CENJOWS

ISSUE BRIEF

CYBER SECURITY FRAMEWORK: IMPACT ON TRI SERVICES COMMAND STRUCTURES

COL B AMARNATH

www.cenjows.in

CENTRE FOR JOINT WARFARE STUDIES

Aligned with the Future

Victory through Joint Knowledge

CENJOWS

CYBER SECURITY FRAMEWORK: IMPACT ON TRI SERVICES COMMAND STRUCTURES

Col B Amarnath, is presently undergoing HDMC -18 at College of Defence Management. The officer has experience of all terrains and operational environments.

"I dream of a digital India where cybersecurity becomes an integral part of National Security." - Shri Narendra Modi

Background

National Cyber Security Policy (2013) has been promulgated by Governments of India (GoI) with the vision to institute a safe & robust cyber domain. The policy functions as a regulatory authority for outlining & guiding the actions linked to the safety of cyber domain. It provides public awareness to efficiently protect the data, associated cyber assets & the networks. The policy also provides an understanding into the GoI methodology and the course of action for the safety of cyber domain. The policy aims to build a cybersecurity framework, to enhance the security posture of the country's cyber domain.

Cyber threat continues to evolve at a rapid pace across the world and data breaches are growing in numbers every day. Internet has rapidly advanced to become an integral part of the world. However, the integration of cyber security practices has not kept pace in spite of Cybersecurity becoming a routine term and a major concern in our daily lives. The cyber domain and its associated expertise have become tools of usable power i.e. diplomacy, information, military and economy (DIME).

DCyA has been established to deter and defend the Nation against cyber threats to digital assets of Armed Forces from adversaries. DCyA is expected to provide a roadmap for combating threats to military targets in cyber domain. The agency will enhance cooperation amongst the three services and will also foster synergy. This will lead to enhanced effectiveness and optimal exploitation of resources in keeping with the Joint Training Doctrine of 2017.

There is a common perception that Armed Forces resort to temporary institutions and adhoc measures to overcome Cyber Security Incidents. Such practice raises concern for which such Command structures for the Cybersecurity are established. These challenges highlight the inescapable requirement to re-visit the present Command Structure for their efficacy and efficiency.

Impact Command Structure

Research was undertaken to study “Cyber Security Framework: Impact on Tri Services Command Structures". The Broad Research area was divided into Sub Topics and finally focused on “**Adequacy of Command Structure for Cyber Security Operations at Armed Forces Command Headquarter Level in Indian Army**”.

Amongst all the important aspects of effectiveness of Cyber Security Operations, one of the most important aspect is responsiveness of Command Structure to the Cyber Threat at operational level. The issue has also gained significance in the backdrop of increasing Cyber Threats, digital India initiatives and modernisation and proposed **Theaterisation** of Armed Forces. Concentrated efforts are being invested both by National authorities and the Armed Forces in combating the Cyber Threats. This study has limited this research only to the aspect of adequacy of command structure, which results in efficacy and efficiency of actions by Armed Forces during Cyber Security Operations.

Research Questions.

There is a need to answer the following questions to arrive at desired end state:-

(a) How efficient are the Tri Services components in responding to Cyber Security Threats?

(b) How Can the Command Structure for Cyber Security Organisation in IA be made more responsive?

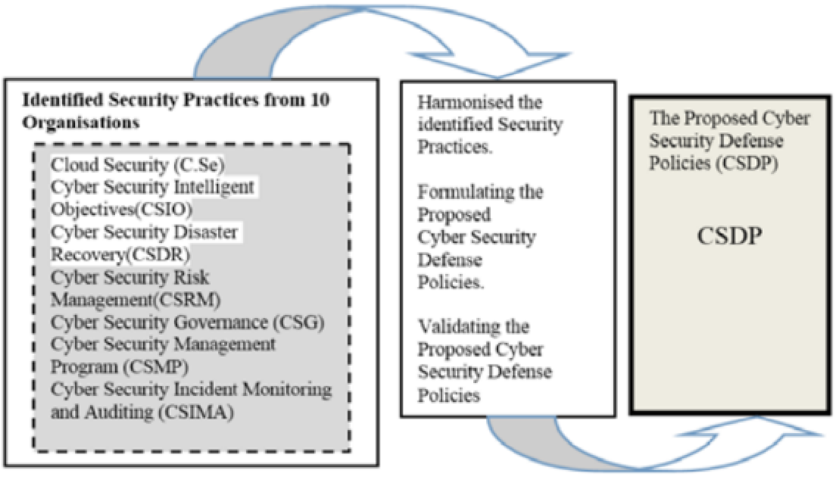
(c) What are the organisational approaches to improve responsiveness of Command Structure for Cyber Security Operations in IA?

Literature Review

Literature Review has been carried out to build suitable contextual understanding on Cyber Security Operations undertaken across the world. The review of Literature included study of the genesis of the Cyber Security Operations, Cybersecurity Frameworks, contemporary cyber threats in the 21st century, IT Risk in the Wake of Armed Conflict Operations especially the Russo-Ukraine war, The diffusion of cyber forces: Military innovation across various Armed Forces, China based State Sponsored Advanced Persistent Threat (APT) group targeting the critical infrastructure for espionage, Importance of robust Cyber Security Infrastructure for implementation of Digital Economy, establishment of Defence Cyber Command, National Cyber Security Policies 2013, Legal Acts, established procedures and guidelines (SOPs) for Cyber Security Operations, books from CDM Library, various articles on the topic, discussions with General Staff Information Warfare of Comd HQs, Offrs who have participated in Cyber Security Operations or were part of Army Cyber Group.

Cyber Security Defence Policies In a research paper titled "A Proposed Guidelines for Organisations Cyber Security Practices". Published in 2020 in International Journal. The paper Hypothesis's and recommends the methodology to formulate a Cyber Security Policy as shown in the ***Figure 1.*** To identify seven basic components from 10 reputable security organisations in the environment, harmonise the identified Security Practices, Formulate the Recommended Cyber Security Policy, Validate the Suggested Policy & Implement the Validated Cyber Security Defence Policy to improve the overall security of the organisation.

***Figure 1**: Methodology to develop a Cyber Security Defence Policy*


Identified Security Practices from 10 Organisations
Cloud Security (C.Se)
Cyber Security Intelligent Objectives(CSIO)
Cyber Security Disaster Recovery(CSDR)
Cyber Security Risk Management(CSRM)
Cyber Security Governance (CSG)
Cyber Security Management Program (CSMP)
Cyber Security Incident Monitoring and Auditing (CSIMA)
Harmonised the identified Security Practices.
Formulating the Proposed Cyber Security Defense Policies.
Validating the Proposed Cyber Security Defense Policies
The Proposed Cyber Security Defense Policies (CSDP)
CSDP

Cyber-Attack Scoring Model. In a research paper titled "Cyber-Attack Scoring Model Based on the Offensive Cybersecurity Framework" by authors Kyounggon Kim, Faisal Abdulaziz Alfouzan, and Huykang Kim Published in 2021 in International Journal The research article having identified that there is an absence of research to measure cyber-attacks, proposed a model for quantification of cyberattacks by undertaking Taxonomy of various factors as shown in the ***Figure 2*** below: -

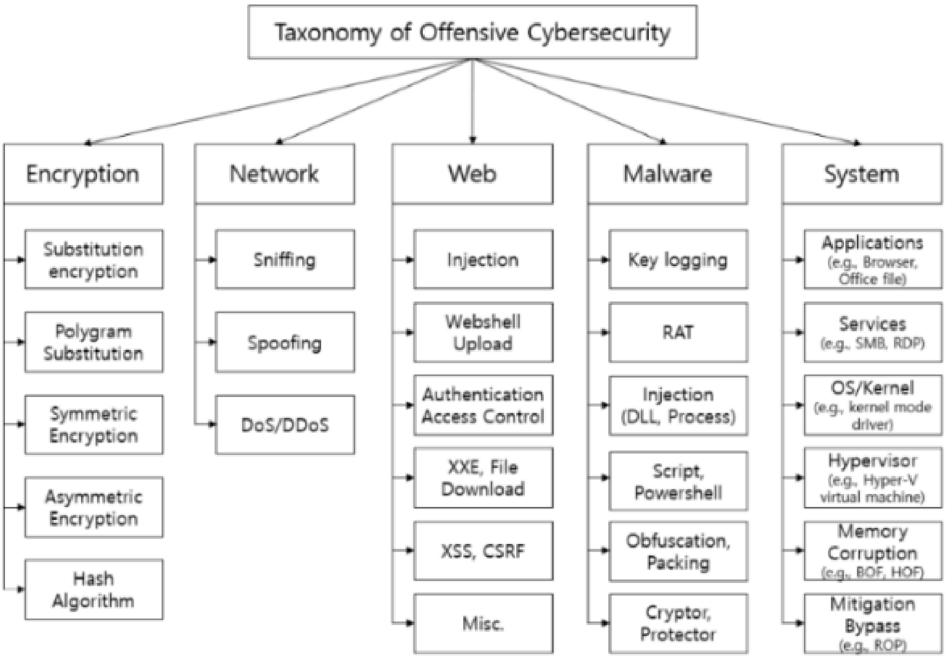
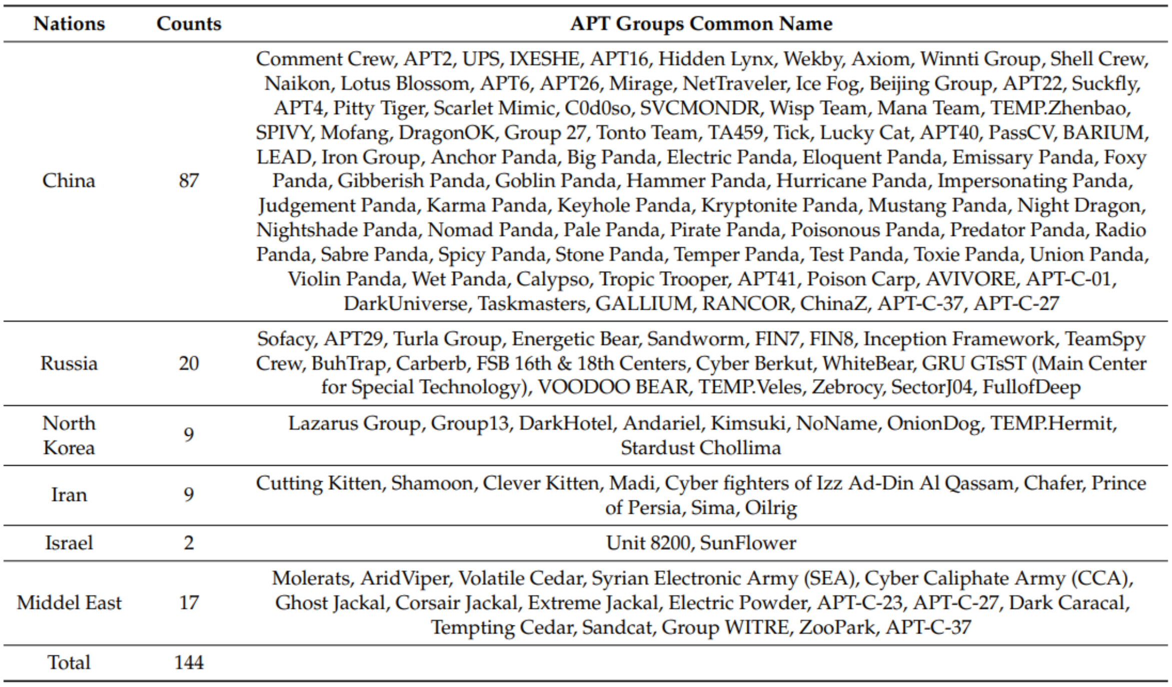


Figure 2: Taxonomy of Offensive Cybersecurity

The research article identified that the hackers sponsored by China are actively using aggressive cybersecurity technology to execute multifaceted attacks. China has the most no of cyber-attack groups and Israel’s Unit 8200 group is recognized to be the most potent group even though it has only two groups. The APT group along with their Nations are as listed in the **Table 1** below: -

Table 1: Nations wise List: Advanced Persistent Threat (APT)



Nations	Counts	APT Groups Common Name
China	87	Comment Crew, APT2, UPS, IXESHE, APT16, Hidden Lynx, Wekby, Axiom, Winnti Group, Shell Crew, Naikon, Lotus Blossom, APT6, APT26, Mirage, NetTraveler, Ice Fog, Beijing Group, APT22, Suckfly, APT4, Pitty Tiger, Scarlet Mimic, C0d0so, SVCMONDR, Wisp Team, Mana Team, TEMP.Zhenbao, SPIVY, Mofang, DragonOK, Group 27, Tonto Team, TA459, Tick, Lucky Cat, APT40, PassCV, BARIUM, LEAD, Iron Group, Anchor Panda, Big Panda, Electric Panda, Eloquent Panda, Emissary Panda, Foxy Panda, Gibberish Panda, Goblin Panda, Hammer Panda, Hurricane Panda, Impersonating Panda, Judgement Panda, Karma Panda, Keyhole Panda, Kryptonite Panda, Mustang Panda, Night Dragon, Nightshade Panda, Nomad Panda, Pale Panda, Pirate Panda, Poisonous Panda, Predator Panda, Radio Panda, Sabre Panda, Spicy Panda, Stone Panda, Temper Panda, Test Panda, Toxie Panda, Union Panda, Violin Panda, Wet Panda, Calypso, Tropic Trooper, APT41, Poison Carp, AVIVORE, APT-C-01, DarkUniverse, Taskmasters, GALLIUM, RANCOR, ChinaZ, APT-C-37, APT-C-27
Russia	20	Sofacy, APT29, Turla Group, Energetic Bear, Sandworm, FIN7, FIN8, Inception Framework, TeamSpy Crew, BuhTrap, Carberb, FSB 16th & 18th Centers, Cyber Berkut, WhiteBear, GRU GTsST (Main Center for Special Technology), VOODOO BEAR, TEMP.Veles, Zebrocy, SectorJ04, FullofDeep
North Korea	9	Lazarus Group, Group13, DarkHotel, Andariel, Kimsuki, NoName, OnionDog, TEMP.Hermit, Stardust Chollima
Iran	9	Cutting Kitten, Shamoon, Clever Kitten, Madi, Cyber fighters of Izz Ad-Din Al Qassam, Chafer, Prince of Persia, Sima, Oilrig
Israel	2	Unit 8200, SunFlower
Middel East	17	Molerats, AridViper, Volatile Cedar, Syrian Electronic Army (SEA), Cyber Caliphate Army (CCA), Ghost Jackal, Corsair Jackal, Extreme Jackal, Electric Powder, APT-C-23, APT-C-27, Dark Caracal, Tempting Cedar, Sandcat, Group WITRE, ZooPark, APT-C-37
Total	144	

Develop of Effective Military Cyber Force. In a research paper titled “How to Develop a Stronger, more Effective Military Cyber Force” by Carlos R. Pesquera published in 2016 in International Journal The study establishes that the U.S. Department of Defence (DoD) and the U.S. Cyber Command have not been successful to recruit technicians to meet their staffing requirements and the concept and implementation of the U.S. Cyber Command has proven ineffective over a period of seven years. It attributes the reason for failure to the following: -

(a) U.S. Cyber Commands ties with the National Security Agency inhibit it from becoming an independent voice for the cyber warfare community.

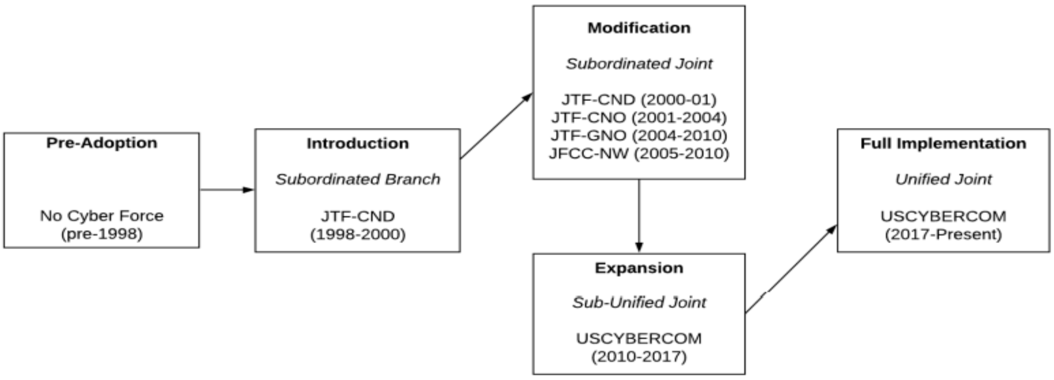
(b) Lack of a cyber-culture in the different services.

The study recommends that the above limitations can be overcome by **establishing a new org exclusively dedicated in combating the adversary in cyber domain**. The new branch needs to take into to account the unique cultural requirements of the technocrats and programmers to appeal and retain them in the Armed Forces.

Cyber Threats in the 21st Century. The article published by Alexander Dean in 2012.in the Security Magazine brings out that the US DoD identifies **cyber as the fifth domain of the battlefield**. The article highlights that about 100 foreign intelligence groups try to hack into the computer networks of the US and **majority of the cyber-attacks appear to originate in China**. It brings out that the Chinese Govt apart from engaging its own hackers also manages considerable SME teams from academia and industry in cyber-attacks with support and direction from PLA.

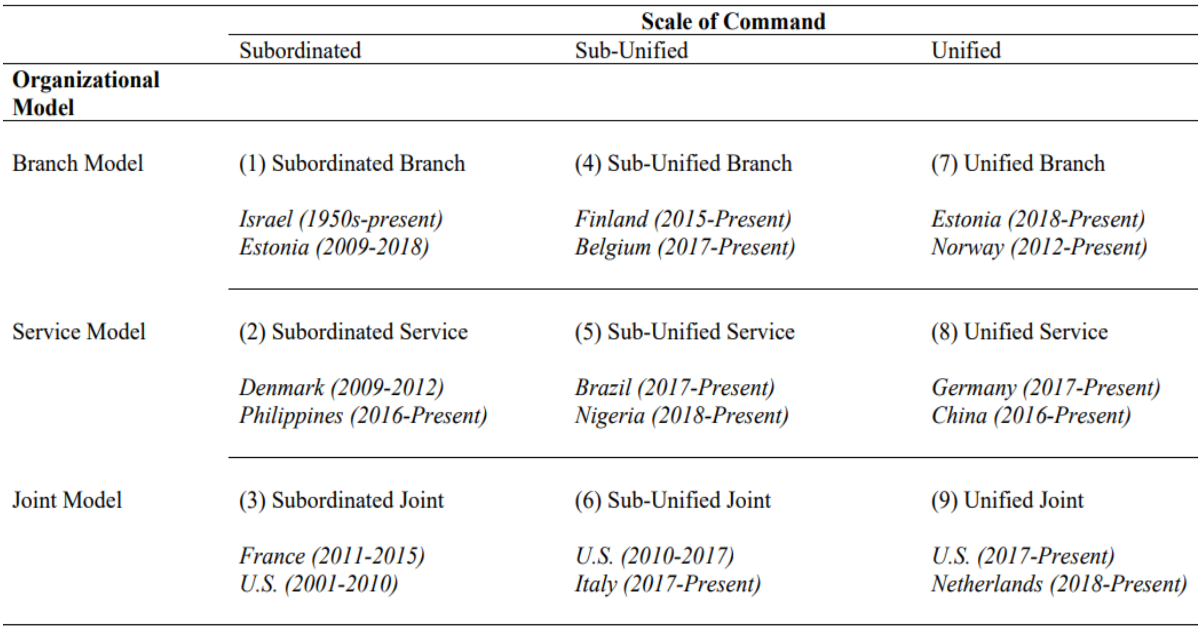
Diffusion of Cyber Forces

In a research paper titled “The Diffusion of Cyber Forces: Military Innovation and the Dynamic Implementation of Cyber Force Structure” by Jason Alexander Blessing M.A. published in 2011. The research highlights that United States has been building cyber capabilities since 1998s and finally established Unified Cyber Command in 2017, the diffusion of innovation has taken over 20 years. It further highlights how various



Nations have created their cyber forces and the region wise growth of cyber forces as shown in the ***Figure 3*** below: -

***Figure 3**: Evolution of US Cyber Command Structure*



	Scale of Command		
	Subordinated	Sub-Unified	Unified
Organizational Model			
Branch Model	(1) Subordinated Branch *Israel (1950s-present)* *Estonia (2009-2018)*	(4) Sub-Unified Branch *Finland (2015-Present)* *Belgium (2017-Present)*	(7) Unified Branch *Estonia (2018-Present)* *Norway (2012-Present)*
Service Model	(2) Subordinated Service *Denmark (2009-2012)* *Philippines (2016-Present)*	(5) Sub-Unified Service *Brazil (2017-Present)* *Nigeria (2018-Present)*	(8) Unified Service *Germany (2017-Present)* *China (2016-Present)*
Joint Model	(3) Subordinated Joint *France (2011-2015)* *U.S. (2001-2010)*	(6) Sub-Unified Joint *U.S. (2010-2017)* *Italy (2017-Present)*	(9) Unified Joint *U.S. (2017-Present)* *Netherlands (2018-Present)*

Table 2: Topology of Cyber Force Structures

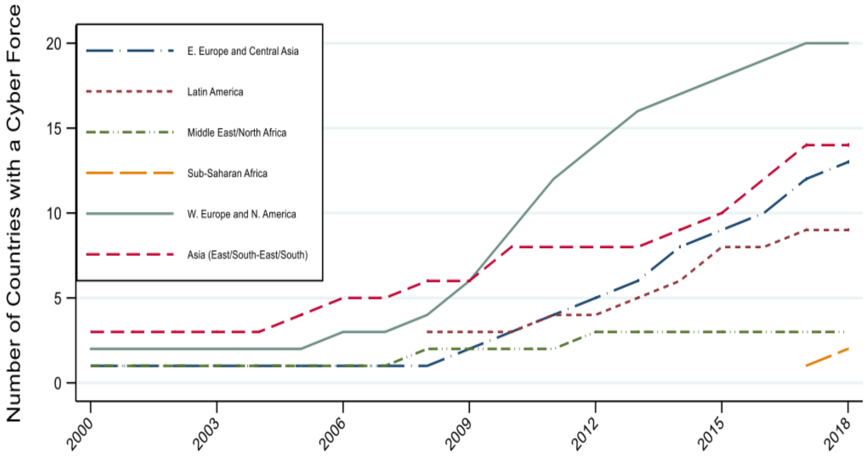
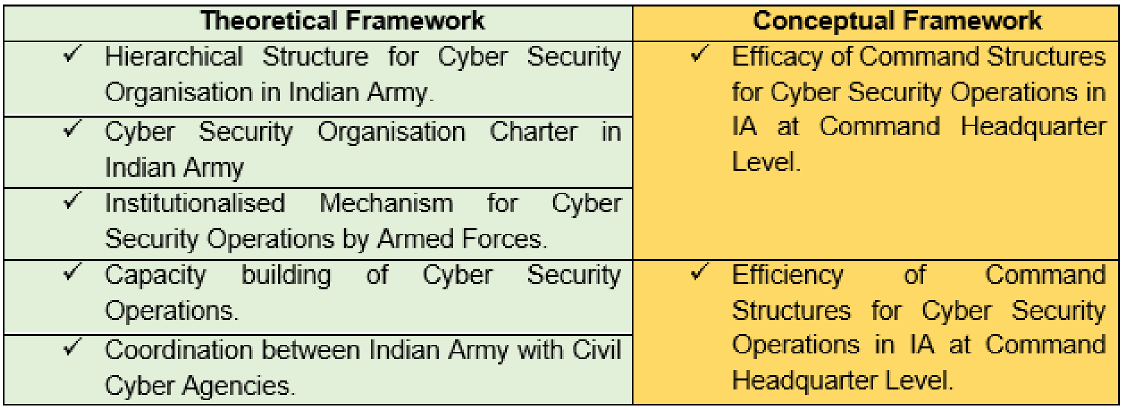


***Figure 4**: Region wise Growth of Cyber Forces*

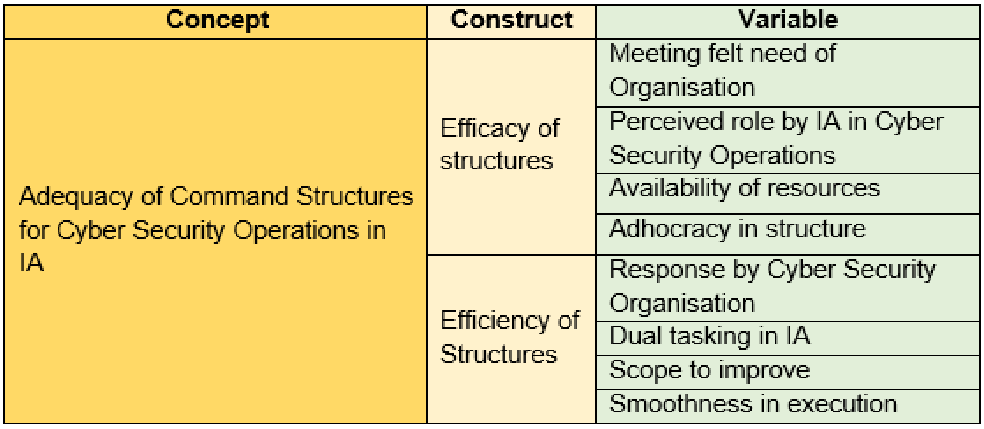
Table 2 brings out the Topology of Cyber Force Structures and Figure 4 shows the Region wise Growth of Cyber Forces**.** The paper also brings out the importance of a dedicated Cyber Force Structure by means of case study of US Cyber Forces and highlights various lessons and challenges faced by larger armed forces vis a vis smaller ones in full implementation of Cyber Force Structure.

<u>Theories Relevant to Subject</u>. The Command Structure established for Cyber Security Operations by Armed Forces at Command Headquarter level are adhoc and are not meeting the felt need. Cyber Security Operations have been satisfactory, but the overall responsiveness has been inadequate.

Primary reason was lack of joint planning and coordination, more so in Tri services environment. **Table 3** below gives out the Theoretical & Conceptual Framework and **Table 4** lists out Concept, Construct & Variables identified for the research



Theoretical Framework	Conceptual Framework
✓ Hierarchical Structure for Cyber Security Organisation in Indian Army.	✓ Efficacy of Command Structures for Cyber Security Operations in IA at Command Headquarter Level.
✓ Cyber Security Organisation Charter in Indian Army	
✓ Institutionalised Mechanism for Cyber Security Operations by Armed Forces.	
✓ Capacity building of Cyber Security Operations.	✓ Efficiency of Command Structures for Cyber Security Operations in IA at Command Headquarter Level.
✓ Coordination between Indian Army with Civil Cyber Agencies.	



Concept	Construct	Variable
Adequacy of Command Structures for Cyber Security Operations in IA	Efficacy of structures	Meeting felt need of Organisation
		Perceived role by IA in Cyber Security Operations
		Availability of resources
		Adhocracy in structure
	Efficiency of Structures	Response by Cyber Security Organisation
		Dual tasking in IA
		Scope to improve
		Smoothness in execution

Table 3 **Theoretical Framework & Conceptual Framework**

Table 4. Concept, Construct & Variables

The research gap, as identified by the Researcher, is that constant efforts are being invested for enhancing Cyber Security Operations, Incident response, Cyber Threat mitigation, preparation of Cyber Security policies, training and capacity building by both Civil Cyber Agencies as well as Armed Forces; However, there has been no study on the relationship between adhoc command structure for Cyber Security Operations in Armed forces and their adequacy for effective response.

Assumptions

The research study has incorporated a few assumptions which are as follows: -

(a) All data used for the research is of unclassified nature and have been obtained from public domain.

(b) The expert opinions are only approximate, applicable only to the present paradigm and not referring to any real-time comparisons.

(c) The attributes and criteria considered are only demonstrative and originally can vary in either direction.

Findings Based on Quantitative Analysis

Summary of the research findings based on Quantitative Data analysis is as under: -

- ***Remove Adhocracy***. Command Structures for Cyber Security Operations in IA at Command HQ level are dual tasked and there is a need to remove adhocracy to improve Command Structures to bring efficacy & efficiency in Cyber Security Operations.

- ***Efficacy of Command Structure***. Majority of the respondents & SMEs Agree that there is a requirement of removing adhocracy from Command & Control structure at command HQ level for Cyber Security Operations.

- ***Efficiency of Command Structure***. Majority of the respondents & SMEs Agree that there is a requirement to bring efficiency in Command structure of Armed Forces at Command HQ level for efficient Cyber Security Operations during incident response

- ***Feasibility to Reinforce Command Structure***. Majority of the respondents & SMEs Agree that there is feasibility to reinforce Command structure at command HQ level for Cyber Security Operations to bring efficiency.

- ***Homogeneity of Perception*****.** There exists homogeneity of views between officers of three different categories of Length of service with respect to “Efficiency of Command structures for Cyber Security Operations in IA”

- **Sufficiency of Evidence**. From the analysis of data, it has emerged that existing Command Structures at Command Headquarters does not meet the felt need with efficacy & efficiency for Cyber Security Operations.

- **Correlation**. One of the finding of the research was existence of a negative, ***weak linear correlation*** between efficacy of Command Structures for Cyber Security Operations in IA and efficiency of Command Structures for Cyber Security Operations in IA.

- However, as responsiveness of IA towards Cyber Security Operations depends on number of other factors such as ***Policies, Training, Technical Infrastructure, collaborative response by other agencies***, hence there exist a weak correlation.

The views of SMEs clearly expressed the requirement to reinforce the Command Structure for Cyber Security Operations at Command Headquarter Level in Indian Army to meet the felt need efficiently.

Analysis The Word Cloud obtained based on responses received from Survey population is as depicted in ***Figure 5*** below: -

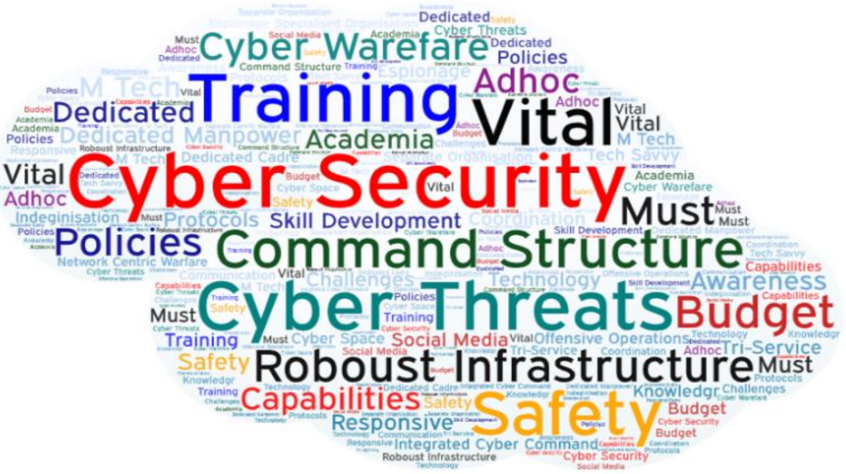


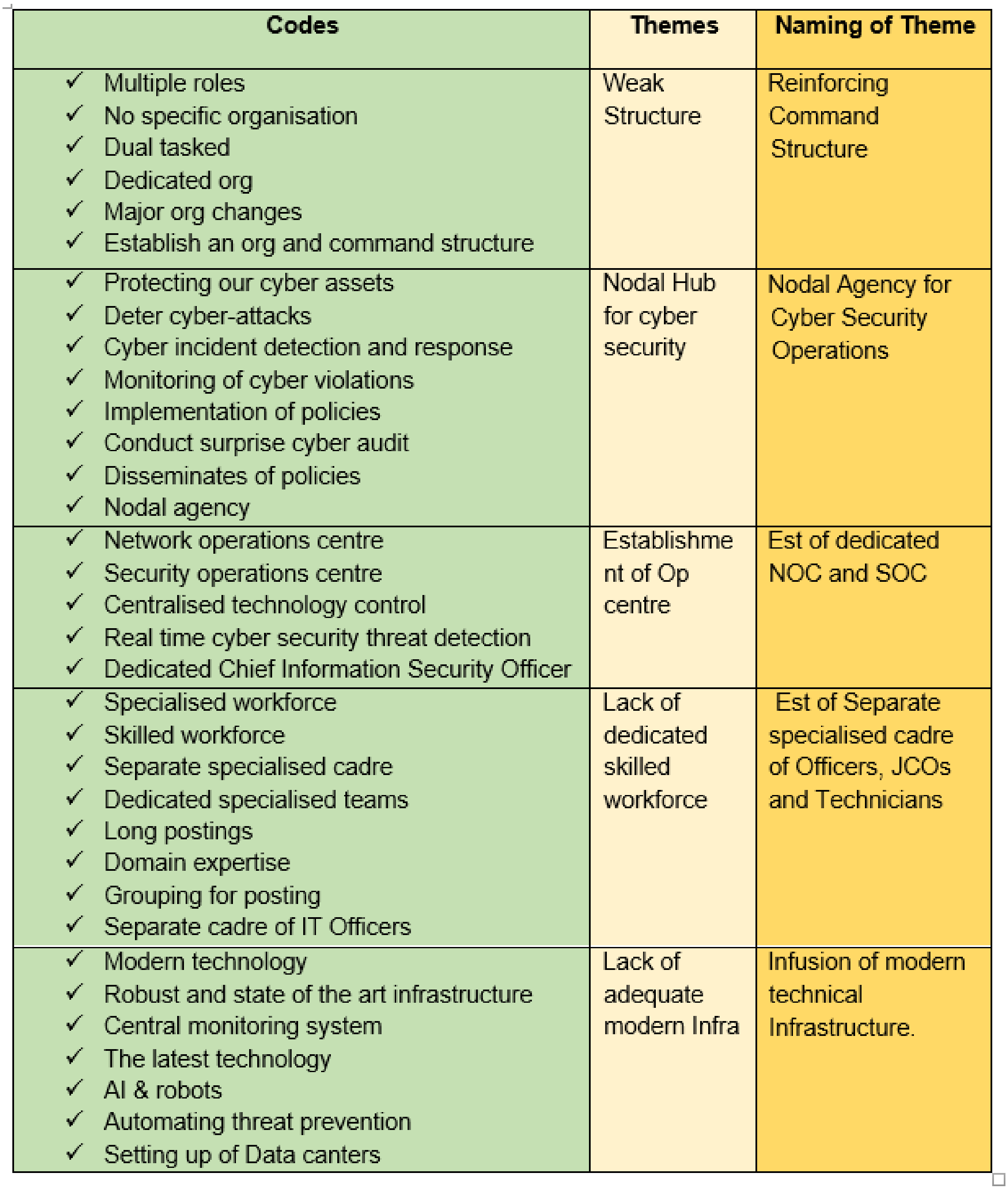
Figure 5: Word Cloud of Open Ended Responses

Findings Based on Qualitative Analysis

The interview transcriptions from six subject matter experts (SME) were Thematically Analysed for entrenched themes with respect to Cyber Security Operations by Armed Forces. The deductive approach, aided the researcher to arrive at Themes reflected in the responses by the SMEs, aligned to the build of the structured rigid interview. The indicated themes are as under: -

Thematic Analysis

Thematic Analysis of SMEs Interviews Transcripts is given in Table 5 below:-



Codes	Themes	Naming of Theme
✓ Multiple roles ✓ No specific organisation ✓ Dual tasked ✓ Dedicated org ✓ Major org changes ✓ Establish an org and command structure	Weak Structure	Reinforcing Command Structure
✓ Protecting our cyber assets ✓ Deter cyber-attacks ✓ Cyber incident detection and response ✓ Monitoring of cyber violations ✓ Implementation of policies ✓ Conduct surprise cyber audit ✓ Disseminates of policies ✓ Nodal agency	Nodal Hub for cyber security	Nodal Agency for Cyber Security Operations
✓ Network operations centre ✓ Security operations centre ✓ Centralised technology control ✓ Real time cyber security threat detection ✓ Dedicated Chief Information Security Officer	Establishment of Op centre	Est of dedicated NOC and SOC
✓ Specialised workforce ✓ Skilled workforce ✓ Separate specialised cadre ✓ Dedicated specialised teams ✓ Long postings ✓ Domain expertise ✓ Grouping for posting ✓ Separate cadre of IT Officers	Lack of dedicated skilled workforce	Est of Separate specialised cadre of Officers, JCOs and Technicians
✓ Modern technology ✓ Robust and state of the art infrastructure ✓ Central monitoring system ✓ The latest technology ✓ AI & robots ✓ Automating threat prevention ✓ Setting up of Data canters	Lack of adequate modern Infra	Infusion of modern technical Infrastructure.

Table 5 **Thematic Analysis of SMEs Interviews Transcripts**

Reinforcing Command Structure. The theme emphasises the necessity of reinforcing the Command Structure for Cyber Security Operations in Indian Army at Command HQ Level. This assumes a great significance in the light of proposed Theaterisation and also keeping the capabilities of adversaries in mind it is imperative for us to create a credible deterrence in the field of Cyber Security. Therefore, in order to efficiently take on the essential functions of planning, coordination and execution of Cyber Security Operations there is an urgent inescapable need to reinforce the Command Structure at Command HQ.

Nodal Agency for Cyber Security Operations. The theme emphasises the necessity of developing Command HQ as Nodal Agencies for Cyber Security Operations in Indian Army. The SMEs perceive and admit the nature of being dual tasked and constant commitment in tedious operational charter by the IW branch of Command HQ, which impedes its optimum level of performance in Cyber Security Operations. Therefore, creating a separate vertical of Command Structure for Cyber Security Operations empowered with the requisite resources will be a step in the right direction for facing the future challenges in the field of Cyber warfare.

Establishment of dedicated NOC and SOC. The subject matter experts indicate that in order to function seamlessly there is a requirement of having a dedicated organisation at Comd HQ level to monitor the entire spectrum of op of cyber security. The org should consist of Network Op Centre and Security Op Centre. While NOC will be ensuring that the network infrastructure is always capable of meeting the needs of the Armed Forces by keeping the network up-to-date and running optimally, SOC will protect cyber assets against all envisaged cyber threats. SOC will be responsible for hardening the cyber assets of org to deter cyber-attacks and will be performing the cyber incident detection and response in the event of a breach.

Establishment of Separate specialised cadre of Officers, JCOs and Technicians. The theme emphasises the need for creating a new branch of the Armed Forces exclusively dedicated in engaging and defeating the adversary in cyberspace to win the future wars. The new branch can be tailored to appeal and retain the dedicated team of skilled workforce and take into to account the unique cultural requirements of hackers and programmers who need not have the same physical standards as the other branches of Armed Forces. The Est of Separate specialised cadre of Officers, JCOs and Technicians in the field of Cyber Security Operations will ensure that our armed forces remain a force to recon with in the new VUCA world which poses contemporary challenges in the Cyber Domain.

Infusion of Modern Technical Infrastructure. The theme emphasises the need for Infusion of Modern Technology and robust Cyber Infrastructure which are pivotal for successful Cyber Security Operations. The subject matter experts indicate the importance of the trusted source policy operationalised by the GoI which mandates all telecom companies to declare the source of their equipment so has to guard against the potential backdoors in hardware. Indigenisation of hardware is also vital in the long run.

Recommendations

Based on the research, the recommendations are given as under: -

- **Augmentation of Command Structure.** There is a need to review and augment the Command Structure for Cyber Security Operations in IA at Command HQ Level. Many SMEs and respondents have indicated augmentation of Grade-1 Staff officer at Formation Headquarter level, which can be studied accordingly. The recommended changes will then have to be ascertained for "Systemic Desirability" and "Cultural Feasibility".

- **Planning & Coordination.** Cyber Security operations need to be planned and coordinated at the highest level in order to meet the desired end state of safe cyber environment in the organisation to protect it from both internal and external threats. Therefore, there is a need to plan the implementation of cybersecurity framework keeping in mind the organisation command structures which needs to be strengthened to achieve the optimum results.

- **Coordination by HQ IDS**. The establishment of DCyA is a step in the right direction which will enhance the cyber security posture of armed forces however there is a requirement of having a regional presence at all command HQs which are very crucial for implementation of Cyber Security considering the proposed Theaterisation and plans for automation to optimise the force structures.

- **Arrest Adhocracy in IA**. The tendency to meet the contemporary challenges from within the existing means and resources must be curbed. It is vital to understand the nature of risk associated with the task and the seriousness it deserves.

- **Review Infrastructure available with IA.** The present infrastructure is insufficient and lacks the inherent capability to deter the possible cyber threats. It is therefore recommended that comprehensive roadmap for acquisition of modern infrastructure to upgrade the networks to optimally exploit technology for fight against cyber threats be implemented.

- **Interaction with Academia**. The academia and the youth play a vital role in the field of cyber operations. Hence it is necessary to make them partners in development of the right framework as also to create the necessary pool of cyber workforce motivated to join the Armed Forces.

- **Joint Training & Exercise**. It is evident from the past experience that the cyber threats are fast evolving and in order to keep ourselves abreast with the contemporary threats and also to learn and imbibe best practises there is a requirement for conducting joint training with best in the field to include the other advanced militaries and the academia.

- **Review of Command Structure**. The research highlights the requirement of improving the command structure for enhancing the efficiency and efficacy of cyber security operations in armed forces. It is therefore recommended that suitable changes be made to augment the command structure.

- **Periodic Review and Feedback**.It is recommended to establish a mechanism for conduct of periodic review in order to steer the right course to achieve the org goals as also to assess the efficacy of the system which will aid the org to gather valuable feedback to correct the course if required for enhancing the cyber hygiene of the organisation.

Conclusion

The adhocracy of Command Structure must be guarded against to provide a strong, effective and efficient framework for Cyber Security Operations in Indian Army. Cyber Security Command Structure of all three services of Indian Armed Forces should lay down the broad Framework for Cyber Security Operations. The Policies cater for Establishment of institutional mechanism at various organisational levels to meet the Cybersecurity Challenges. Despite these polices & guidelines, the coordinated action during Incident Response and Cyber Threat mitigation assumes an important role with regards to smooth coordination between Command Structures at Command HQ level (Theatre level) in the present volatile, uncertain complex and ambiguous (VUCA) cyber environment.

DISCLAIMER

The paper is author's individual scholastic articulation and does not necessarily reflect the views of CENJOWS. The author certifies that the article is original in content, unpublished and it has not been submitted for publication/ web upload elsewhere and that the facts and figures quoted are duly referenced, as needed and are believed to be correct.

References

1. Lumley, L. (2022). IT RISK IN THE WAKE OF ARMED CONFLICT operations. *The Banker,* , 31. Retrieved from https://www.proquest.com/trade-journals/risk-wake-armed-conflict-operations/docview/2676618484/se-2

2. Oyelami, J. O., & Azleena, M. K. (2020). Cyber security defence policies: A proposed guidelines for organisations cyber security practices. *International Journal of Advanced Computer Science and Applications, 11*(8) doi:https://doi.org/10.14569/IJACSA.2020.0110817

3. Georgiadou, A., Mouzakitis, S., Bounas, K., & Askounis, D. (2022). A cyber-security culture framework for assessing organization readiness. *The Journal of Computer Information Systems, 62*(3), 452-462. doi:https://doi.org/10.1080/08874417.2020.1845583

4. Kim, K., Alfouzan, F. A., & Kim, H. (2021). Cyber-attack scoring model based on the offensive cybersecurity framework. *Applied Sciences, 11*(16), 7738. doi:https://doi.org/10.3390/app11167738

5. Pesquera, C. R. (2016). *How to develop a stronger, more effective military cyber force* (Order No. 10112482). Available from Military Database. (1800536451). Retrieved from https://www.proquest.com/dissertations-theses/how-develop-stronger-more-effective-military/docview/1800536451/se-2

6. Alexander, D. (2012). Cyber threats in the 21st century. *Security, 49*(9), 70-70,72,74,76. Retrieved from https://www.proquest.com/trade-journals/cyber-threats-21st-century/docview/1223497697/se-2

7. Blessing, J. A. (2020). *The diffusion of cyber forces: Military innovation and the dynamic implementation of cyber force structure* (Order No. 28091801). Available from Military Database. (2450188085). Retrieved from https://www.proquest.com/dissertations-theses/diffusion-cyber-forces-military-innovation/docview/2450188085/se-2

8. Chandrashekhar, A. (2021, Mar 02). Chinese backed hackers targeted india's electricity companies during india-china standoff, says US cyber security firm [defence]. *The Economic Times* Retrieved from https://www.proquest.com/newspapers/chinese-backed-hackers-targeted-indias/docview/2494537843/se-2

9. Ray, A. (2020, Sep 19). Cyber security: Robust cyber infrastructure pivotal for india's digital economy push [Internet&Online]. *The Economic Times* Retrieved from https://www.proquest.com/newspapers/cyber-security-robust-infrastructure-pivotal/docview/2443916131/se-2

10. National cyber exercise underway to train govt officials on cyber threat. (2022, Apr 18). *Mint* Retrieved from https://www.proquest.com/newspapers/national-cyber-exercise-underway-train-govt/docview/2651834106/se-2

11. Sevastopulo, D. (2022). FBI director warns china espionage is greatest threat to US and allies. *FT.Com,* Retrieved from https://www.proquest.com/trade-journals/fbi-director-warns-china-espionage-is-greatest/docview/2700235543/se-2

12. Honey, T. M. (2021). *Leadership is what you need: An investigation into information security culture* (Order No. 28546752). Available from Publicly Available Content Database. (2572600539). Retrieved from https://www.proquest.com/dissertations-theses/leadership-is-what-you-need-investigation-into/docview/2572600539/se-2

13. Grassett, S. (2022). *Enhanced organizational security awareness: A qualitative study* (Order No. 29212930). Available from Publicly Available Content Database. (2680306355). Retrieved from https://www.proquest.com/dissertations-theses/enhanced-organizational-security-awareness/docview/2680306355/se-2

14. Valencia, G., Jr. (2022). *A correlation analysis of organizational commitment and support toward ISP compliance intention* (Order No. 29169202). Available from Publicly Available Content Database. (2662738663). Retrieved from https://www.proquest.com/dissertations-theses/correlation-analysis-organizational-commitment/docview/2662738663/se-2

15. Lt. General P.C. Katoch (Retd). (2021, Jul 06). Defence cyber command. *SP's Naval Forces,* Retrieved from https://www.proquest.com/magazines/defence-cyber-command/docview/2549926053/se-2

16. Chockalingam, S., & Maathuis, C. (2022). *An ontology for effective security incident management*. Reading: Academic Conferences International Limited. Retrieved from https://www.proquest.com/conference-papers-proceedings/ontology-effective-security-incident-management/docview/2681923668/se-2

17. DeVore, M. R., Orr, A., PhD., & Rossiter, A., PhD. (2022). Winning by outlasting: The united states and ukrainian resistance to russia. *Military Review, 102*(4), 11-22. Retrieved from https://www.proquest.com/trade-journals/winning-outlasting-united-states-ukrainian/docview/2697157734/se-2

18. CYBERSECURITY ADVISORY: UNDERSTANDING AND MITIGATING RUSSIAN STATE-SPONSORED CYBER THREATS TO US CRITICAL INFRASTRUCTURE. (2022). *Journal of Internet Law, 25*(6), 1-16. Retrieved from https://www.proquest.com/trade-journals/cybersecurity-advisory-understanding-mitigating/docview/2640797659/se-2

19. Chandrakanth, R. (2015, May 21). Cyber security, a looming global threat. *SP's MAI,* Retrieved from https://www.proquest.com/magazines/cyber-security-looming-global-threat/docview/1682200186/se-2.