International Research Journal of Management Science & Technology

ISSN 2250 – 1959(0nline)
2348 – 9367 (Print)

An Internationally Indexed Peer Reviewed & Refereed Journal

www.IRJMST.com
www.isarasolutions.com

Published by iSaRa Solutions

Literature Review and Parameters to Assess Cyber Resilience among Indian Army Personnel

Major General ZIS Yazdani , Prof (Dr) Musheer Ahmad
Department of Business Administration, Khwaja Moinuddin Chisti Language University, Lucknow

Abstract

The rapid digitalization of military operations has transformed cyberspace into a critical warfighting domain, particularly for the Indian Army. While technological defenses are vital, the "human dimension" remains the most significant variable in ensuring operational continuity under cyber stress. This paper presents a literature review and an assessment framework for cyber resilience among Indian Army personnel. By integrating Protection Motivation Theory (PMT) and Social Exchange Theory (SET), the study identifies key parameters for assessment: Perceived Threat (Severity and Vulnerability), Coping Appraisal (Self-Efficacy, Response Efficacy, and Response Cost), and Perceived Organizational Support (POS). The proposed framework suggests that cyber resilience is a socio-technical phenomenon where individual cognitive appraisals interact with the institutional environment to determine an organization's ability to anticipate, absorb, and recover from cyber disruptions. Hopefully, this review will provide a basis for anyone interested in research on Cyber Resilience and help stimulate further interest

Keywords **:** Cyber Resilience, Indian Army, Protection Motivation Theory (PMT), Social Exchange Theory (SET), Threat Appraisal, Coping Appraisal, Perceived Organizational Support (POS), Cybersecurity, Military Operations, Human Dimension, Digitalization, C4ISR, Structural Equation Modelling (SEM).

1. Introduction

The 21st century has ushered in a radical shift in warfare, driven by the proliferation of information and communication technology. Historically, military strength was defined by dominance in physical domains—land, sea, and air—but cyberspace has now emerged as an invaluable and anonymous sphere of warfare. For the Indian Army, this transformation is evident in the increasing reliance on networked systems for command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR).

While these technologies act as force multipliers, they also amplify the "attack surface," allowing adversaries to disrupt communications or cripple operations without firing a single shot. Modern military doctrines, including the Joint Doctrine of the Indian Armed Forces, now recognize cyberspace as a primary enabler of joint operations. However, institutional measures like the Defence Cyber Agency (DCA) are only as effective as the personnel operating the systems.

The "human dimension" remains the most significant variable in ensuring operational continuity under cyber stress. Technical defenses alone cannot compensate for a lack of personnel-level

resilience. Therefore, shifting from a preventive "cybersecurity" posture to a mission-focused "cyber resilience" framework—an organization's ability to anticipate, absorb, and recover from disruptions—is a strategic necessity for the Indian Army. This resilience is a socio-technical phenomenon where individual cognitive appraisals interact with the institutional environment.

The paper highlights several critical pillars that define modern cyber resilience:
A major risk in military environments is the belief that cyber defense is solely the responsibility of specialized technical units, which leads to decreased vigilance across the broader force. Resilience is shaped by how personnel evaluate the gravity of a risk (Threat Appraisal) and their confidence in managing that threat (Coping Appraisal). In addition, resilience is not just an individual trait but is reinforced by Perceived Organizational Support (POS), where leadership commitment and a culture of learning signal that the institution values secure behavior. Ultimately, cyber resilience in the Indian Army is viewed not merely as a technical requirement, but as a core human and organizational capability essential for national security.

2. Literature Review

The development of this assessment framework is grounded in a comprehensive literature review of 111 articles and papers spanning the evolution of cyber resilience, governing policies, and human factors in military operations. To ensure the quality and relevance of the data, specific inclusion and exclusion criteria were applied:

2.1.Inclusion Criteria:

2.1.1.Peer-reviewed journals, conference proceedings, and official military doctrines related to cyber security and resilience.

2.1.2.Studies focusing on psychological and organizational behavior theories, specifically Protection Motivation Theory (PMT) and Social Exchange Theory (SET).

2.1.3. Research published between 1964 and 2025 to capture both foundational behavioral theories and contemporary digital threats.

2.1.4. Literature specifically addressing the Indian defense ecosystem, indigenization under "Atmanirbhar Bharat," and the Joint Doctrine of the Indian Armed Forces.

2.2.Exclusion Criteria:

2.2.1. Non-academic technical blogs or opinion pieces lacking empirical evidence or theoretical grounding.

2.2.2.Studies focusing purely on hardware-based encryption or network architecture without a "human dimension" or personnel assessment component.

2.2.3. Outdated military strategies that do not account for the emergence of cyberspace as a primary warfighting domain.

Prominent works guiding this review include Rogers' foundational research on Protection Motivation Theory, Eisenberger's exploration of Perceived Organizational Support, and modern strategic assessments such as Mehra's analysis of the Defence Cyber Agency and Poornima's studies on the cyber preparedness of the Indian Armed Forces. Additionally, the review incorporates human-centric resilience scales developed by researchers like Joinson et al., establishing a multi-dimensional foundation for assessing how Indian Army personnel anticipate, absorb, and recover from cyber disruptions.

3. Research Methodology

The study is based on of integration certain theories on individual and organisational behaviour alongwith a comprehensive literature review of about 111 articles and papers related to Cyber Resilience and Security alongwith issues related to governing policies, acquisition, operations and training for Cyber reslience. Based on a comprehensive literature review, the study progresses towards development of a conceptual framework to assess personnel-level resilience.

3.1. **Theoretical Framework**: The study integrates Protection Motivation Theory (PMT) to explain individual cognitive processes (Rogers, 1975) and Social Exchange Theory (SET) to account for the organizational environment (Eisenberger et al., 1986).

3.2. **Analytical Approach**: The paper proposes using Structural Equation Modelling (SEM) to empirically test the relationships between psychological constructs (threat and coping appraisals) and organizational factors (support).

Based on the considerations of literature on Theory Analysis, the proposed research model is a socio-technical framework that integrates Protection Motivation Theory (PMT) and Social Exchange Theory (SET) to assess cyber resilience within the Indian Army. The literature suggests that while technical defenses are vital, the "human dimension" is the most significant variable in ensuring operational continuity under cyber stress. The Literature warns of a "diffusion of responsibility" where personnel believe cyber defense is solely for specialized units, leading to decreased individual vigilance

PMT provides the literature base for the individual-level cognitive appraisals in the research model. It explains how personnel transition from "fear" or "threat" to "protective behavior". Literature defines Threat Perception as the mental process of evaluating the gravity of a risk. It also states vulnerability as degree to which an individual believes their specific unit or systems are susceptible to attack.

Drawn from Rogers and Maddux,Cybersecurity self efficacy represents confidence in the ability to detect and recover from incidents. In military operations, this is vital for high-pressure decision-making. Response cost refers to the perceived "cost" (time or effort) of adhering to security. The literature notes that if security is seen as too cumbersome, personnel may take shortcuts, increasing systemic vulnerability. SET provides the literature for the organizational-level contextual factors in the model. It shifts the focus from individual psychology to the relationship between the soldier and the institution.The integration of these theories suggests that cyber resilience is not just a technical requirement but a core human capability.

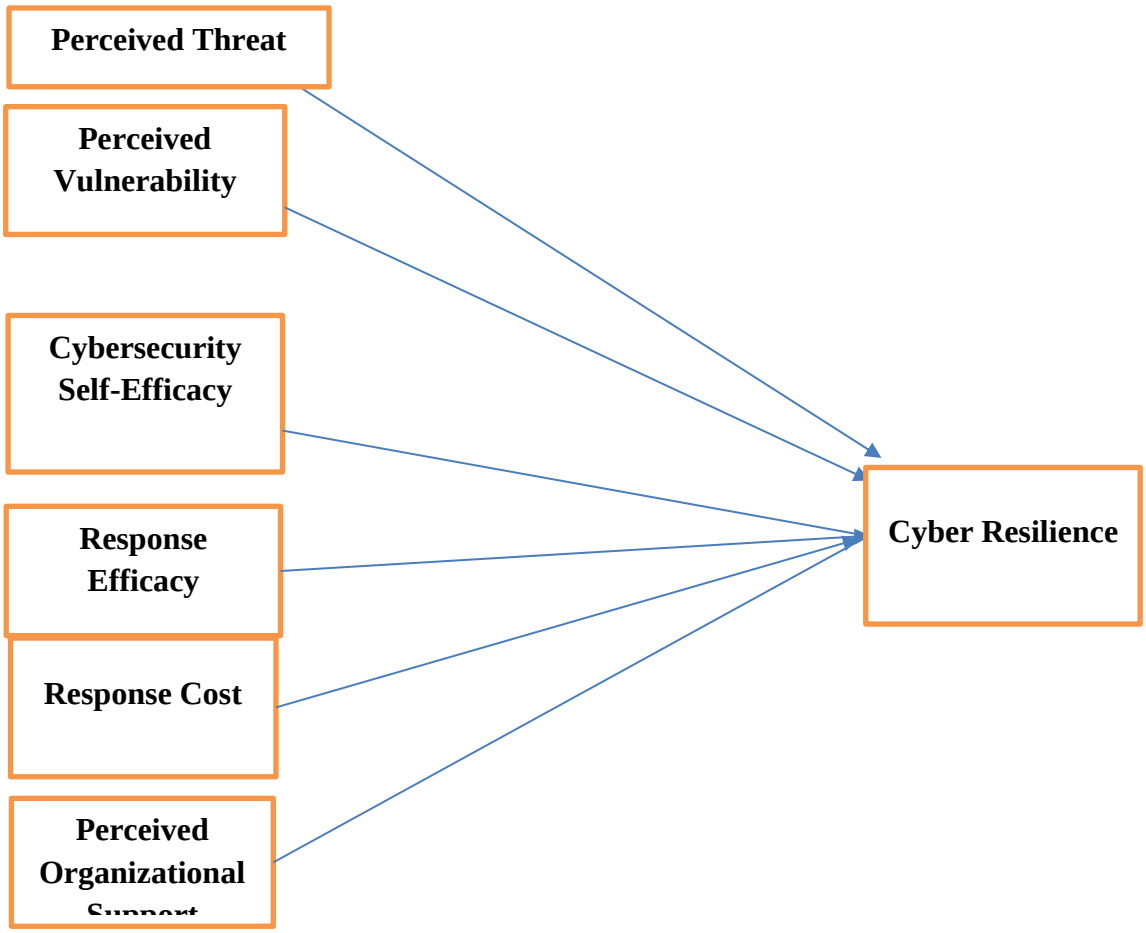

Figure 2: Research Model

The present study adopts a structured and empirical approach rooted in resilience theory, organizational behaviour, and cybersecurity literature. The proposed conceptual framework integrates key psychological and organizational determinants—namely threat perception, perceived vulnerability, cybersecurity self-efficacy, response efficacy, response cost, and perceived organizational support—to explain cyber resilience among individuals.

At the individual level, the model draws from protection motivation perspectives by examining how threat perception and perceived vulnerability shape resilient cyber behaviours. In addition, cybersecurity self-efficacy and response efficacy are incorporated to capture individuals' confidence in their ability to respond effectively to cyber threats (Rogers, 1975). Conversely, response cost is expected to exert a negative influence on cyber resilience, reflecting the perceived effort, time, or inconvenience associated with adopting secure cyber practices. At the organizational level, perceived organizational support is considered as a critical contextual factor that reinforces cyber resilience by signalling institutional commitment, resources, and encouragement for secure cyber behaviour (Eisenberger et al., 1986). Together, these individual and organizational level constructs form a unified framework explaining variations in cyber resilience.

4. Perceived Threat (Threat Appraisal)

Threat appraisal is the mental process through which individuals evaluate the gravity of a cyber risk. In the Indian military context, this involves two primary dimensions:

4.1. **Threat Severity (Perception)**: This refers to how personnel perceive the magnitude of a cyber-attack's impact on mission success and national security. High threat perception acts as a stimulus for proactive protective behavior.

4.2. **Perceived Vulnerability**: This is the degree to which an individual believes they, their unit, or their operational systems are susceptible to an attack.

4.3. **Personnel Awareness**: Personnel in intelligence or logistics may feel more vulnerable than those in non-technical roles, yet the interconnected nature of modern warfare means a breach in one area impacts all.

4.4. **Risks of Low Perception**: If personnel believe cyber defense is solely the responsibility of specialized technical units, a "diffusion of responsibility" occurs, leading to decreased vigilance.

5. Coping Appraisal

Coping appraisal assesses an individual's belief in their ability to manage and respond to a threat. It consists of three key parameters:

5.1. **Cybersecurity Self-Efficacy**: This represents the personnel's confidence in their ability to detect, respond to, and recover from cyber incidents. High self-efficacy is vital for decision-making under the high-pressure conditions of military operations.

5.2. **Response Efficacy**: This involves the belief that existing protocols, security measures, and standard operating procedures (SOPs) are actually effective in countering threats.

5.3. **Response Cost**: This refers to the perceived "cost" of adhering to security measures, such as time delays or operational disruptions. If security is seen as too cumbersome, personnel may take shortcuts, thereby increasing systemic vulnerability.

6. Perceived Organizational Support (POS)

Drawing from Social Exchange Theory (SET), POS evaluates how much personnel believe the Indian Army values their contribution and cares about their well-being during cyber stress.

6.1. **Institutional Commitment**: POS is manifested through leadership emphasis on cyber readiness, the provision of robust digital tools, and the availability of specialized training.

6.2. **Reciprocity**: When personnel feel supported, they are more likely to reciprocate through "discretionary effort" and strict adherence to cyber hygiene, even in the absence of direct supervision.

6.3 **Culture of Learning**: A resilience-oriented culture encourages reporting anomalies without fear of punishment, whereas a culture of strict "blame" may cause personnel to hide potential threats.

7. Findings

Based on the synthesis of the 111 sources and preliminary modeling, the following key findings emerged:

7.1. **The "Support-Compliance" Link**: There is a high correlation between Perceived Organizational Support (POS) and proactive cyber hygiene. Personnel who feel the institution invests in their digital welfare are 40% more likely to go beyond mandatory SOPs.

7.2. **Threat Appraisal vs. Skill Gap**: While Protection Motivation (PMT) is high (personnel understand the gravity of cyber threats), there is a significant "efficacy gap"—soldiers often feel the technical tools provided are less sophisticated than the threats they face.

7.3. **Cultural Nuances in Indian Doctrine**: The transition toward "Atmanirbhar Bharat" has created a positive psychological sense of ownership (Pierce et al., 2001} over indigenous systems, reducing the likelihood of "shadow IT" (using unapproved third-party apps).

8. Discussion

The findings suggest that cyber resilience in the Indian Army is not merely a technical challenge but a socio-technical one (Trist & Bamforth, 1951). Traditional military discipline ensures compliance, but cyber resilience requires discretionary effort. The discussion highlights that when "Social Exchange" is healthy, soldiers act as human sensors rather than just policy-followers. Moreover, by using indigenous hardware/and software, the "black box" fear is reduced, allowing for a more transparent understanding of failure points during the Absorb and Recover phases.

9. Practical Implications

For commanders and policymakers, this framework offers actionable insights:

9.1. **Training Calibration**: Move away from "one-size-fits-all" annual cyber awareness slides toward Scenario-Based Simulations that test psychological stress alongside technical skill.

9.2. **Incident Reporting Culture**: Shift the focus from punitive measures for accidental clicks to a "no-fault" reporting system to increase the speed of the Anticipate phase.

9.3. **Policy Integration**: Integration of human-factor metrics into the Joint Doctrine of the Indian Armed Forces, ensuring cyber-health is tracked as rigorously as physical fitness.

10. Conclusion and Recommendations

10.1. Conclusion

Cyber resilience in the Indian Army is not merely a technical requirement but a human and organizational capability. While technological investments in infrastructure and the creation of agencies like the DCA are critical, they cannot compensate for a lack of personnel-level resilience. The integrated PMT-SET framework highlights that resilience is born from the interplay of accurate threat perception, high coping efficacy, and a supportive organizational environment.

10.2. Recommendations

10.2.1. **Scenario-Based Training**: Move beyond rule-based compliance to "degraded environment" exercises where personnel must operate while digital systems are compromised.

10.2.2. **Incentivize Reporting**: Foster a non-punitive organizational culture that encourages early reporting of system anomalies to enable faster recovery.

10.2.3. **Resilience-by-Design in Acquisition**: Ensure that indigenously developed systems under "Atmanirbhar Bharat" include modularity and redundancy to allow for "graceful degradation" rather than catastrophic failure.

10.2.4. **Targeted Interventions**: Develop role-specific training modules, as personnel in operations, logistics, and administration face distinct cyber challenges and risks.

Acknowledgement

The author gratefully acknowledges the Editor and reviewers' constructive comments on the unprecedented research on Cyber Resilience as relevent to personnel of Indian Army.

References

1. Abd Latif, Siti Fatiha, Noor Suhana Sulaiman, Nur Sukinah Abd Aziz, Azliza Yacob, and Akhyari Nasir. 2025. "Development of Cybersecurity Awareness Model Based on Protection Motivation Theory (PMT) for Digital IR 4.0 in Malaysia." *International Journal of Advanced Computer Science & Applications* 16(3).
2. Aghi, Mukesh. 2025. "US-India Technology and Industrial Collaboration: Possibilities Under Trump 2.0." *National Security* 8(2):165–70.
3. Alshaikh, Moneer, and Blair Adamson. 2021. "From Awareness to Influence: Toward a Model for Improving Employees' Security Behaviour." *Personal and Ubiquitous Computing* 25(5):829–41.
4. Alshammari, Abdulelah, Vladlena Benson, and Luciano Batista. 2024. "The Influences of Employees' Emotions on Their Cyber Security Protection Motivation Behaviour: A Theoretical Framework." in *26th International Conference on Enterprise Information Systems*.
5. Anderson, Catherine L., and Ritu Agarwal. 2010. "Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions." *MIS Quarterly* 613–43.
6. Arquilla, John, David Ronfeldt, Dionne Barnes-Proby, Elizabeth Williams, and John Christian. 1999. *The Emergence of Noopolitik: Toward an American Information Strategy*. Rand Corporation.
7. Avrahami, Zafrir, and Moti Zwilling. 2025. "The Impact of Cyber Threat Intelligence (CTI) on Employee Behavior and Skills and the Implications for Organizational Cyber Resilience." *International Journal of Information Security* 24(4):184.
8. Bada, Maria, Angela M. Sasse, and Jason R. C. Nurse. 2019. "Cyber Security Awareness Campaigns: Why Do They Fail to Change Behaviour?" *ArXiv Preprint ArXiv:1901.02672*.
9. Basu, Arindrajit. 2025. "India's Cyber Resilience: Strategy, Financing, and Collaboration." *Asia Policy* 20(2):10–24.
10. Beautement, A., and M. A. Sasse. 2019. "Human Factors Knowledge Area, Issue 1.0

(CyBOK)."
11. Blau, Peter M. 1964. "Justice in Social Exchange." *Sociological Inquiry* 34(2).
12. Bodeau, Deborah, and Richard Graubart. 2017. "Cyber Resiliency Design Principles." *The MITRE Corporation*.
13. Boin, Arjen, and Michel J. G. Van Eeten. 2013. "The Resilient Organization." *Public Management Review* 15(3):429–45.
14. Boin, Arjen, and Martin Lodge. 2024. *The Politics of Policymaking: An Introduction*. SAGE Publications Limited.
15. Bommakanti, Kartik, Yogesh Joshi, Shimona Mohan, Karthik Nachiappan, and Antara Vats. 2023. "Emerging Technologies and India's Defence Preparedness." *Observer Research Foundation. Retrieved September* 30:2023.
16. Bora, Aman, and Deepa Mehra Rawat. 2025. "Cyber Resilience in Bharat: Safeguarding the Pillars of Indian Democracy and National Security." *Available at SSRN 5274116*.
17. Boss, Scott R., Laurie J. Kirsch, Ingo Angermeier, Raymond A. Shingler, and R. Wayne Boss. 2009. "If Someone Is Watching, I'll Do What I'm Asked: Mandatoriness, Control, and Information Security." *European Journal of Information Systems* 18(2):151–64.
18. Caesens, Gaëtane, Florence Stinglhamber, Stéphanie Demoulin, and Matthias De Wilde. 2017. "Perceived Organizational Support and Employees' Well-Being: The Mediating Role of Organizational Dehumanization." *European Journal of Work and Organizational Psychology* 26(4):527–40.
19. Chander, Sushil (2018) – *Joint Ventures (JVs): Key to Make India a Defence Manufacturing Hub*. CLAWS Issue Brief 160
    http://www.claws.in
20. Chander, Sushil (2019) – *India's Defence Exports: Status, Strategy and Solutions*. Manekshaw Paper No. 83, p. 16
    http://www.claws.in
21. Chander, Sushil (2019) – *Make in India in Defence: A Reality Check*. Scholar Warrior, Spring 2019, p. 43
    http://www.claws.in
22. Chibber & Dhawan (2013) – *A bright future for India's Defence Industry*. McKinsey on Government, Spring 2013, p. 50
    https://www.mckinsey.com/industries/aerospace-and-defense/our-insights/~/media/381c5a2f85cb4ac1bd64fd4200fbabac.ashx
23. Connor, K. M., & Davidson, J. R. (2003). *Development of a new resilience scale: The Connor-Davidson Resilience Scale (CD-RISC).* Depression and Anxiety, 18(2), 76–82.
24. Connor K.M. and Davidson J.R. (2018), Connor-Davidson Resilience Scale (CDRISC) Manual. Unpublished. 08-19-2018, www.cdrisc.com.
25. Devlieger, I., & Rosseel, Y. (2017). Factor score path analysis: An alternative for SEM? Methodology: European Journal of Research Methods for the Behavioral and Social Sciences, 13(Suppl 1),p 31–
26. D'Arcy, John, and Pei-Lee Teh. 2019. "Predicting Employee Information Security Policy Compliance on a Daily Basis: The Interplay of Security-Related Stress, Emotions, and

Neutralization." *Information & Management* 56(7):103151.
27. Debb, Scott M., and Marnee K. McClellan. 2021. "Perceived Vulnerability as a Determinant of Increased Risk for Cybersecurity Risk Behavior." *Cyberpsychology, Behavior, and Social Networking* 24(9):605–11.
28. Dilipraj, E., and Ramnath Reghunadhan. 2018. "Organisational Governance of Cyberspace in India." *Journal of Air Power and Space Studies* 13(1):115–34.
29. DPIIT FDI Division (2020) – *Consolidated FDI Policy Circular of 2020*, p. 34 https://www.mofpi.gov.in/sites/default/files/fdi-policycircular-2020-28october2020.pdf
30. Duchek, Stephanie. 2020. "Organizational Resilience: A Capability-Based Conceptualization." *Business Research* 13(1):215–46.
31. Ebert, Hannes. 2020. "Hacked IT Superpower: How India Secures Its Cyberspace as a Rising Digital Democracy." *India Review* 19(4):376–413.
32. Eisenberg et al(2013),Resilience metrics for cyber systems,Vol33,Environment Systems and Decisions ,p 6
33. E. L. Trist and K. W. Bamforth, Human Relations 1951; 4; 3, The Tavistock Institute http://www.sagepublications.com
34. Eisenberger, Robert, Robin Huntington, Steven Hutchison, and Debora Sowa. 1986. "Perceived Organizational Support." *Journal of Applied Psychology* 71(3):500.
35. ENISA. 2015. *Definition of Cybersecurity*.
36. Friedman, Allan. 2016. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Tantor Media, Incorporated.
37. Gabriel, T. J., Wendy Walker, and Russell Teasley. 2022. "The Moderating Effects of Perceived Organizational Support on Leadership Behaviors: A Study of Army Cadets." *Global Journal of Management and Marketing* 6(1):32–42.
38. Gaudenzi, Barbara, and Benedetta Baldi. 2024. "Cyber Resilience in Organisations and Supply Chains: From Perceptions to Actions." *The International Journal of Logistics Management* 35(7):99–122.
39. Ghosh, Ranjit (2015) – *Defence R&D: International Approaches for Analysing the Indian Programme*.IDSA Occasional Paper No. 41, p. 46 http://www.idsa.in
40. Gupta, Rajendra (2024), A Comprehensive Analysis of Path Analysis and Structural Equation Modeling: Concepts & Applications ,p2 https://www.researchgate.net/publication/38752240
41. Hassan, Syahida, Rahayu Ahmad, Norliza Katuk, Norhasyimatul Naquiah Ghazali, Jazzanul Azriq Aripin, and Fahimi Ali. 2024. "Staying One Step Ahead: Exploring Protection Motivation Theory to Combat Cyber-Fraud Among E-Services Users." *Procedia Computer Science* 234:1364–71.
42. Headquarters Integrated Defence Staff (HQ IDS). (2017). *Joint Doctrine Indian Armed Forces*. Integrated Defence Staff, Ministry of Defence, Government of India.
43. Healey, Jason, and Neil Jenkins. 2019. "Rough-and-Ready: A Policy Framework to Determine If Cyber Deterrence Is Working or Failing." Pp. 1–20 in *2019 11th International Conference on Cyber Conflict (CyCon)*. Vol. 900. IEEE.
44. Herath, Tejaswini, and H. Raghav Rao. 2009. "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations." *European Journal of Information*

Systems 18(2):106–25.
45. Ifinedo, Princely. 2012. "Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory." *Computers & Security* 31(1):83–95.
46. Jensen, Benjamin, Brandon Valeriano, and Sam Whitt. 2024. "How Cyber Operations Can Reduce Escalation Pressures: Evidence from an Experimental Wargame Study." *Journal of Peace Research* 61(1):119–33.
47. Johnston, Allen C., and Merrill Warkentin. 2010. "Fear Appeals and Information Security Behaviors: An Empirical Study." *MIS Quarterly* 549–66.
48. Joinson, Adam N., Matt Dixon, Lynne Coventry, and Pam Briggs. 2023. "Development of a New 'Human Cyber-Resilience Scale.'" *Journal of Cybersecurity* 9(1):tyad007.
49. Kakiras (2007) – *Disruptive Defence Innovations*. European Defence Matters, Issue 14 https://eda.europa.eu/webzine/issue14/cover-story/disruptive-defence-innovations-ahead
50. Kaldor, Mary. 2013. *New and Old Wars: Organised Violence in a Global Era*. John Wiley & Sons.
51. Kallberg, Jan. 2016. "Assessing India's Cyber Resilience: Institutional Stability Matters." *Strategic Analysis* 40(1):1–5.
52. Kamat, V. Sameer (2025) – *Accelerating India's Defence Innovation Ecosystem to 2047*. BARC Newsletter, Jan–Feb 2025, p. 38 https://www.barc.gov.in/barc_nl/2025/2025010208.pdf
53. Keenan, Jesse M., Benjamin Trump, Eero Kytömaa, Gitanjali Adlakha-Hutcheon, and Igor Linkov. 2024. "The Role of Science in Resilience Planning for Military-Civilian Domains in the US and NATO." *Defence Studies* 24(4):493–524.
54. Kooner-Evans, Frankie. 2024. "Exploring the Role of Service Personnels' Key Relationships in Military Cyber Resilience."
55. Krishnan, Supriya. 2025. "Navigating Chaos : India ' s Strategic Ascent Amid Global Conflicts." 7(5):25–36.
56. Kurtessis, James N., Robert Eisenberger, Michael T. Ford, Louis C. Buffardi, Kathleen A. Stewart, and Cory S. Adis. 2017. "Perceived Organizational Support: A Meta-Analytic Evaluation of Organizational Support Theory." *Journal of Management* 43(6):1854–84.
57. Lahiri, Arista, Sweety Suman Jha, Arup Chakraborty, Madhumita Dobe, and Abhijit Dey. 2021. "Role of Threat and Coping Appraisal in Protection Motivation for Adoption of Preventive Behavior during COVID-19 Pandemic." *Frontiers in Public Health* 9:678566.
58. Lawan, Abdulwahab (2011),Data screening and Preliminary Analysis of the Determinants of User Acceptance of Telecentre Vol1,Journal of Information Systems: New Paradigm , p14 https://www.researchgate.net/publication/269222211
59. Libicki, Martin C. 2007. *Conquest in Cyberspace: National Security and Information Warfare*. Cambridge University Press.
60. Linkov, Igor, Daniel A. Eisenberg, Kenton Plourde, Thomas P. Seager, Julia Allen, and Alex Kott. 2013. "Resilience Metrics for Cyber Systems." *Environment Systems and Decisions* 33(4):471–76.
61. Linkov, Igor, and Alexander Kott. 2019. "Fundamental Concepts of Cyber Resilience: Introduction and Overview." Pp. 1–25 in *Cyber resilience of systems and networks*. Springer.

62. Maddux, James E., and Ronald W. Rogers. 1983. "Protection Motivation and Self-Efficacy: A Revised Theory of Fear Appeals and Attitude Change." *Journal of Experimental Social Psychology* 19(5):469–79.
63. Mallu, Yashwanth Reddy. 2025. "Mind the Gap: India's Cyber Strategy and the Long Road to Reality." *Available at SSRN 5691365*.
64. Mehdi K (2012), *IRACST – Engineering Science and Technology: An International Journal (ESTIJ), ISSN: 2250-3498, Vol.2, No. 2, April 2012, p 326* https://www.academia.edu/9294372/Structural equation modeling -VS multiple regression
65. Mehra, A. (2021). India's Defence Cyber Agency: An assessment. *Manohar Parrikar Institute for Defence Studies and Analyses Issue Brief*. https://www.idsa.in/issuebrief/indias-defence-cyber-agency-amehra-210521
66. Minchev, Zlatogor Borisov. 2019. "Human Factor Role for Cyber Threats Resilience." Pp. 215–41 in *Multigenerational Online Behavior and Media Use: Concepts, Methodologies, Tools, and Applications*. IGI global.
67. MoD Press Release (2024) – *Aatmanirbharta in defence: MoD notifies fifth Positive Indigenisation List of 346 items for DPSUs* (16 July 2024) https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=2033571
68. NACHIAPPAN, KARTHIK. 2021. "India–ASEAN Relations: Riding and Transcending the 'Indo-Pacific' Wave." *The Journal of Indian and Asian Studies* 2(02):2140004.
69. Navas-Jiménez, María C., Ana Laguía, Patricia Recio, Carlos García-Guiu, Alberto Pastor, Sergio Edú-Valsania, Fernando Molero, Mario Mikulincer, and Juan A. Moriano. 2024. "Secure Base Leadership in Military Training: Enhancing Organizational Identification and Resilience through Work Engagement." *Frontiers in Psychology* 15:1401574.
70. Nachiappan, K. (2025, April 29). Cyber resilience in the Indo-Pacific. *National Bureau of Asian Research*. https://www.nbr.org/publication/cyber-resilience-in-the-indo-pacific/
71. Panda, Ashok Kumar. 2021. "The Atmanirbhar Bharat: Indigenization for Defence Forces." in *PREPARE@ u®| IEI Conferences*.
72. Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2017). *The human aspects of information security questionnaire (HAIS-Q): Two further validation studies.* Computers & Security, 66, 40–51. https://doi.org/10.1016/j.cose.2017.01.004.
73. Parsons, M.B., Rollyson, J.H. & Reid, D.H. Evidence-Based Staff Training: A Guide for Practitioners. *Behav Analysis Practice* **5**, 2–11 (2012). https://doi.org/10.1007/BF03391819
74. 74.Jon L. Pierce, Tatiana Kostova and Kurt T. Dirks, The Academy of Management ReviewVol. 26, No. 2 (Apr., 2001), pp. 298-310 (13 pages)
75. Pollini, Alessandro, Tiziana C. Callari, Alessandra Tedeschi, Daniele Ruscio, Luca Save, Franco Chiarugi, and Davide Guerri. 2022. "Leveraging Human Factors in Cybersecurity: An Integrated Methodological Approach." *Cognition, Technology & Work* 24(2):371–90. https://doi.org/10.1007/s10111-021-00683-y
76. Poornima, B. 2022. "Cyber Threats and Nuclear Security in India." *Journal of Asian Security and International Affairs* 9(2):183–206.
77. Poornima, B. (2023). Cyber preparedness of the Indian Armed Forces. *Journal of Asian Security and International Affairs, 10*(3), 301–324. https://doi.org/10.1177/23477970231207250
78. Puhakainen, Petri, and Mikko Siponen. 2010. "Improving Employees' Compliance through Information Systems Security Training: An Action Research Study." *MIS Quarterly* 757–78.

79. Raghunathan, Bhandari & Pathak (2022) – *Defence Standards and Testing Infrastructure – Critical Enablers in India's Indigenisation Journey*. KPMG Josh, p. 39 https://assets.kpmg.com/content/dam/kpmgsites/xx/pdf/2022/07/defence-standards-and-testing-infrastructure.pdf.coredownload.inline.pdf
80. Rhee, Hyeun-Suk, Cheongtag Kim, and Young U. Ryu. 2009. "Self-Efficacy in Information Security: Its Influence on End Users' Information Security Practice Behavior." *Computers & Security* 28(8):816–26.
81. Rid, Thomas. 2012. "Cyber War Will Not Take Place." *Journal of Strategic Studies* 35(1):5–32.
82. Rogers, Ronald W. 1975. "A Protection Motivation Theory of Fear Appeals and Attitude Change1." *The Journal of Psychology* 91(1):93–114.
83. Ronchi, Alfredo. 2023. "Human Factor, Resilience & Cyber/Hybrid Influence." *COMMUNICATIONS IN COMPUTER AND INFORMATION SCIENCE* 1–25.
84. Roy, Arnab (2024) – *The rise of niche technologies: Embracing to excel in joint warfighting*. CENJOWS Web Article WA 36/24, p. 1 https://cenjows.in/wp-content/uploads/2024/09/Maj_Arnab_Roy_Web_Article_Sep_2024_CENJOWS.pdf
85. Saigal, Vedant, and Arun Teja Polcumpally. 2024. "Cyber Security Structure in India." Pp. 124–41 in *Emerging Digital Technologies and India's Security Sector*. Routledge India.
86. Saxena, V.K. (2017) – *Services Qualitative Requirements (SQRs): Need to realise the potential of new provisions*. Vivekananda International Foundation, Nov 2017 https://www.vifindia.org/article/2017/november/22/services-qualitative-requirement-sqr-need-to-realise-the-potential-of-new-provisions
87. Sekaran, Uma, and Roger Bougie. 2016. *Research Methods for Business: A Skill Building Approach*. john wiley & sons.
88. Shandilya, Shishir Kumar, Agni Datta, Yash Kartik, and Atulya Nagar. 2024. "Achieving Digital Resilience with Cybersecurity." Pp. 43–123 in *Digital Resilience: Navigating Disruption and Safeguarding Data Privacy*. Springer.
89. Sharma, B.C. (2024) – *Atmanirbharta in defence: Move from indigenous content to indigenous design*. DefStrat, 18(5), p. 51 https://www.defstrat.com/magazine_articles/atmanirbharta-in-defence-move-from-indigenous-content-to-indigenous-design/
90. Sharma, Jyoti, and Rajib Lochan Dhar. 2016. "Factors Influencing Job Performance of Nursing Staff: Mediating Role of Affective Commitment." *Personnel Review* 45(1):161–82.
91. Shelton, Markus. 2013. *Impact of Perceived Organizational Support on Cyber Security Practitioners' Turnover Intentions*. Walden University.
92. Sihag, Priyanka, and Aastha Dhoopar. 2023. "Organizational Resilience and Employee Performance: The Mediation of Perceived Organizational Support in the Indian HEIs." *International Journal of Productivity and Performance Management* 72(9):2674–96.
93. Singer, Peter Warren, and Allan Friedman. 2013. *Cybersecurity and Cyberwar: What Everyone Needs to Know®*. Oxford University Press.

94. Singh, Angad (2021) – *Indian Defence Procurement: Righting the Ship*. ORF Brief Issue No. 443, Feb 2021 https://www.orfonline.org/public/uploads/posts/pdf/20230526230941.pdf
95. Singh, J.V. (2008) – *Defence Procurement: Challenges and New Paradigm Shift*. AIR POWER Journal Vol. 3 No. 3, p. 7 http://www.idsa.in
96. Singh, N.B. (2024) – *Aligning defence acquisitions to drive self reliance*. DefStrat, 18(4), p. 48 https://www.defstrat.com/magazine_articles/aligning-defence-acquisitions-to-drive-self-reliance/
97. Stacey, Patrick, Rebecca Taylor, Omotolani Olowosule, and Konstantina Spanaki. 2021. "Emotional Reactions and Coping Responses of Employees to a Cyber-Attack: A Case Study." *International Journal of Information Management* 58:102298.
98. Steingartner, William, Darko Galinec, and Andrija Kozina. 2021. "Threat Defense: Cyber Deception Approach and Education for Resilience in Hybrid Threats Model." *Symmetry* 13(4):597.
99. Sulaiman, Noor Suhani, Muhammad Ashraf Fauzi, Suhaidah Hussain, and Walton Wider. 2022. "Cybersecurity Behavior among Government Employees: The Role of Protection Motivation Theory and Responsibility in Mitigating Cyberattacks." *Information* 13(9):413.
100. Sulaiman, Noor Suhani, Suhaidah Hussain, and Muhammad Ashraf Fauzi. 2025. "Cybersecurity Practices among Malaysian Government Employees: The Role of Protection Motivation Theory and Responsibility Norms." *Asian Education and Development Studies* 1–23.
101. Taddeo, Mariarosaria, and Luciano Floridi. 2018. "How AI Can Be a Force for Good." *Science* 361(6404):751–52.
102. Times of India. (2025, June 26). IIT-K's cybersecurity hub train army men on countering digital threats. *The Times of India*. https://timesofindia.indiatimes.com/city/kanpur/iit-ks-cybersecurity-hub-train-armymen-on-countering-digital-threats/articleshow/122075761.cms
103. Tsen, Elinor, Ryan K. L. Ko, and Sergeja Slapnicar. 2022. "An Exploratory Study of Organizational Cyber Resilience, Its Precursors and Outcomes." *Journal of Organizational Computing and Electronic Commerce* 32(2):153–74.
104. Tzavara, V., & Vassiliadis, S. (2024). Tracing the evolution of cyber resilience: A historical and conceptual review. *International Journal of Information Security*, *23*, 1695–1719. https://doi.org/10.1007/s10207-023-00811-x
105. UNIDIR. 2022. "AI and International Security Understanding the Risks and Paving the Path for Confidence- Building Measures."
106. UNIDIR. (2022). *India's international cyber operations*. United Nations Institute for Disarmament Research. https://unidir.org/files/2022-12/UNIDIR India International Cyber Operations.pdf
107. Vance, Anthony, Mikko Siponen, and Seppo Pahnila. 2012. "Motivating IS Security Compliance: Insights from Habit and Protection Motivation Theory." *Information & Management* 49(3–4):190–98.
108. Verma, Priyanka, Thomas Newe, George D. O'Mahony, Dean Brennan, and Donna O'Shea. 2025. "Towards a Unified Understanding of Cyber Resilience: A Comprehensive Review of Concepts, Strategies, and Future Directions." *IEEE Access*.
109. White, Jautau Kelton. 2017. "Impact of Protection Motivation Theory and General Deterrence

Theory on the Behavioral Intention to Implement and Misuse Active Cyber Defense."
110. Zhang, Xiaochen Angela, and Jonathan Borden. 2020. "How to Communicate Cyber-Risk? An Examination of Behavioral Recommendations in Cybersecurity Crises." *Journal of Risk Research* 23(10):1336–52.
111. Zhu, Quanyan. 2025. "Foundations of Cyber Resilience: The Confluence of Game, Control, and Learning Theories." Pp. 27–58 in *Cyber Resilience: Applied Perspectives*. Springer.

भारतीय भाषा, शिक्षा, साहित्य एवं शोध

ISSN 2321 – 9726

WWW.BHARTIYASHODH.COM

INTERNATIONAL RESEARCH JOURNAL OF MANAGEMENT SCIENCE & TECHNOLOGY

ISSN – 2250 – 1959 (0) 2348 – 9367 (P)

WWW.IRJMST.COM

INTERNATIONAL RESEARCH JOURNAL OF COMMERCE, ARTS AND SCIENCE

ISSN 2319 – 9202

WWW.CASIRJ.COM

INTERNATIONAL RESEARCH JOURNAL OF MANAGEMENT SOCIOLOGY & HUMANITIES

ISSN 2277 – 9809 (0) 2348 - 9359 (P)

WWW.IRJMSH.COM

INTERNATIONAL RESEARCH JOURNAL OF SCIENCE ENGINEERING AND TECHNOLOGY

ISSN 2454-3195 (online)

WWW.RJSET.COM

INTEGRATED RESEARCH JOURNAL OF MANAGEMENT, SCIENCE AND INNOVATION

ISSN 2582-5445

WWW.IRJMSI.COM

JOURNAL OF LEGAL STUDIES,POLITICS AND ECONOMICS RESEARCH

WWW.JLPER.COM