards and Technology, 2024).

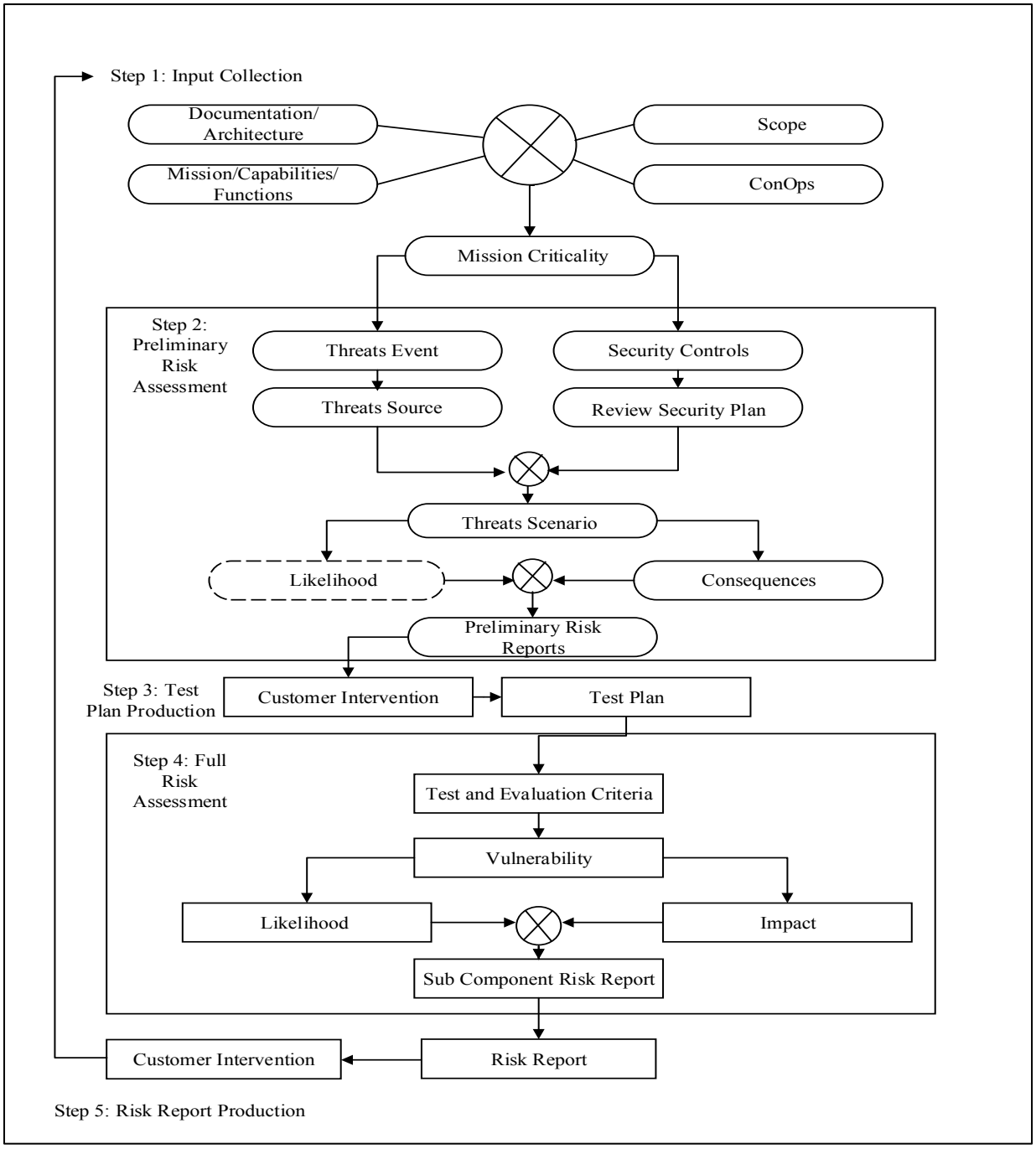


Figure 1: Framework Functions (National Institute of Standards and Technology, 2024)

Cyber Risk Assessment (CRA) framework introduces Military Risk Evaluation (MRE), to address the unique challenges of military cyberspace. Integrating quantitative data from Vulnerability Detection (VD) tools and qualitative insights from focus groups, CRA enhances standard risk assessment for comprehensive national cyber security planning (Dr. Peter Katsumata, 2010).

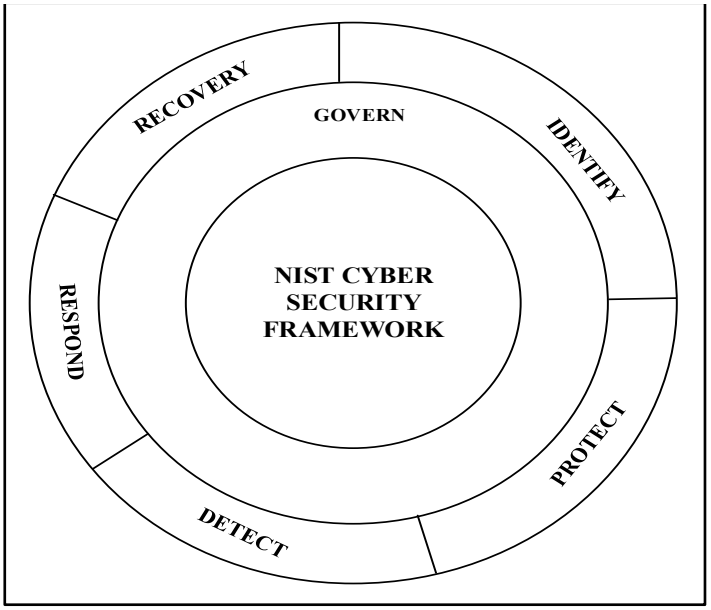


Figure 2: Risk Assessment Framework

Cyber threat information comprises data assisting organizations in identifying, assessing, monitoring, and responding to cyber threats. This includes indicators of compromise, tactics, techniques, and procedures utilized by threat actors, along with suggested actions for detection, prevention, and incident analysis findings. Sharing such information enhances security postures for both sharing and receiving entities, fostering collaboration and proactive defense against cyber threats (Chris Johnson, 2016).

Table 1: Launching a Threat Information Sharing Capability

Threat Information	Description
Indicators	Observables signal potential attacks or compromises, aiding in threat detection and defense. Examples include suspicious IP addresses, malicious URLs, or file hashes.
Tactics, Techniques, and Procedures (TTPs)	Behavior of threat actors, detailing their methods, tools, and attack patterns.
Security Alerts	Brief technical notifications regarding current vulnerabilities and exploits, sourced from organizations like US-CERT, ISACs, and commercial security providers.
Threat Intelligence Reports	Narrative documents providing insights into TTPs, threat actors, and targeted systems, offering greater situational awareness.
Tool Configurations	Recommendations for setting up and using tools to facilitate the automated collection, analysis, and utilization of threat information, enhancing organizational security posture.

Vulnerabilities are weaknesses in products or systems that attackers exploit to access sensitive information or cause harm. These weaknesses exist in various components such as software, firewalls, network protocols, wireless networks, operating systems, and web servers. Attackers search for errors or misconfigurations in these areas to compromise security and gain unauthorized access or control, posing significant risks to organizations (Omer Aslan, 2023).

Table 2: Various Types of Vulnerabilities

Vulnerability Type		Description
Software Vulnerabilities		Flaws within software applications due to errors or bugs, exploited by attackers to compromise system integrity. Examples include buffer overflow and race conditions.
Firewall Vulnerabilities		Mistakes, deficiencies, or faulty assumptions during design, implementation, or configuration of firewalls, allowing attackers to exploit weaknesses and launch attacks.
TCP/IP Vulnerabilities		Weaknesses in network protocols across various layers, lacking desired features in unsecured networks. Examples include ARP attacks and fragmentation attacks.
Wireless Network Vulnerabilities		Protocol-based attacks and insecure access points in Wireless Local Area Networks (LANs), providing unauthorized entry points for attackers. Examples include SSID and WEP issues.
Operating System Vulnerabilities		Security vulnerabilities in operating systems like Windows, macOS, and Unix, influencing the security of running applications.
Web Server Vulnerabilities		Design and engineering errors in web servers leading to vulnerabilities exploited by attackers for sniffing and spoofing attacks.

In today's digital landscape, cybersecurity adapts to the evolving dynamics of the internet, emphasizing flexibility in countering threats. Global internet usage mandates adherence to common standards, with cybersecurity standards offering crucial best practices to fortify companies against cyber threats. These frameworks benefit businesses across industries, providing essential guidelines regardless of size or sector.

7. Methodology

The rapid evolution of cyber threats demands continuous evaluation and enhancement of existing practices to ensure the resilience and effectiveness of military operations. It endeavors to conduct a comprehensive gap analysis of cyber security frameworks and practices within the military domain, aiming to identify areas of improvement and propose strategies for bolstering cyber defense capabilities.

The cybersecurity framework is essential to identify gaps and practices within the military. The research design primarily focuses on addressing the specific research problem, which entails determining methods for acquiring information, assessing the researcher's capabilities, organizing chosen information-gathering methods, considering the available time frame, and managing allocated financial resources. These key considerations ensure the research is conducted effectively and efficiently, providing valuable insights into military cybersecurity practices (Kothri, 2004).

The conceptual framework for this study is structured around the NIST Cybersecurity Framework (CSF) Version 2.0. The NIST Cybersecurity Framework (CSF) 2.0 serves as a guiding tool for organizations

across various sectors, including industry and government agencies, to effectively manage cybersecurity risks. It presents a comprehensive taxonomy of key cybersecurity objectives that organizations of any size or maturity level can utilize to evaluate, prioritize, and communicate their cybersecurity endeavors. Rather than dictating specific methods for achieving these objectives, the CSF provides links to supplementary resources offering guidance on various practices and controls that can be employed to meet these goals (NIST, 2024).

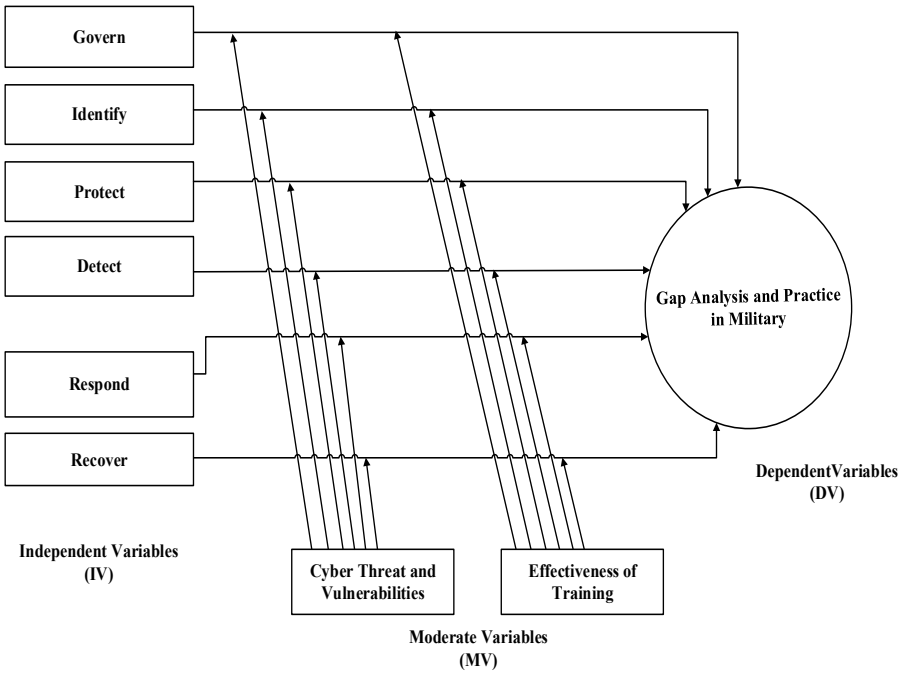


Figure 3: Conceptual Framework

The population for this study encompasses both governmental and non-governmental organizations involved in military defense and security operations. Governmental organizations include military branches, defense agencies, intelligence units, and other entities responsible for national defense. Non-governmental organizations encompass defense contractors, private security firms, and industry partners supporting military operations.

In determining the sampling size based on the questionnaire respondents, it is required to balance the need for comprehensive coverage with practical considerations such as time, resources, and accessibility.

		Frequency	Percent	Cumulative Percent
Valid	Enlisted	19	4.9	4.9
	Junior Officer (Lieutenant, Captain)	92	23.8	28.8
	Senior Officer (Major, colonel)	120	31.1	59.8
	General Officer (Brigadier General, Major General)	25	6.5	66.3

	Civilian Employee	41	10.6	76.9
	Manager	55	14.2	91.2
	IT Officer	29	7.5	98.7
	Other	5	1.3	100.0
	Total Respondents	386	100.0	

The research is based on the primary and secondary data. Survey questionnaire was designed for the collection of relevant data to analyze the gap of cyber security framework and practices in military. The questionnaire is divided into two sections: Demographic and Gap Analysis of Cyber Security Framework. Both the section includes the Likert scale to collect the qualitative data based on the variables defined in the Conceptual Framework.

The pilot review on Gap Analysis, CSF Core Framework and Practices in Military was done to initialize the direction of the research, to identify and develop the instruments for measuring the variables and to pilot test the different data collected for the conceptual framework. The general survey was done to collect the data and the views of the respondents. The data necessary for conducting the gap analysis outlined were derived from the survey responses provided by the participants.

The testing of reliability for the research, the SPSS instrument was selected with the identification of different variables. Thus, Cronbach's Alpha as the reliability coefficient was determined to measures the internal consistency of the items showing the close relationship of items are as a group.

8. Results and Discussion

The total 386 respondents profile has been carefully analyzed based on the Business Demographic BD) and the Participants Demographic (PD). Business Demographic (BD) refers to the collective characteristics of individuals within an organization, focusing on their roles, ranks, occupations, and the financial size of the organization.

Statistics						
		BD1_Role	BD2_Employee	BD3_Sector	BD4_Investment	BD5_Incident
N	Valid	386	386	386	386	386
	Missing	0	0	0	0	0

Participants demographics includes factors such as age, gender, education level, occupation, and any other relevant details about the participants.

Statistics						
		Rank	Experience	Age	Gender	Qualification
N	Valid	386	386	386	386	386

	Missing	0	0	0	0	0

On checking the normality of the data, the data are normally distributed and has the significance importance in the research study.

Descriptive Statistics						
	N	Mean	Std. Deviation	Skewness		Kurtosis
	Statistic	Statistic	Statistic	Statistic	Std. Error	Statistic
Business_ Demographic	386	2.8487	.61708	-.299	.124	-.285
Participant_ Demographic	386	2.6062	.44050	-.519	.124	.531
Valid N (List-wise)	386					

The normality check depicts that the variables identified were normal and the performance of the variables are good enough for the justification of the conceptual data modelling and the survey data collection.

Descriptive Statistics						
	N	Mean	Std. Deviation	Skewness		Kurtosis
	Statistic	Statistic	Statistic	Statistic	Std. Error	Statistic
Govern	386	3.2509	.46652	-.818	.124	1.292
Identify	386	2.8912	.47699	.751	.124	.731
Protect	386	1.7223	.57837	.927	.124	-.008
Detect	386	2.1337	.38350	.999	.124	2.226
Response	386	2.1431	.37461	1.496	.124	4.697
Recovery	386	2.0964	.33098	.850	.124	3.453
Vulnerabilities_Training	386	4.0611	.54382	-.968	.124	1.556
Gap_ Analysis	386	3.2617	.45474	-.608	.124	1.642
Valid N (List-wise)	386					

Inferential Analysis

The purpose of inferential analysis is to the draw conclusions based on the data collected from the respondents.

Pearson's Correlation Analysis was done to find the relation between the independent variable, dependent variable and moderating variables.

Correlations				
		GV3	GV4	GV6
GV3	"Pearson Correlation"	1	.189**	.286**
	Sig. (2-tailed)		.000	.000
	Covariance	.968	.179	.273
	N	386	386	386
GV4	Pearson Correlation"	.189**	1	.734**
	Sig. (2-tailed)	.000		.000
	Covariance	.179	.930	.688
	N	386	386	386
GV6	Pearson Correlation"	.286**	.734**	1
	Sig. (2-tailed)	.000	.000	
	Covariance"	.273	.688	.944
	N	386	386	386

**. "Correlation is significant at the 0.01 level (2-tailed)".

By this process, the reliability and accuracy of conceptual framework designed was examined.

Reliability Statistics		
Variables	Cronbach's Alpha	N of Items
Govern	.668	3
Identify	.782	4
Protect	.761	4
Detect	.768	3
Response	.840	3
Recovery	.869	3

Cyber Vulnerabilities and Effectiveness of Training	.732	19
Gap Analysis and Practice in Military	.833	3

Based on the values of the variables, it has given the actual relationship between the dependent and independent variables.

Model Summary[b]				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.484[a]	.235	.223	.40095
a. Predictors: (Constant), Recovery, Govern, Identify, Detect, Response, Protect				
b. Dependent Variable: Gap_Analyss				

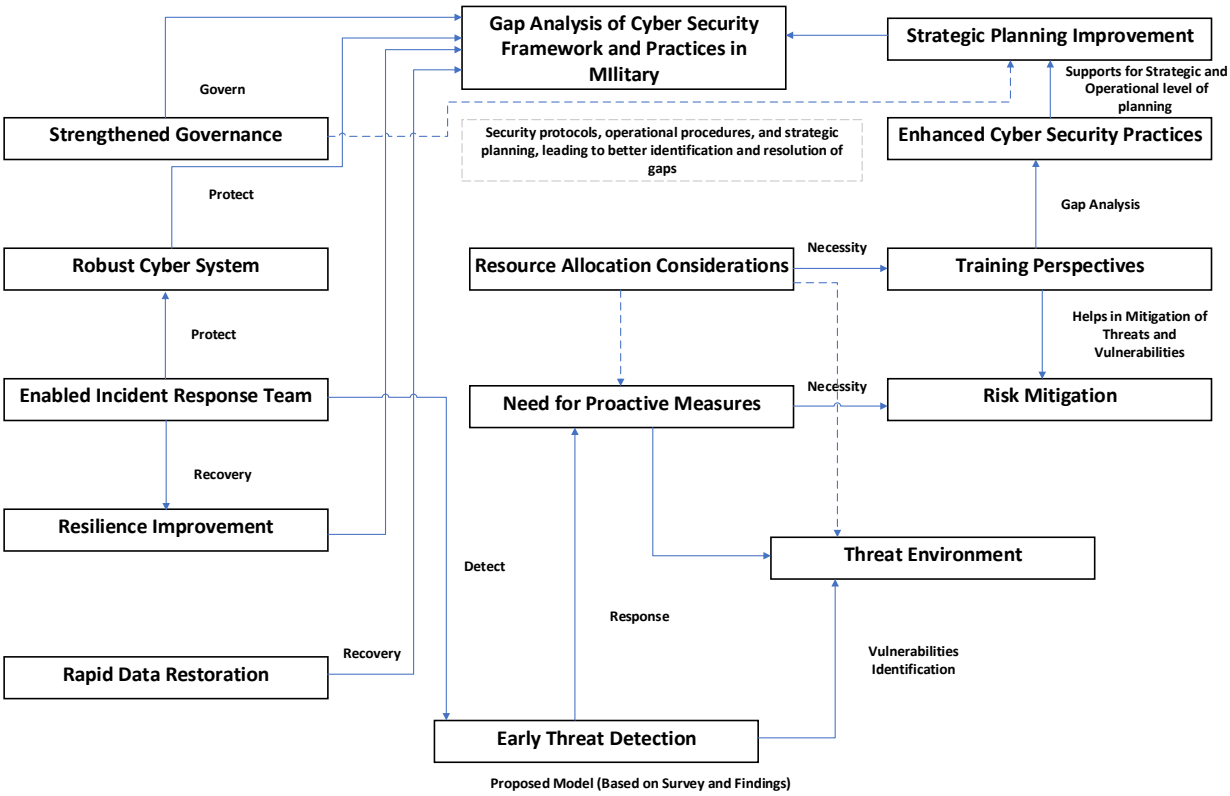
ANOVAa						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	18.683	6	3.114	19.369	.000[b]
	Residual	60.929	379	.161		
	Total	79.613	385			
a. Predictors: (Constant), Recovery, Govern, Identify, Detect, Response, Protect b. Dependent Variable: Gap_Analysis						

Coefficients[a]						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1.394	.197		7.086	.000
	Govern	.146	.059	.150	2.499	.013
	Identify	.414	.074	.434	5.573	.000
	Protect	-.313	.067	-.398	-4.699	.000
	Detect	.043	.073	.037	.592	.554
	Response	.313	.078	.257	4.027	.000
	Recovery	-.014	.091	-.010	-.153	.878

Indeendent Variables	Dependent Variable	Significance value	P Value ($p < 0.05$)	Remarks
Govern	Gap_Analyss	.000	$p < 0.05$	Statistically significant
Identify		.013	$p < 0.05$	Statistical significance
Protect		.000	$p < 0.05$	Statistical significance
Detect		.000	$p < 0.05$	Statistical significance
Response		.554	$p > 0.05$	Not statistically significant
Recovery		.000	$p < 0.05$	Statistical significance

After the analysis of all the test and variables, attributes and literature reviews, the cyber security plays the pivotal role in the military domain. The enhanced and upgraded system is the crucial part on the paradigm of present information and communication technology era. The robust and skilled-manpower in the military cyber security is paramount for dealing with the present cyberspace and threat landscape.

After the survey, the actual relationship was traced out which implies the following outcomes as the major findings proposed in the model form.



Proposed Model (Based on Survey and Findings)

9. Conclusion

In the military domain, cyber security is a paramount concern given the sensitive nature of military operations and the vast amounts of classified information stored and transmitted through digital systems. Cyber security encompasses a range of measures designed to protect military networks, systems, and data from unauthorized access, disruption, or destruction by cyber threats. These threats can take various forms, including sophisticated cyber-attacks launched by state-sponsored adversaries, malicious insiders seeking to exploit vulnerabilities, and opportunistic hackers probing for weaknesses in defense systems. Moreover, the complexity and interconnectedness of military networks present inherent vulnerabilities that must be continuously monitored and addressed to maintain operational readiness and ensure mission success.

The comprehensive overview of the critical role of cyber security within military operations, highlights the importance of addressing gaps in cyber security frameworks. Future research in the field of cyber security within military operations can build upon the findings of this study and address several limitations or gaps to further advance knowledge and enhance practical applications. Some suggestions for future research include:

Cross-National Comparative Studies: Cross-national comparative studies can help identify common challenges and innovative approaches to cyber security that can be shared and adapted across borders.

Qualitative Research: Qualitative research methods, such as interviews, focus groups, and case studies, can provide deeper insights into the experiences, perceptions, and challenges faced by military personnel and leaders in implementing cyber security measures.

Simulation and Scenario-Based Studies: By simulating realistic cyber threats and incidents, military organizations can identify weaknesses, test response procedures, and evaluate the effectiveness of training programs in a controlled environment.

Integration of Emerging Technologies: Future research can explore the integration of emerging technologies, such as artificial intelligence, machine learning, and block chain, in enhancing cyber security practices within military operations.

Cyber Threat Intelligence and Information Sharing: Research on cyber threat intelligence gathering, analysis, and information sharing mechanisms can help improve situational awareness and enable proactive threat detection and response.

References

(NATO). (2021). Cyber Security Risk Assessment Process for Military Systems. NORTH ATLANTIC TREATY ORGANIZATION, SCIENCE AND TECHNOLOGY ORGANIZATION. STO/NATO.

Alshar, M. (2023, February). CYBER SECURITY FRAMEWORK SELECTION: COMPARISION OF NIST AND ISO27001. Applied Computing Journal, 3(1), pp 245-255.

Annya Dixit, S. N. (2023, December). CYBER SECURITY CHALLENGES IN MILITARY SECTOR . (Volume:05/Issue:12/December, Ed.) International Research Journal of Modernization in Engineering Technology and Science, 5(12).

Asst. Prof. Benjamin C. Leitzel, A. P. (2022). Strategic Cyberspace Operations Guide. U.S. Army War College.

Bhadwal, A. (2023, September 15). The History of Cyber Security: A Detailed Guide [Infographic]. (K. S. Limited, Producer) Retrieved from upGrad Knowledge Hut: https://www.knowledgehut.com/blog/security/history-of-cyber-security

Borghard, M. M. (2021). Cyber Threats and Vulnerabilities to Conventional and Strategic Deterrence. Joint Force.

C.R.Kothari. (2004). ResearchMethodology: Methods & Techniques (2nd Edition ed.). Rajasthan, Jaipur, India: New Age International (P) Ltd.

Chris Johnson, L. B. (2016). Guide to Cyber Threat Information Sharing: Computer Security. NIST.

Delinea . (2024). Mapping the NIST Cybersecurity Framework 2.0 to Delinea Privileged Access Management. Delinea Privileged Access Management (PAM). Delinea .

Dnyandev, R. (2023, July). Application and Importance of Cyber Security in Military Service: A Literature Review. International Journal of Advanced Research in Science, Communication and Technology (IJARSCT), 3(1).

Don Snyder, J. D.-B. (2015). Improving the Cybersecurity of U.S. Air Force Military Systems Throughout Their Life Cycles . RAND Corporation. Santa Monica, Calif.: RAND Corporation.

Dr. Peter Katsumata, J. H. (2010). Cybersecurity Risk Management . The 2010 Military Communications Conference:Cyber Security and Network Management. Los Angeles: IEEE.

G. Alexander Crowther, P. (2018). National Defense and the Cyber Domain . The Heritage Foundation .

Ghazali, N. H. (2016). A Reliability and Validity of an Instrument to Evaluate the School-Based Assessment System: A Pilot Study. International Journal of Evaluation and Research in Education (IJERE), 5(2), 148-157.

Glasow, P. A. (2005). Fundamentals of Survey Research Methodology . MITRE PRODUCT .

Haradhan, M. a. (2017). Two Criteria for Good Measurements in Research: Validity and Reliability . Munich Personal RePEc Archive.

Joy Fraser, D. (. (2018, February). Pilot Testing for Feasibility in a Study of Student Retention and Attrition in Online Undergraduate Programs . International Review of Research in Open and Distributed Learning , Vol.9(1).

Kothri, C. (2004). Research Methodology Methods and Techniques (2nd Edition ed.). Rajasthan, Jaipur, India: New Age International (P) Ltd.

Leroy R. Thacker II, P. (2020). What Is the Big Deal About Populations in Research? Progress in Transplantation , 30(1).

Masterson, A. D. (2019). "Contrasting cybersecurity implementation frameworks (CIF) from three countries", Information & Computer Security . Emerald Insight .

Ministry of Defense . (2022). Cyber Primer (Vol. 3rd). U.K: UK Ministry of Defence (MOD) .

Muhammer Karaman, H. Ç. (2016). Institutional Cybersecurity from Military Perspective. INTERNATIONAL JOURNAL OF INFORMATION SECURITY SCIENCE, Vol. 5(1).

Muhammer Karaman, H. C. (2016). Institutional Cybersecurity from Military Perspective. INTERNATIONAL JOURNAL OF INFORMATION SECURITY SCIENCE, 5(1).

Muhammer Karaman, H. C. (2016, March). Institutional Cybersecurity from Military Perspective . INTERNATIONAL JOURNAL OF INFORMATION SECURITY SCIENCE, 5(1).

Nadia Al. Muqrashi & Muhammed Saqib, I. D. (2022, July 20). An Overview of Cybersecurity and Proposed Framework of Security & Protection. Elsevier.

National Computer and Cybercrimes Coordination Committee(NC4) Secretariat. (n.d.). NATIONAL CYBERSECURITY STRATEGY. THE REPUBLIC OF KENYA, NATIONAL COMPUTER AND CYBERCRIMES COORDINATION COMMITTEE (NC4) SECRETARIAT. Nairobi, Kenya: National Computer and Cybercrimes Coordination Committee(NC4) Secretariat.

National Institute of Standards and Technology. (2024, February 26). The NIST Cybersecurity Framework (CSF) 2.0. NIST Cybersecurity White Paper (CSWP) NIST CSWP 29.

NIST. (2024). The NIST Cybersecurity Framework (CSF) 2.0. National Institute of Standards and Technology, US Department of Commerce. Gaithersburg, MD: National Institute of Standards and Technology, NIST Cybersecurity White Paper (CSWP) NIST CSWP 29.

NIST. (2024). The NIST Cybersecurity Framework (CSF) 2.0. National Institute of Standards and Technology.

Omer Aslan, S. S. (2023, March). A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solution. Electronics, 12(6), 1-42.

Oribhabor, C. B. (2019). Research Sampling and Sample Size Determination: A practical Application. Journal of Educational Research (Fudjer), 2(1), 47-56.

PATEL, T. P. (2017, June). Cyber security: Study on Attack, Threat, Vulnerability. International Journal of Research in Modern Engineering and Emerging Technology, 5(6).

Poornima, B. (2023). Cyber Preparedness of the Indian Armed Forces. Journal of Asian Security and International Affairs.

Rane, R. D. (2023, July). Application and Importance of Cyber Security in Military Service: A Literature Review. International Journal of Advanced Research in Science, Communication and Technology (IJARSCT), Vol. 3(1).

Scott J. Shackelford, J. P. (2015). SECURING NORTH AMERICAN CRITICAL INFRASTRUCTURE: A COMPARATIVE CASE STUDY IN CYBERSECURITY REGULATION. Canada-US Law Journal 15-20, https://ssrn.com/abstract=2576460.

Smeets, A. B. (2020). Military Operations in Cyberspace. In A. Sookermany, Handbook of Military Sciences (pp. pp 1–16). Springer.

Smith, W. (2019). A Comprehensive Cybersecurity Defense Framework for Large Organizations. Nova Southeastern University, College of Computing and Engineering . Nova Southeastern University, NSUWorks.

The NIST (CSF) 2.0. (2024, Feburary). National Institute of Standards and Technology(NIST).

The White House, Washington. (2023). NATIONAL CYBERSECURITY STRATEGY.

UK Ministry of Defence. (2022). Cyber Primer, 3rd Edition. MOD Abbeywood South, UK: UK Ministry of Defence © Crown copyright (2022).

ZUKIC, C. A. (2020). ASSESSING THE ROLE OF THE MILITARY IN NATIONAL CYBERSECURITY EFFORTS. U.S.

Army Command and General Staff College, Faculty of the U.S. Army Command and General Staff College.

ATTN: ATZL-SWD-GD Fort Leavenworth, KS 66027-2301: U.S. Army Command and General Staff College.