International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(17s) 2026 pp. 800-808
https://doi.org/10.70917/ijcisim-2026-4798
Article

THE SIGNIFICANCE OF HUMAN RESOURCES IN MILITARY CYBER DEFENSE INTEROPERABILITY IN SUPPORT OF NATIONAL DEFENSE

Immer H. P. Butarbutar[1], Rudy Agus Gemilang Gultom[2], R. Djoko Andreas Navalino[3], Susilo Adi Purwantoro[4]

[1] Defense Science Study Program, Postgraduate School, Republic of Indonesia Defense University, Indonesia
[2,3,4] Republic of Indonesia Defense University, Indonesia
Email: immerbutarbutar2@gmail.com

Abstract: Rapid technological development and growing dependence on digital data have made cyber threats increasingly complex and diverse. The strategic value of digital data has encouraged a wide range of actors to seek unauthorized access to data centers belonging to individuals, organizations, and states. Recent incidents cited in the source manuscript include Brain Cipher ransomware attacks affecting Indonesia's National Data Center and cyber incidents involving security and defense institutions. In the defense domain, cyberspace has become a new operational arena for targeting adversary information systems, while modern military equipment and infrastructure increasingly rely on digital systems and artificial intelligence. Consequently, cyber defense depends not only on technology but also on the quality and readiness of the personnel who operate it. This study examines the significance of human resources in military cyber defense interoperability in support of national defense. The research was conducted within the Indonesian Ministry of Defence, Indonesian National Armed Forces Headquarters, and the armed services. A qualitative approach was employed to address the research question concerning the significance of human resources in military cyber defense interoperability. The study uses Soft Systems Methodology (SSM) as the principal methodological approach, supported by NVivo, PESTEL, and SWOT analyses. The analytical framework draws on national defense theory, human resource management theory, the concept of interoperability, and the concept of cyber defense. The findings indicate that human resources play a highly significant role in enabling military cyber defense interoperability and, consequently, in strengthening national defense capacity.
Keywords: human resources; interoperability; military cyber defense; national defense; cyber security

1. Introduction

The contemporary global strategic environment is characterized by what Owen Jacobs describes as VUCA—volatility, uncertainty, complexity, and ambiguity. Volatility reflects the rapidly changing and dynamic nature of the strategic environment, in which change frequently occurs in unpredictable ways (Pangestu, 2020). Rapid environmental shifts create substantial uncertainty in the strategic landscape. Complexity arises from the dense interrelationships among strategic actors and variables, while ambiguity complicates planning and decision-making because causal patterns and established assumptions are often unclear (Putra & Hakim, 2016).

Competition over energy, food, and water resources has become increasingly intense as global population growth places greater pressure on resource availability. This condition adds to the complexity of global competition and encourages states to strengthen their capacity for survival and resilience. At the same time, advances in artificial intelligence and big data have become significant components of the strategic environment. Such technological

developments represent tangible challenges that may shape the projection of power in the twenty-first century and beyond (Lee, 2021). Across sectors, enormous volumes of information are continuously generated and processed as big data. Advances in computing and internet technologies have likewise accelerated, contributing to the emergence of cyber warfare as a new domain of conflict (Vashishtha, 2018).

These developments have also broadened the national security paradigm beyond conventional territorial defense to include the protection of citizens in the digital sphere. A fundamental obligation of the state is to provide security for its population, including protection from various forms of cybercrime and cyber-enabled threats (Yusuf Perwej, 2022).

Limited cyber operations have repeatedly been attributed to state actors and may be interpreted as tests of capability, while the evolution of cyber conflict indicates preparation for larger and more sophisticated forms of warfare. The source manuscript traces this evolution from the 1990s to 2020 through a sequence of attack techniques, including internet-based social engineering, network sniffing, packet spoofing, session hijacking, automated probes and scans, graphical-user-interface intrusion tools, automated large-scale attacks, denial-of-service attacks, executable-code attacks against browsers, vulnerability analysis without source code, attacks on DNS infrastructure, abuse of NNTP for attack distribution, stealth and advanced scanning techniques, remotely controlled Windows Trojans such as Back Orifice, malicious-code propagation through email, large-scale Trojan distribution, distributed attack tools, distributed denial-of-service (DDoS) attacks, targeted attacks against specific users, anti-forensic techniques, large-scale worm propagation, and sophisticated command-and-control attacks (Matthew N. O. Sadiku, 2020).

Indonesia has progressively strengthened its policy attention to cyber warfare and cyber defense. The Ministry of Defence has conducted seminars and workshops involving ministries and non-ministerial government agencies, universities, experts, and other stakeholders to formulate an integrated information-technology system for addressing cyber-based information warfare. This initiative was framed within the concept of a Cyber Defense System. On 23 October 2012, the Minister of Defence established a Cyber Defense Working Team chaired by the Director General of Defense Potential and supported by relevant Ministry of Defence units, ministries/non-ministerial agencies, universities, experts, and cyber-community representatives. The team was tasked with formulating a national defense strategic roadmap related to cyber threats and preparing the establishment of a national-scale cyber defense organization. This process was subsequently reinforced through Minister of Defence Regulation No. 82 of 2014 on Cyber Defense (Kemenhan RI, 2014), which addresses four core elements: policy, institutions, technology/infrastructure, and human resources.

2. Literature Review

According to the American Management Association, Human Resource Management (HRM) is a field of management concerned with planning, organizing, and controlling operational functions for acquiring, developing, maintaining, and effectively utilizing the workforce. Its central objective is to optimize the use of human resources for both organizational and individual interests. HRM is therefore important for improving work efficiency, maintaining constructive relationships between organizations and employees, responding to competition, and sustaining organizational existence in highly competitive environments.

HRM is inherently multidisciplinary and draws on economics, psychology, sociology, and law. Its principal activities include human resource planning, human resource policy, salary and benefits administration, human rights and labor-law compliance, recruitment, selection, orientation, performance management, staff training and development, communication, and counseling.

In the context of cyber defense, HRM responsibilities extend to ensuring that recruitment and selection assess candidates not only on technical competence but also on integrity and cyber-security awareness. Thorough background screening is therefore important for reducing risks associated with insider threats. Effective and comprehensive HRM practices are likewise essential for strengthening organizational data security. Cyber-security training should be

incorporated into orientation programs for new personnel, while continuous training is needed to ensure that personnel remain informed about emerging threats and current data-security practices.

This study uses an appropriate qualitative research approach and several theoretical perspectives as analytical lenses to examine the relationship between human resource management and the organizational requirements of cyber defense.

3. Research Method

This study employs a qualitative research approach to examine phenomena under natural conditions, with the researcher serving as a key research instrument. Qualitative research seeks to explain phenomena through in-depth data collection and emphasizes the depth and detail of the evidence obtained (Sugiyono, 2005). The research design applies Secondary Data Analysis (SDA) using material collected from multiple media and information sources, including scientific journals, books, electronic media, newspapers, and online sources (Creswell, J., 2014). As stated in the source manuscript, the broader analytical process also incorporates interview material and questionnaire responses, with Soft Systems Methodology (SSM) as the principal methodological framework and NVivo, PESTEL, and SWOT analyses as supporting approaches. The study is situated within the Indonesian Ministry of Defence, Indonesian National Armed Forces Headquarters, and the armed services, focusing on the significance of human resources for military cyber defense interoperability.

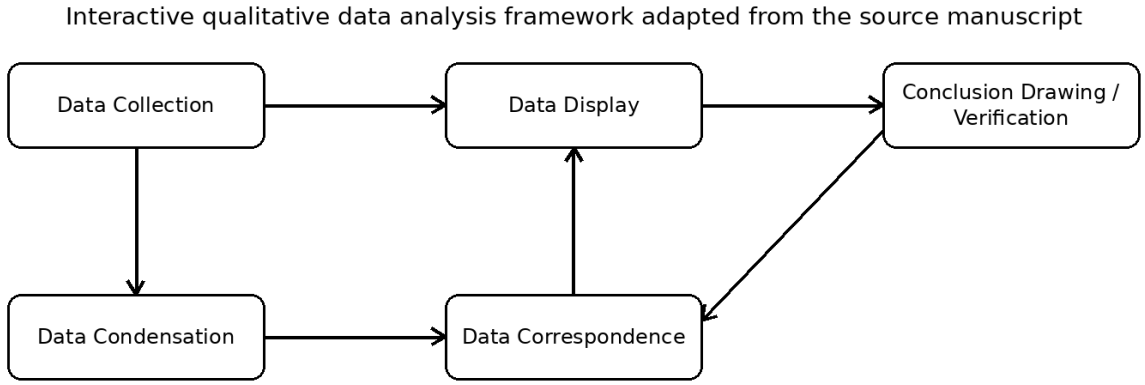

Figure 1. Qualitative data analysis process based on the Miles–Huberman and Spradley techniques as represented in the source manuscript.

4. Results

NVivo analysis of informant interviews concerning the significance of human resources in military cyber defense interoperability identified three major themes: (1) the current condition of the operational interoperability model, (2) the operational interoperability process currently in place, and (3) the expected operational interoperability model.

4.1 Current Operational Interoperability Model

The data indicate that inter-agency collaborative structures have already been established, but they continue to face both technical and institutional constraints. The principal issues include continuously evolving cyber threats, weak technological interoperability, and procedural gaps among institutions. Several enabling mechanisms are already available, including official communication channels and coordination forums, but they have not yet been utilized to their full potential.

4.2 Existing Operational Interoperability Process

Current collaboration is implemented through formal coordination, intelligence-information exchange, and limited joint operations. The findings indicate that process effectiveness is strongly affected by the speed of data sharing, the consistency of security protocols, and the degree of information openness among participating institutions. Key constraints include real-time data sharing, network security, and system compatibility across institutions.

4.3 Expected Operational Interoperability Model

Informants described the preferred model as an integrated system combining cyber defense technology, shared situational awareness, and joint operational command. The principal expectations are as follows:

Standardization of platforms and communication protocols.

An early-warning system based on joint intelligence.

Application of the Anti-Access/Area Denial (A2/AD) concept to strengthen control of cyber and physical domains.

An integrated management principle combining technological capability, trained human resources, and adaptive policy.

The final NVivo data-processing output in the source manuscript is summarized in Figure 2, which links the current collaborative model, collaborative process, and expected model with thematic nodes derived from the informants.

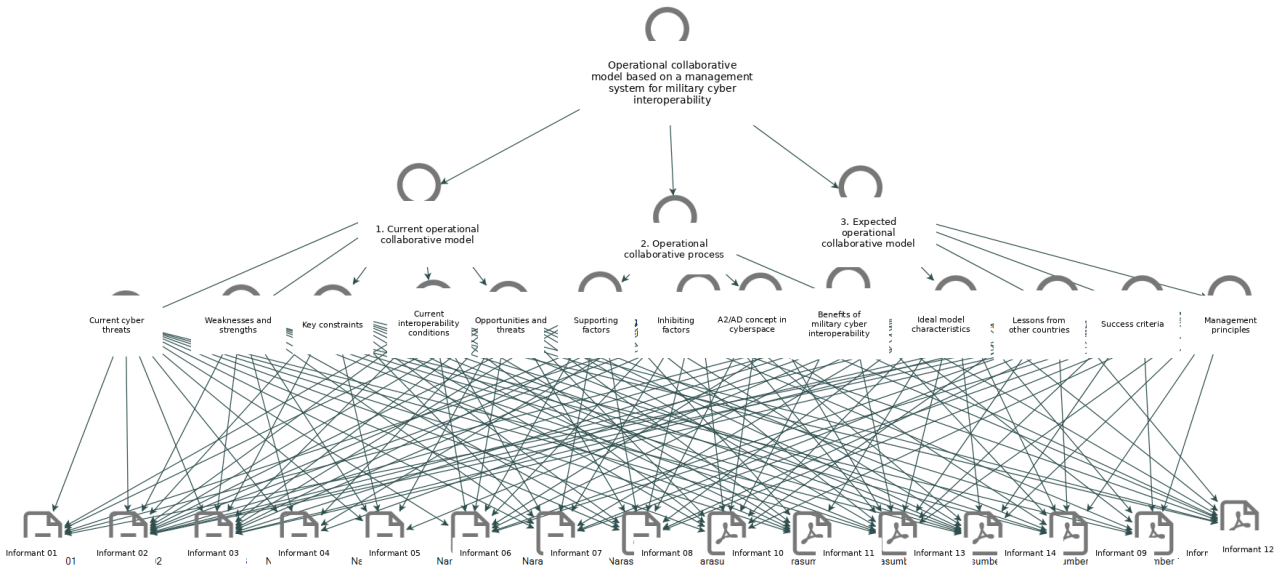

Figure 2. NVivo-based thematic network of operational collaboration and military cyber interoperability (translated from the source manuscript).

5. Discussion

HRM faces a range of challenges that are particularly relevant to military cyber defense, including globalization, changing workforce dynamics, diversity management, work–life balance, and organizational attitudes toward labor representation. HRM is important because it directly influences the quality of services delivered by an organization; weak HRM can contribute to weak organizational performance. In the twenty-first century, effective knowledge management can generate competitive advantage because institutional knowledge is created, retained, and applied through the workforce.

A number of states have established specialized cyber units within their defense and security institutions. These organizations consolidate efforts to defend networks, respond to hostile cyber activity, and strengthen cyber operational capability. The growth of cyber military forces reflects the fact that cyber conflict is no longer confined to virtual simulation or fiction but has become an integral component of contemporary strategic competition. Cyberspace is often described as a fifth dimension of warfare alongside land, sea, air, and outer space because technological innovation is transforming modern military tactics and making the cyber domain a frontline operational environment. This development also has implications for future military doctrine, as advances in information and communication technology are likely to shape the evolution of military strategy.

Cyber-based military defense is particularly important for Indonesia because a growing proportion of strategic infrastructure and public services depends on information systems, digital technology, and internet-connected networks. This dependence creates exposure to threats, disruptions, and attacks affecting energy transmission and distribution systems, air-defense systems, transportation systems, public services, banking, defense, and other critical sectors.

In the digital era, HRM is therefore central to organizational cyber security. As cyber threats become more complex, HRM must develop effective strategies for strengthening personnel awareness and knowledge of cyber-security risks. Continuous training and professional development are essential for building a strong security culture and reducing the likelihood and impact of cyber incidents.

The cyberattack on Indonesia's national data center, as cited in the source manuscript, illustrates the importance of data security and the consequences of weaknesses in cyber-protection systems. Such incidents compel organizations to reassess the strategies used to safeguard data. HRM has a significant role in supporting organizational response, recovery, and mitigation because cyber resilience depends on both technical systems and the readiness of the people who operate them.

To address continuously evolving cyber threats, HRM should work closely with information-technology teams and organizational management to review and update cyber-security policies. This collaboration is essential because HRM manages people and organizational behavior, whereas IT teams possess the technical expertise needed to identify system vulnerabilities and threat patterns. Lessons derived from cyber incidents should be incorporated into updated policies, procedures, and security protocols. Following an incident, comprehensive evaluation should identify vulnerabilities and inform measures designed to prevent recurrence. HRM must also ensure that such updates are communicated effectively so that personnel understand their responsibilities for protecting organizational data.

In addition to strategic coordination, emergency-response training is a key element of organizational preparedness for cyber incidents. HRM should design and implement training programs that prepare personnel to respond rapidly and effectively during cyber emergencies. Such programs should cover incident reporting, initial response procedures, and appropriate escalation protocols. Personnel also need a clear understanding of indicators of cyberattack and the immediate actions required to minimize potential impact. With adequate preparation, employees and military personnel can function as an effective first line of defense, reducing response time and limiting the damage caused by cyber incidents.

Transparent communication is equally important during crisis situations. HRM should ensure that information regarding cyber incidents, organizational response measures, and policy changes is communicated clearly to personnel and other stakeholders. Transparent communication helps reduce misinformation, uncertainty, and anxiety while demonstrating organizational integrity and concern for stakeholders. Where relevant, external stakeholders should also receive appropriate information regarding incidents and measures undertaken to restore and protect affected data.

Human personnel are among the principal assets of cyber security and play a decisive role in cyber defense. A central challenge in implementing cyber defense is therefore the availability of competent personnel who can respond rapidly to a cyber environment that changes alongside technological and social developments. Human-resource development strategies should consequently be supported by continuous competency-development programs.

5.1 National Defense Theory

Defense constitutes an essential national requirement and a recognizable expression of state sovereignty. Within the state, defense develops in relation to the political system and the execution of national defense functions. In general terms, defense refers to the capacity to resist attack. National defense can therefore be understood as an effort to minimize potential threats to the state through the continuous development and modernization of national defense capabilities. Its basic principles include medium- and long-term defense priorities and measures undertaken both in peacetime and when national security is threatened.

Within an anarchic international system, where no sovereign central authority exists above the state (Jervis, 1978, p. 167), states remain concerned about threats from other states while pursuing their national interests. This condition can produce a security dilemma that encourages arms competition as well as defense cooperation as forms of self-defense. States consequently seek defense capabilities sufficient to deter or overcome potential attacks.

Indonesia's 2015 Defence White Paper describes national defense as involving all citizens and national resources and as operating comprehensively across national life. Indonesia's defense is based on the Total Defense System (Sistem Pertahanan Semesta), which combines military and non-military defense to build robust national defense strength and capability. Defense preparedness is developed continuously to address both actual and potential threats.

National defense theory is used in this study as a framework for analyzing how states strengthen military capability, develop defense strategy, preserve territorial integrity, respond to rapid global change, deter threats, and pursue national interests. In Indonesia, early and comprehensive defense preparation requires optimal use of national resources. However, this system must also be adapted to increasingly complex and technologically enabled threats, including cyber threats. Military modernization is therefore important because a defense system that depends only on the mass mobilization of resources, without modern capabilities and effective operational capacity, risks consuming resources without achieving strategic objectives.

5.2 Human Resource Management Theory

Human Resource Management is a core management function. Whereas management broadly focuses on achieving organizational objectives through people, HRM focuses specifically on people as organizational actors and resources. Effective HRM seeks to increase the contribution of personnel toward organizational objectives. Edwin B. Flippo, as cited in Malayu Hasibuan, defines personnel management in terms of planning, organizing, directing, and controlling the procurement, development, compensation, integration, maintenance, and separation of employees in order to achieve organizational, individual, employee, and societal objectives. The HRM challenges identified by Mathis and Jackson, as cited in Subheki, include the following:

Economic and technological change.

Availability and quality of the workforce.

Growth of contingent or non-permanent employment.

Demographic issues.

Work–family balance.

Organizational restructuring and mergers/acquisitions.

Taken together, these perspectives indicate that HRM is an effort to manage the workforce as an organizational asset in order to achieve effectiveness and efficiency while addressing constraints that may affect organizational objectives.

According to Chaplin, ability encompasses capacity, skill, agility, talent, or competence that enables an individual to perform an action. Robbins distinguishes ability as either an innate capacity or a capability developed through training and practice.

Slameto further describes ability as competence that includes the capacity to confront and adapt to new situations rapidly and effectively, to understand and use abstract concepts effectively, and to recognize and learn responses quickly.

On this basis, ability can be understood as the competence or potential to master a skill, whether innate or developed through training and practice, and to apply it through action. Individuals differ in their levels of ability, and these differences influence the potential each person brings to organizational tasks. This perspective is relevant to cyber defense because personnel capability must be matched with technological and operational requirements (Wijanarka, Musani, & Bayu D., 2022).

5.3 Interoperability Concept

The Federal Research Division, as cited by Kom and McDaniel (2020), defines interoperability as the capacity to exchange information across and among people, processes, and negotiations in a manner characterized by a shared understanding of the information exchanged. This capacity depends on integrated equipment and resources, agreed and documented procedures, and alignment across culture, language, motivation, and politics. Interoperability is also closely related to the use of technology. Presidential Instruction No. 3 of 2003 identifies activities directly associated with electronic data processing, information management, management systems, work processes, and the use of information technology to improve public-service accessibility.

Two distinctions are particularly important. First, interoperability is not the same as integration. Interoperability strengthens loosely connected systems without requiring them to remain continuously connected, because a particular system may only be required to support a specific operation (Mansyur et al., 2019). Second, interoperability does not require complete homogeneity. Different systems do not need to be merged merely because their devices or programming are similar. In this study, the concept of interoperability is used to analyze the gap between the ideal condition of information-system interoperability and actual operational conditions.

Within Indonesia's cyber defense, particularly the military cyber domain, the source manuscript identifies an interoperability gap among the Ministry of Defence, Indonesian National Armed Forces Headquarters, and the armed services in relation to organizational arrangements, competency standards for cyber personnel, and the equipment and infrastructure required for operations.

5.4 Cyber Defense Concept

Cyber-security threats can emerge in many forms and at different levels of severity. Artificial intelligence (AI) has the potential to play an increasingly important role in military prevention, operational enhancement, and cyber security. In 2016, U.S. Cyber Command Commander Admiral Michael Rogers argued before the U.S. Senate Armed Services Committee that relying solely on human intelligence in cyberspace constituted a losing strategy. Traditional cyber-security systems may depend heavily on historical similarities with known malicious code, whereas AI-enabled technologies can be trained to identify anomalies across broader network patterns and thereby provide more dynamic defense against attacks (Macri, 2016). This development reinforces the growing significance of cyber warfare as a national defense concern.

The source manuscript identifies ransomware, social engineering, and malicious insider activity as major categories of digital attack capable of affecting society. It also cites the 2022 Conti ransomware incident affecting Bank Indonesia and a 2017 incident involving the Ministry of Finance that disrupted national tax-service and communication systems. The manuscript further discusses the expansion of digital-asset and non-fungible-token markets and notes the potential need for law-enforcement institutions to address possible misuse of emerging technologies for financial crime.

Scientific and technological progress has also transformed the security and defense sector. Contemporary defense systems increasingly depend on digital technologies capable of protecting or concealing military capabilities and of transmitting sensor assessments directly to weapon systems with satellite support. One widely discussed concept is Anti-Access/Area Denial (A2/AD), which has conceptual roots in efforts to prevent stronger opponents from gaining access to or freedom of movement within a defended area.

A2/AD generally refers to defensive tactics that prioritize prevention or the construction of defenses capable of resisting attacks by a stronger opponent. To defend national sovereignty and conduct effective countermeasures, defense and attack planning must coordinate national defense resources in an integrated manner. The source manuscript cites the armed conflict in Nagorno-Karabakh between Armenia and Azerbaijan as an illustration of the growing role of technology in contemporary warfare (Syafi'i, Supriyadi, Prihantoro, & Gultom, 2023).

6. Conclusion

The analysis demonstrates that advances in science and technology generate complex implications for human life and interstate relations. Since internet-based communication became central to modern society, conventional boundaries established through international practice have become increasingly blurred in cyberspace. Over the past two decades, cyber war has become a persistent international security concern and has been associated with the potential to intensify interstate tension and threaten peace (Pawankumar Sharma, 2022).

Against this background, Human Resource Management in support of cyber defense constitutes a highly strategic and significant component of national defense. Effective management of qualified personnel can maximize the contribution of military cyber capabilities in responding to cyber-domain threats and in protecting state sovereignty, territorial integrity, and the security of the population. The study therefore concludes that the human-resource dimension is indispensable to military cyber defense interoperability and cannot be treated as secondary to technology or infrastructure.

7. Recommendations

Effective cyber defense depends on collaboration among technological capability, sound organizational design, and appropriate human resource management. Accordingly, the preparation of personnel with qualifications aligned to military cyber-defense requirements should be treated as a primary institutional priority.

The source manuscript identifies the following general requirements for human-resource development in cyber-defense organizations:

Human resource recruitment should include psychological assessment of mental readiness and suitability for cyber-defense roles. Required characteristics include the ability to perform under pressure, high integrity, discipline, strong learning capacity, and compliance with established standards. Recruitment requirements should be periodically reviewed to accommodate technological change and evolving national cyber-defense needs. Competency analysis should cover the scope of duties, required knowledge and skills, additional requirements for operational effectiveness, and the design of professional career pathways in cyber defense.

Selected personnel should possess competencies appropriate to their placement and assignment, including the required knowledge and skills, and should receive clear and sustainable career development within the cyber-defense organization.

For specialized tasks that are confidential and strategically sensitive, selected personnel should have an employment or service status consistent with the principles of defense organization, particularly for offensive cyber tasks or operations conducted under conditions of cyber warfare.

REFERENCES

Books

1. Arikunto, S. (2006). Prosedur Penelitian: Suatu Pendekatan Praktik. Jakarta: PT Rineka Cipta.

2. Bandur, A. (2019). Penelitian Kualitatif: Studi Multi-Disiplin Keilmuan dengan NVivo 12 Plus. Bogor: Penerbit Mitra Wacana Media.
3. Creswell, J. W., & Creswell, J. D. (2018). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches (5th ed.). SAGE Publications.
4. C. Verhaak, R., & Haryono Imam. (1991). Filsafat Ilmu. Jakarta: Gramedia.
5. Daft, R. L., Murphy, J., & Willmott, H. (2013). Organization Theory and Design. London: Cengage Learning Inc.
6. Jervis, R. (1978). Cooperation under the security dilemma. World Politics, 167–214.
7. Kom, J., & McDaniel, N. (2020). Military Interoperability: Definitions, Models, Actors, and Guidelines. Library of Congress; CGHE, Uniformed Services University.
8. Miles, M. B., & Huberman, A. M. (1984). Analisis Data Kualitatif (T. R. Rohidi, Trans., 1992). Jakarta: Penerbit Universitas Indonesia.
9. Pangestu, L. G. (2020). Strategi Indonesia Mewujudkan ASEAN Outlook on Indo-Pacific (AOIP) untuk Menciptakan Stabilitas di Kawasan Indo-Pasifik. UPN Veteran Jakarta, Fakultas Ilmu Sosial dan Ilmu Politik, Hubungan Internasional, 11–27.
10. Siagian, S. P. (2009). Manajemen Sumber Daya Manusia. Jakarta: Bumi Aksara.
11. Subheki, A., & Jauhar, M. (2012). Pengantar Sumber Daya Manusia (MSDM). Jakarta: Prestasi Pustaka.
12. Sugiyono. (2010). Metode Penelitian Pendidikan: Pendekatan Kuantitatif, Kualitatif, dan R&D. Bandung: Alfabeta.
13. Sugiyono. (2014). Metode Penelitian Kuantitatif, Kualitatif, dan Kombinasi (Mixed Methods). Bandung: Alfabeta.
14. Supriyatno, M. (2014). Tentang Ilmu Pertahanan. Jakarta: Yayasan Pustaka Obor.
15. Tippe, S. (2016). Ilmu Pertahanan: Sejarah, Konsep, Teori, dan Implementasi. Jakarta: Salemba Humanika.
16. Vashistha, P. (2018). Big Data Analytics Techniques: A Survey. India: Grupta Vishal.

Journal Articles

17. Jervis, R. (1978). Cooperation under the security dilemma. World Politics, 167–214.
18. Sadiku, M. N. O., Fagbohungbe, O. I., & Musa, S. M. (2020). International Journal of Engineering Research and Advanced Technology (IJERAT), 6(5). https://doi.org/10.31695/IJERAT.2020.3612
19. Putra, I. N., & Hakim, A. (2016). Analisa peluang dan ancaman keamanan maritim Indonesia sebagai dampak perkembangan lingkungan strategis. Asrojurnal-STTAL, 6.
20. Perwej, Y., Abbas, S. Q., Dixit, J. P., Akhtar, N., & Jaiswal, A. K. (2022). A systematic literature review on cyber security. International Journal of Scientific Research and Management, 9(12), 669–710. https://doi.org/10.18535/ijsrm/v9i12.ec04

Electronic Source

21. Macri, G. (2016). NSA Chief Says Without Artificial Intelligence, Cyber 'Is a Losing Strategy'. Retrieved from the web source listed in the original manuscript.