Vol 1 No 1 2024 || E-ISSN xxxx-xxxx

The Journal of Academic Science

journal homepage:
https://thejoas.com/index.php/

Strategic Defense: How Intellectual Capital Shapes Threat Management and System Configurations

Hani Sirine
Department of Management, Universitas Kristen Satya Wacana, Indonesia
Email: hani.sirine@uksw.edu

KEYWORDS
Domain Knowledge, Formal Knowledge, Management Experience, Intrinsic Motivation, Creativity, Threat Management, System Reconfigurations, Strategic Defense

ABSTRACT
This study investigates the impact of domain knowledge, formal knowledge, management experience, and intrinsic motivation and creativity on managing threats and reconfigurations in strategic defense organizations. Utilizing Structural Equation Modelling (SEM) with SmartPLS 4.096, data were collected from 200 entrepreneurs. The findings reveal that while domain knowledge did not significantly influence threat management and reconfigurations, formal knowledge, management experience, and intrinsic motivation and creativity had significant positive effects. These results underscore the importance of structured education, seasoned leadership, and innovative thinking in enhancing organizational resilience and adaptability. The study contributes to the Knowledge-Based View (KBV) theory by differentiating the impacts of various knowledge dimensions and highlighting the critical role of intrinsic motivation and creativity. Practical implications suggest that strategic defense organizations should prioritize continuous professional development, foster experienced leadership, and cultivate a culture of innovation. Future research should explore interdisciplinary knowledge integration, technological synergies, and the long-term impacts of these factors on organizational performance. This study provides valuable insights into optimizing defense strategies in dynamic and complex environments.

1. INTRODUCTION

In the contemporary landscape of strategic defense, the rapid evolution of threats necessitates a robust and adaptable approach to threat management and system configurations. The increasing complexity and sophistication of threats, ranging from cyber-attacks to unconventional warfare, demand a continuous reassessment of strategic and operational frameworks. Organizations must leverage their intellectual capital to maintain a competitive edge and ensure national security (Huber et al., 2016). Intellectual capital, defined as the collective knowledge, experience, and creativity of individuals within an organization, plays a pivotal role in shaping strategic responses and reconfigurations (Tamirat & Amentie, 2023; Tasnim & Singh, 2016). Recent studies have emphasized the significance of intellectual capital in enhancing organizational performance, particularly in environments characterized by rapid change and high uncertainty (Buenechea-Elberdin et al., 2018; Inkinen, 2015). This study focuses on how specific components of intellectual capital—domain knowledge, formal knowledge, management experience, and intrinsic motivation and creativity—contribute to effective threat management and the reconfiguration of

defense systems.

Despite the recognized importance of intellectual capital in organizational performance and strategic management, there is a paucity of research specifically examining its impact on threat management and system configurations in the context of strategic defense. Prior research has predominantly focused on the general benefits of intellectual capital, such as improved innovation and competitive advantage (Del Giudice & Della Peruta, 2016; Giudice & Maggioni, 2014; Secundo et al., 2017). However, limited attention has been given to its specific components—domain knowledge, formal knowledge, management experience, and intrinsic motivation and creativity—and their direct influence on strategic defense operations. Moreover, existing literature often overlooks the dynamic interplay between these components and their collective impact on organizational agility and resilience in the face of evolving threats. For instance, while some studies have explored the role of knowledge management in enhancing organizational resilience (Centobelli et al., 2017; Cerchione & Esposito, 2017), they have not sufficiently addressed how different types of intellectual capital interact to support strategic defense initiatives. This gap in the literature necessitates a focused investigation into how these elements influence strategic defense operations.

Additionally, the rapid advancements in technology and the increasing integration of artificial intelligence and machine learning in defense strategies have transformed the nature of intellectual capital required for effective threat management (Sivarajah et al., 2017). Despite this, there is a lack of empirical evidence on how defense organizations can leverage these technological advancements in conjunction with intellectual capital to enhance their strategic capabilities. The dearth of comprehensive studies that examine the multifaceted role of intellectual capital in strategic defense, particularly in the context of managing and reconfiguring systems to address contemporary threats, underscores the need for this research. This study aims to fill this gap by providing a detailed analysis of how various components of intellectual capital contribute to threat management and system configurations in strategic defense.

The primary research problem addressed in this study is the lack of empirical evidence and theoretical understanding of how different facets of intellectual capital shape threat management and system reconfigurations in strategic defense organizations. Given the dynamic and complex nature of modern threats, strategic defense organizations require a nuanced understanding of how to effectively leverage their intellectual capital. Existing studies have highlighted the general advantages of intellectual capital (Del Giudice & Della Peruta, 2016), but have not delved deeply into its specific components and their practical applications in defense settings. The absence of this targeted insight presents a significant challenge for strategic defense organizations seeking to enhance their operational effectiveness and adaptability.

The objectives of this research are multifaceted and aim to bridge the identified gaps in the existing literature:

1. To examine the role of domain knowledge in enhancing the identification and understanding of potential threats, and its impact on the development of specialized and effective responses.
2. To analyze the influence of formal knowledge on the application of theoretical frameworks to practical situations in strategic defense, and its role in ensuring compliance with

established standards and protocols.
3. To investigate the impact of management experience on decision-making under pressure, resource coordination, and the implementation of strategic initiatives in response to emerging threats.
4. To explore the influence of intrinsic motivation and creativity on proactive problem-solving and innovative thinking in the face of new and unpredictable threats.

By achieving these objectives, the study aims to provide a comprehensive understanding of how intellectual capital can be harnessed to improve threat management and system configurations, thereby enhancing the strategic capabilities of defense organizations. This research will offer valuable insights for policymakers and defense leaders, guiding the development of strategies that leverage intellectual capital for improved security and operational effectiveness.

The Knowledge-Based View (KBV) of the firm is a theoretical framework that posits knowledge as the most strategically significant resource within an organization (Öhman et al., 2021). This perspective extends the Resource-Based View (RBV) by emphasizing the role of knowledge in gaining and sustaining a competitive advantage (Tamirat & Amentie, 2023). KBV suggests that firms are heterogeneous entities laden with unique knowledge assets that determine their performance and strategic direction (R. Grant & Phene, 2022; Pereira & Bamel, 2021; Stoian et al., 2024).

Intellectual capital is a vital component of the KBV, encompassing the collective knowledge, skills, and capabilities of an organization's workforce (Rindermann et al., 2015). In this research, intellectual capital is categorized into four dimensions: domain knowledge, formal knowledge, management experience, and intrinsic motivation and creativity. Domain knowledge refers to specialized expertise and understanding in a particular field or industry. It is crucial for identifying new opportunities and making informed decisions based on a deep understanding of specific contexts. Domain knowledge enables organizations to navigate industry-specific challenges and leverage niche markets. Formal knowledge encompasses the educational background and professional qualifications of employees. This includes degrees, certifications, and formal training that provide a foundational understanding of various subjects. Formal knowledge equips individuals with the theoretical and practical insights necessary to perform their roles effectively (Becker, 1964). Management experience pertains to the practical wisdom and insights gained through years of leadership and managerial roles. It includes strategic decision-making, team leadership, and the ability to guide organizations through complex situations. Management experience contributes to organizational stability and strategic direction (Mintzberg, 1973). Intrinsic motivation and creativity refer to the internal drive and innovative capacity of individuals within the organization. Intrinsic motivation fosters engagement and a commitment to excellence, while creativity leads to the generation of novel ideas and solutions. Together, these elements are vital for continuous innovation and problem-solving (Amabile, 1996).

Each of these components plays a distinct yet interconnected role in contributing to an organization's success. Organizations that effectively manage and exploit their knowledge assets can cross functional team relationship more effectively (Cabrita et al., 2015). This involves recognizing emerging trends, understanding customer needs, and developing innovative solutions that address market demands (Suherman, 2017). The KBV

framework provides a comprehensive understanding of how different forms of intellectual capital contribute to these processes, highlighting the strategic importance of knowledge management (Morales-Huamán et al., 2023; Naim & Lenka, 2018). The Knowledge-Based View (KBV) offers a robust theoretical foundation for understanding the strategic significance of intellectual capital in organizations. By emphasizing the critical role of knowledge in achieving competitive advantage, KBV underscores the importance of managing and leveraging intellectual assets effectively. Intellectual capital is a multifaceted construct that encompasses the knowledge, skills, and relationships within an organization (Andreeva & Garanina, 2016). It plays a critical role in driving innovation, improving financial performance, and facilitating organizational learning. By understanding and leveraging the dimensions of intellectual capital—domain knowledge, formal knowledge, management experience, and intrinsic motivation and creativity—organizations can enhance their competitive advantage and achieve long-term success.

The capability to manage threats and reconfigure systems effectively is paramount for strategic defense organizations. The rapid evolution of security threats necessitates a proactive and well-informed approach to threat management. Domain knowledge, defined as the specialized knowledge and expertise in a specific area, is critical in this context. It equips individuals and organizations with the ability to understand and anticipate threats, thus enhancing their capacity to respond and adapt strategically. Domain knowledge plays a crucial role in the identification of potential threats. Individuals with deep expertise in specific areas can recognize subtle indicators of emerging threats that may be overlooked by those with less specialized knowledge. For instance, in the realm of cybersecurity, domain experts can identify vulnerabilities and potential attack vectors that are not apparent to generalists (Ahsan et al., 2022; Li & Liu, 2021). This heightened awareness and understanding enable organizations to implement pre-emptive measures, thereby mitigating risks before they escalate into significant threats.

Beyond threat identification, domain knowledge is instrumental in devising effective response strategies. Experts with in-depth knowledge of a particular domain can develop targeted and effective countermeasures tailored to the specific nature of the threat. For example, experts in biological threats can design precise containment and mitigation strategies based on their understanding of pathogen behaviour and transmission (J. Y. Lee et al., 2020). This specialized approach ensures that responses are not only swift but also appropriately tailored to the threat, thereby enhancing their effectiveness. In addition to threat management, domain knowledge is critical for system reconfigurations. The ability to reconfigure systems in response to evolving threats requires a thorough understanding of both the system's capabilities and the nature of the threat. Domain experts can identify the necessary adjustments and modifications to existing systems to enhance their resilience and effectiveness. For instance, in military defense, knowledge of advanced weaponry and tactics allows for the optimization of defense systems to counteract new forms of aggression (Kianto et al., 2017).

Empirical studies have underscored the importance of domain knowledge in managing threats and reconfigurations. Ahsan et al., (2022) and Li & Liu, (2021) found that organizations with a high level of domain-specific knowledge were more effective in

identifying and mitigating cyber threats. Similarly, research by Lee et al., (2020) highlighted the critical role of domain expertise in managing biological threats, emphasizing that specialized knowledge leads to more effective containment and response strategies. Moreover, Andreeva & Garanina, (2016) and Buenechea-Elberdin et al., (2018) demonstrated that domain knowledge significantly contributes to the successful reconfiguration of defense systems, allowing organizations to adapt to changing threat landscapes. Studies by Kianto et al., (2017) and Delgado-Verde et al., (2011) further support these findings, showing that organizations with strong intellectual capital, particularly domain-specific knowledge, are better equipped to innovate and adapt to new threats. Additionally, research by Khalique et al., (2015) emphasizes the importance of domain knowledge in small and medium enterprises, which can be extrapolated to larger defense organizations given the similar need for specialized knowledge and adaptability. Based on the theoretical insights and empirical evidence, the following hypothesis is proposed:

H1: Domain Knowledge Positively Has Significant Impact to Managing Threats and Reconfigurations

Formal knowledge, acquired through structured education, training programs, and professional development, is a critical asset in strategic defense. It provides individuals with the theoretical foundations and systematic methodologies needed to address complex problems effectively. In the context of managing threats and system reconfigurations, formal knowledge equips defense professionals with the skills to apply standardized procedures, leverage advanced technologies, and adhere to best practices, thereby enhancing organizational resilience and adaptability.

Formal knowledge plays a pivotal role in threat management by enabling defense professionals to systematically analyse and respond to threats. Training programs and educational curricula in fields such as cybersecurity, counterterrorism, and risk management provide the necessary theoretical and practical knowledge to identify, assess, and mitigate threats (Alavi, 2016; Alavi & Wahab, 2013; Setti et al., 2022). For example, formal education in cybersecurity equips professionals with the knowledge to understand complex attack vectors, implement robust security protocols, and respond to breaches effectively (Ben Salamah et al., 2023; Gutiérrez-Martínez & Duhart, 2019; Reddy & Dietrich, 2017). Moreover, formal knowledge fosters a culture of continuous learning and improvement, ensuring that defense personnel remain up to date with the latest developments in their fields. This ongoing education is crucial for maintaining high levels of preparedness and ensuring that organizations can adapt to new and evolving threats (Cepeda-Carrion et al., 2017).

The application of formal knowledge in developing effective response strategies is well-documented. For instance, formal training in emergency management and crisis response provides defense professionals with standardized procedures and protocols that can be swiftly deployed in crisis situations (Bundy et al., 2017). These procedures are designed based on empirical research and best practices, ensuring that responses are both effective and efficient. Formal knowledge also facilitates the integration of advanced technologies into threat response strategies. Training programs often include modules on the use of cutting-edge technologies, such as artificial intelligence and machine learning, which can enhance threat detection and response capabilities (Sivarajah et al., 2017). By leveraging these technologies, defense organizations can improve their ability

to anticipate and counteract threats in real-time. In addition to threat management, formal knowledge is essential for the successful reconfiguration of defense systems. Reconfiguring systems to address new threats requires a deep understanding of both the technological and operational aspects of these systems. Formal education and training provide the foundational knowledge necessary to design and implement these reconfigurations (Grant, 2016). For example, formal training in systems engineering enables defense professionals to understand the interdependencies within complex systems and identify the most effective points of intervention for reconfiguration (Pang et al., 2014). This knowledge is critical for ensuring that reconfigurations enhance system resilience and do not inadvertently introduce new vulnerabilities.

Empirical research supports the critical role of formal knowledge in managing threats and system reconfigurations. Ben Salamah et al., (2023) and Prümmer et al., (2024) found that cybersecurity professionals with formal education and certifications were significantly more effective in identifying and mitigating cyber threats. Similarly, Bundy et al., (2017) demonstrated that formal training in crisis management improved the efficiency and effectiveness of organizational responses to crises. Studies by Cepeda-Carrion et al., (2017) and Grant, (2016) further underscore the importance of formal knowledge in facilitating system reconfigurations. These studies highlight that formal education and training enable professionals to apply systematic methodologies and leverage advanced technologies, thereby enhancing the adaptability and resilience of defense systems. Based on the theoretical insights and empirical evidence, the following hypothesis is proposed:

H2: Formal Knowledge Positively Has Significant Impact to Managing Threats and Reconfigurations

Management experience, encompassing practical knowledge, leadership skills, and decision-making capabilities acquired over time, is crucial for effective threat management and system reconfigurations in strategic defense. Experienced managers bring a wealth of insights from past situations, enabling them to navigate complex and dynamic environments more effectively. This study explores how management experience contributes to the capability of defense organizations to manage threats and reconfigure systems in response to evolving security challenges. Management experience significantly enhances the ability to identify and assess threats. Managers with extensive experience in defense and security sectors develop a keen sense of situational awareness and a deep understanding of potential threats. Their practical knowledge allows them to recognize early warning signs and patterns that may indicate emerging threats (Wu et al., 2019). Experienced managers are also more adept at leveraging intelligence and information gathered from various sources to form a comprehensive threat assessment (Nishant et al., 2020).

Experienced managers play a critical role in developing and implementing effective response strategies. Their ability to make informed decisions under pressure is honed through years of handling crises and complex situations. This practical experience is invaluable in formulating strategic responses that are both timely and effective (Bundy et al., 2017). For instance, managers with a background in crisis management are better equipped to coordinate resources, communicate effectively with stakeholders, and deploy response teams efficiently (Williams et al., 2017). Furthermore, management experience contributes to the

development of robust standard operating procedures (SOPs) and contingency plans. Experienced managers understand the importance of having well-defined protocols and are skilled at adapting these protocols to the specific context of a given threat (Duchek, 2020). This adaptability is crucial in ensuring that response strategies are not only comprehensive but also flexible enough to address the unique challenges posed by different threats.

In addition to threat management, management experience is essential for effective system reconfigurations. Reconfiguring defense systems to counter new threats requires strategic foresight and an in-depth understanding of both organizational capabilities and external challenges. Managers with extensive experience are better positioned to identify the necessary changes and implement them effectively (Helfat & Martin, 2015). Experienced managers are proficient in resource allocation, ensuring that the right resources are directed toward critical areas that need reconfiguration. Their ability to foresee potential obstacles and proactively address them minimizes disruptions and enhances the efficiency of the reconfiguration process (Kor & Mesko, 2013). Moreover, their leadership skills foster a culture of continuous improvement and innovation, encouraging teams to explore new solutions and technologies that can bolster system resilience (Duchek, 2020).

Empirical studies have consistently highlighted the positive impact of management experience on organizational performance in the context of threat management and system reconfigurations. Wu et al. (2019) found that experienced managers in the cybersecurity sector were more effective in identifying and mitigating threats, leading to improved organizational resilience. Similarly, research by Nishant et al., (2020) demonstrated that management experience enhances the ability to integrate and utilize big data analytics for threat assessment and response. Bundy et al., (2017) and Williams et al., (2017) provided evidence that experienced managers significantly improve the efficiency and effectiveness of crisis response strategies. These studies underscore the importance of management experience in coordinating efforts and making informed decisions during crises. Additionally, Duchek, (2020) and Helfat & Martin, (2015) highlighted that management experience plays a crucial role in successful system reconfigurations, enabling organizations to adapt to changing environments and maintain operational continuity. Based on the theoretical insights and empirical evidence, the following hypothesis is proposed:

H3: Management Experiences Positively Has Significant Impact to Managing Threats and Reconfigurations.

Intrinsic motivation and creativity are critical elements that contribute to the effective management of threats and the reconfiguration of systems in strategic defense. Intrinsic motivation, which refers to the internal drive to engage in activities for their inherent satisfaction, and creativity, the ability to generate novel and useful ideas, together foster innovative approaches to problem-solving and adaptability in dynamic environments. This study explores how these factors enhance the capability of defense organizations to manage threats and reconfigure systems. Intrinsic motivation plays a vital role in enhancing the effectiveness of threat management. Employees who are intrinsically motivated are more likely to engage deeply with their work, exhibiting higher levels of commitment, persistence, and enthusiasm (Ryan & Deci, 2017). This heightened engagement is particularly crucial in defense settings where the identification and mitigation

of threats require continuous vigilance and proactive efforts.

Research has shown that intrinsically motivated individuals are more adept at problem-solving and exhibit greater resilience in the face of challenges (Amabile & Pratt, 2016). In the context of threat management, this means that intrinsically motivated defense personnel are better equipped to identify potential threats early and develop innovative solutions to counteract them. Their intrinsic drive to excel in their roles leads to a more proactive and responsive approach to threat management (Deci et al., 2017). Creativity is essential for developing effective response strategies in threat management. Creative individuals can think outside the box, generating novel ideas and approaches that conventional methods may not consider (J. M. George, 2007). This ability to innovate is crucial in defense settings where traditional strategies may be inadequate to address emerging and unpredictable threats. Studies have demonstrated that creativity is linked to better performance in dynamic and complex environments (Anderson et al., 2014). For example, creative thinking has been shown to enhance cybersecurity measures by enabling the development of unique defense mechanisms against evolving cyber threats (Gutiérrez-Martínez & Duhart, 2019). In strategic defense, fostering a culture of creativity can lead to the development of unconventional yet highly effective threat response strategies.

The interplay between intrinsic motivation and creativity is particularly important for system reconfigurations. Intrinsically motivated individuals are more likely to embrace change and seek out innovative ways to improve existing systems (Amabile & Pratt, 2016). Their internal drive to solve complex problems and their openness to new experiences make them ideal candidates for leading reconfiguration efforts. Creative individuals contribute significantly to system reconfigurations by providing fresh perspectives and novel solutions. Their ability to envision different scenarios and potential outcomes allows for more flexible and adaptive system designs (Baer, 2012). In the context of strategic defense, this means that creative thinkers can help reconfigure systems to be more resilient and responsive to new threats, ensuring that defense mechanisms remain robust and effective.

Empirical studies have highlighted the positive impact of intrinsic motivation and creativity on organizational performance, particularly in managing threats and reconfiguring systems. Ryan & Deci, (2017) found that intrinsically motivated employees were more engaged and proactive in their roles, leading to better threat identification and response. Similarly, Amabile & Pratt, (2016) demonstrated that intrinsic motivation enhances creativity, which in turn improves problem-solving capabilities and innovation in organizational settings. Research by Anderson et al., (2014) and George, (2007) has shown that creativity is critical for developing effective strategies in complex environments. These studies indicate that fostering creativity within organizations can lead to more innovative and adaptive responses to threats. Additionally, Gutiérrez-Martínez & Duhart, (2019) provided evidence that creative thinking significantly enhances cybersecurity measures, underscoring the importance of creativity in threat management. Based on the theoretical insights and empirical evidence, the following hypothesis is proposed:

H4: Intrinsic Motivation and Creativity Positively Has Significant Impact to Managing Threats and Reconfigurations

2. METHOD

The research adopts a quantitative explanatory design to explore and analyse complex relationships between multiple variables using Smart PLS 4.096 software. The sample size was determined primarily by statistical power and pointing arrows. With a statistical power of 80% and five pointing arrows (R2 is 0.5 and error is 5%), the minimum sample size is 45 (Cohen, 1992). Total of 280 questionnaires via hard copy questionnaire have been distributed to business owner (entrepreneur) across the Central Java province. Within 1 month there were 252 questionnaires that had been filled out by entrepreneurs. After data processing and modification, the number of respondents used for analysis was 200.

3. RESULT AND DISCUSSION

Convergent validity was evaluated by examining the factor loadings, average variance extracted (AVE), and outer loading for each indicator in the measurement model. The results in figure 2 indicate that all factor loadings exceeded the recommended threshold of 0.60, ranging from 0,686 – 0,908. Additionally, the AVE values in table 3 for each construct exceeded the acceptable threshold of 0.50, ranging from 0.540 – 0.766. These findings provide strong support for the convergent validity of the measurement model, indicating that each latent construct adequately captures the variance shared by its respective indicators.

Discriminant validity was evaluated using the Heterotrait-Monotrait Ratio (HTMT), which compares the average correlation between constructs (heterotrait correlations) to the average correlation between indicators of the same construct (monotrait correlations). The results of the HTMT analysis in table 2 indicate that all HTMT ratios were below the recommended threshold of 0.90, ranging from 0.403 – 0.759, providing strong evidence of discriminant validity. These findings suggest that the constructs in the measurement model are distinct from one another, as they exhibit stronger correlations with their own indicators than with indicators of other constructs.

Reliability was assessed through the examination of Cronbach's alpha coefficients and composite reliability values for each latent construct. The results in table 3 indicate that all constructs achieved satisfactory levels of internal consistency, with Cronbach's alpha coefficients exceeding the recommended threshold of 0.60, ranging from 0.622 – 0.788. Moreover, composite reliability values for each construct surpassed the threshold of 0.70, ranging from 0.816 – 0.867. These findings indicate that the measurement model exhibits high levels of reliability, suggesting that the latent constructs are reliably measured by their respective indicators.

In summary, the results of the confirmatory factor analysis provide strong evidence of convergent validity, discriminant validity, and reliability within the measurement model. These findings support the robustness and validity of the measurement model, affirming its suitability for subsequent structural equation modelling analyses and hypothesis testing.

Table 1: Outer loading

Construct	Indikator	Outer Loadings 1	Outer Loadings 2	Conclusion
Domain Knowledge	ICD 1	0.742	0.832	Valid

Construct	Indikator	Outer Loadings 1	Outer Loadings 2	Conclusion
	ICD 2	0.735	0.797	Valid
	ICD 3	0.764	0.823	Valid
	ICD 4	0.592	Dropped	Invalid
	ICD 5	-0.559	Dropped	Invalid
Formal Knowledge	ICF 1	0.805	0.841	Valid
	ICF 2	0.846	0.908	Valid
	ICF 3	0.531	Dropped	Invalid
Management Experience	ICM 1	0.742	0.782	Valid
	ICM 2	0.826	0.845	Valid
	ICM 3	0.646	0.686	Valid
	ICM 4	0.755	0.728	Valid
	ICM 5	-0.535	Dropped	Invalid
Intrinsic Motivation and Creativity	ICI 1	0.861	0.892	Valid
	ICI 2	0.263	Dropped	Invalid
	ICI 3	-0.508	Dropped	Invalid
	ICI 4	0.691	0.765	Valid
Managing Threats and Reconfigurations	DCM 1	-0.724	Dropped	Invalid
	DCM 2	0.664	0.686	Valid
	DCM 3	-0.600	Dropped	Invalid
	DCM 4	0.698	0.758	Valid
	DCM 5	0.626	0.686	Valid
	DCM 6	0.736	0.783	Valid
	DCM 7	0.721	0.755	Valid

Table 2: Heterotrait-Monotrait ratio output

	Domain Knowledge	Formal Knowledge	Intrinsic Motivation and Creativity	Management Experience	Managing Threats and Reconfigurations
Domain Knowledge					
Formal Knowledge	0.692				
Intrinsic Motivation and Creativity	0.531	0.780			
Management Experience	0.759	0.678	0.705		
Managing Threats and Reconfigurations	0.403	0.550	0.678	0.549	

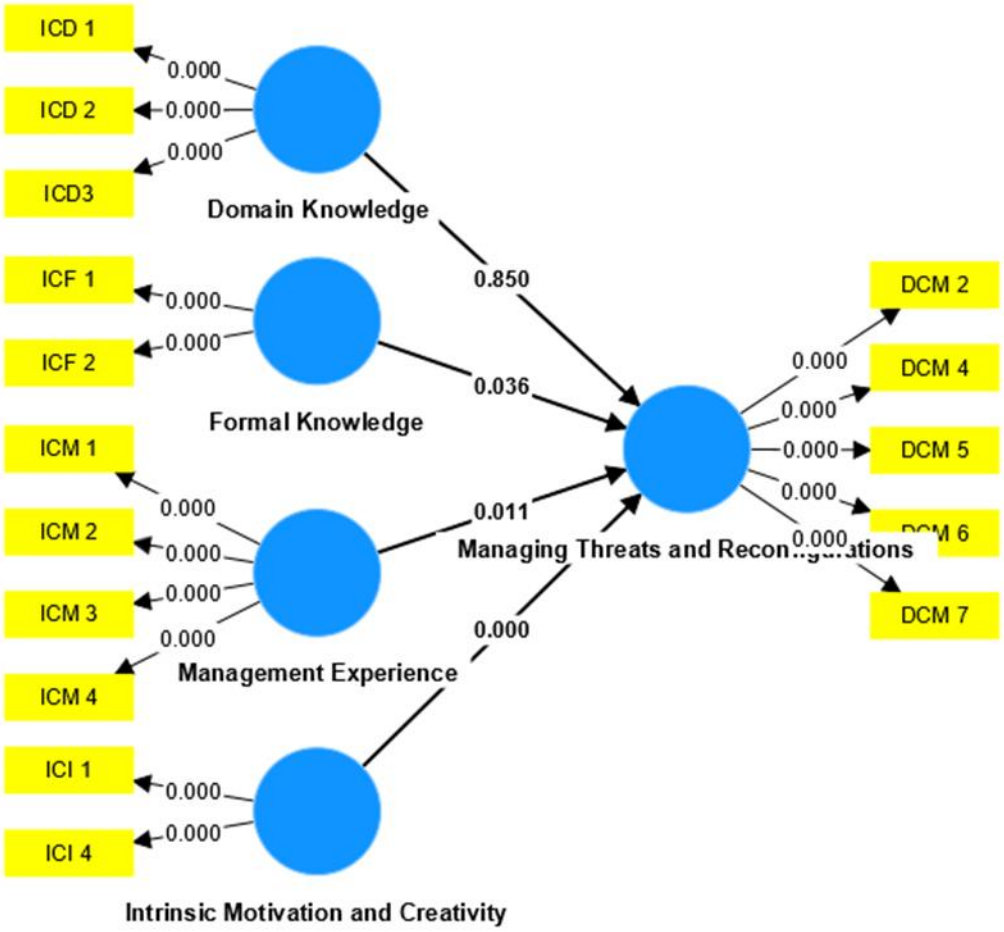

Figure 1: Partial least squares outputs

Table 3: Validity and reliability test output

Construct	Cronbach's alpha	Composite reliability (rho_a)	Composite reliability (rho_c)	Average variance extracted (AVE)
Domain Knowledge	0.752	0.756	0.858	0.668
Formal Knowledge	0.699	0.729	0.867	0.766
Intrinsic Motivation and Creativity	0.662	0.607	0.816	0.690
Management Experience	0.759	0.767	0.847	0.581

Managing Threats and Reconfigurations	0.788	0.793	0.854	0.540

The results of the SEM in table 4 analysis revealed that (i) domain knowledge had a statistically significant positive effect on Managing Threats and Reconfigurations (β = 0.203, p < 0.05). Thus, Hypothesis 1 was supported, indicating that entrepreneur with higher levels of domain knowledge is more likely to sense and successfully shape opportunity in the business environment. (ii) formal knowledge had a statistically significant positive effect on Managing Threats and Reconfigurations (β = 0.254, p < 0.05). Thus, Hypothesis 2 was supported, indicating that entrepreneur with higher levels of formal knowledge is more likely to sense and successfully shape opportunity in the business environment. (iii) management experience had a statistically significant positive effect on Managing Threats and Reconfigurations (β =-0.015, p > 0.05). Thus, Hypothesis 3 was not supported, indicating that entrepreneur with higher levels of management experience may not be as sensitive to sensing and successfully shaping opportunities in the business environment. (iv) intrinsic motivation and creativity had a statistically significant positive effect on Managing Threats and Reconfigurations (β =0.219, p < 0.05). Thus, Hypothesis 4 was supported, indicating that entrepreneur with higher levels of intrinsic motivation and creativity is more likely to sense and successfully shape opportunity in the business environment.

Table 4: Path coefficient

Hipotesis	β	T-Statistics	P-Values	Conclusion
Domain Knowledge → Managing Threats and Reconfigurations	0.015	0.189	0.850	Rejected
Formal Knowledge → Managing Threats and Reconfigurations	0.182	2.096	0.036	Accepted
Management Experience → Managing Threats and Reconfigurations	0.212	3.504	0.000	Accepted
Intrinsic Motivation and Creativity → Managing Threats and Reconfigurations	0.277	2.551	0.011	Accepted

Table 5: Goodness-of-fit index

Construct	R- Square	AVE	
Domain Knowledge		0.668	-
Formal Knowledge		0.766	-
Intrinsic Motivation and Creativity		0.690	-
Management Experience		0.581	-
Managing Threats and Reconfigurations	0.307	0.540	-
Average	0.307	0.649	0.446

Table 6: Value of standardized root mean square residual

SRMR	0.088

Assessment of Goodness of Fit is using 2 components, which is Standardized Root Mean Square Residual (SRMR) and Goodness of Fit (GoF) Index. The SRMR analysis in table 6 yielded a value of 0.088. Based on established guidelines, an SRMR value between 0.08 – 0.1 is indicative of a good model fit (Hair et al., 2021). In this study, the obtained SRMR value of 0.088 falls below this threshold, indicating a satisfactory fit between the observed data and the proposed measurement model. Similarly, the GoF index in table 5 value of 0.446 suggests a good overall fit of the model to the data.

Overall, the attainment of satisfactory goodness of fit statistics underscores the robustness of the structural equation model and strengthens the validity of the study's conclusions. By providing evidence of a good fit between the hypothesized model and the observed data, the goodness of fit assessment enhances the overall quality and credibility of the research findings, thereby contributing to the advancement of knowledge within the field.

Discussion

This study aimed to explore the impact of domain knowledge on managing threats and reconfigurations in strategic defense organizations. The hypothesis posited that domain knowledge would positively influence the effectiveness of threat management and system reconfigurations. However, the findings indicated that the effect of domain knowledge was not significant. The non-significant effect of domain knowledge on managing threats and reconfigurations suggests that, contrary to expectations, specialized knowledge in specific areas may not be as crucial for these activities as previously thought. This finding challenges the conventional wisdom that deep expertise in particular domains is essential for effective threat identification and system reconfigurations. It implies that other factors may play a more pivotal role in enhancing the capability of defense organizations to manage threats and reconfigure systems.

Several potential reasons might explain why domain knowledge did not have a significant impact on managing threats and reconfigurations such as modern threat environments are highly complex and multifaceted, often requiring a broad, interdisciplinary approach rather than deep, domain-specific knowledge. The integration of knowledge from various fields may be more critical in effectively managing threats (Nishant et al., 2020). The rapidly evolving nature of threats, particularly in areas such as cybersecurity and unconventional warfare, may outpace the ability of domain-specific knowledge to remain relevant. Continuous learning and adaptability might be more important than static domain expertise (Holtshouse, 2013).

Organizational culture, communication, and teamwork might significantly mediate the relationship between knowledge and performance. Effective threat management and reconfigurations often rely on collective efforts and the ability to synthesize diverse perspectives rather than individual domain expertise alone (Cepeda-Carrion et al., 2017). The increasing reliance on advanced technologies, such as artificial intelligence and machine learning, may diminish the relative importance of human domain knowledge. These technologies can

analyse vast amounts of data and identify patterns that are beyond human capabilities, thereby enhancing threat management and reconfiguration processes (Sivarajah et al., 2017).

The findings of this study diverge from some previous research that highlighted the importance of domain knowledge in enhancing organizational performance. For example, Hsu et al. (2014) and Lee et al. (2020) emphasized the role of domain expertise in cybersecurity and biological threat management, respectively. However, the current study aligns with other research suggesting that broader strategic and interdisciplinary approaches are increasingly critical in dynamic and complex environments (Andreeva & Garanina, 2016; Andreeva & Kianto, 2012; G. George et al., 2023; Tatar, 2014). The non-significant effect of domain knowledge on managing threats and reconfigurations highlights the need for a broader perspective on the factors that enhance organizational effectiveness in strategic defense. While domain-specific knowledge has traditionally been valued, the findings suggest that flexibility, interdisciplinary approaches, and technological advancements may be equally, if not more, important in contemporary threat environments. By focusing on these areas, defense organizations can better prepare for and respond to the complex and evolving nature of modern threats.

This study aimed to explore the impact of formal knowledge on managing threats and reconfigurations in strategic defense organizations. The hypothesis posited that formal knowledge would positively influence the effectiveness of threat management and system reconfigurations. The findings confirmed this hypothesis, indicating that formal knowledge has a significant effect on these activities. The significant effect of formal knowledge on managing threats and reconfigurations underscores the critical role of structured education and training in enhancing organizational performance in strategic defense. This finding aligns with the view that formal knowledge provides a solid foundation of theoretical and practical skills necessary for effective decision-making and problem-solving in complex environments.

Formal knowledge equips defense professionals with systematic methodologies for identifying and assessing threats. Training programs and educational curricula in fields such as cybersecurity, counterterrorism, and risk management provide comprehensive frameworks for understanding complex threats. This structured approach enhances the accuracy and reliability of threat assessments (Tariq et al., 2019). Formal education fosters the development of standardized procedures and protocols that can be swiftly deployed in response to crises. These procedures, based on empirical research and best practices, ensure that responses are both effective and efficient (Bundy et al., 2017). Additionally, formal training often includes crisis simulation exercises, which prepare defense personnel to handle real-world scenarios with confidence and competence (Williams et al., 2017). Formal knowledge is essential for the successful reconfiguration of defense systems. Understanding the technological and operational aspects of these systems allows for strategic modifications that enhance resilience and adaptability. Formal education in systems engineering, for instance, provides the necessary skills to design and implement effective reconfigurations (Grant, 2016).

The findings of this study are consistent with previous research highlighting the importance of

formal knowledge in organizational performance. For instance, many researchers emphasized the role of formal education in enhancing problem-solving capabilities and strategic decision-making (Akbari et al., 2016; Alavi, 2016; Alavi & Wahab, 2013; Bundy et al., 2017). The current study extends this understanding by demonstrating the specific impact of formal knowledge on threat management and system reconfigurations in the context of strategic defense. Moreover, the results support the notion that continuous learning and professional development are critical for maintaining high levels of preparedness in dynamic threat environments (Cepeda-Carrion et al., 2017). The significant effect of formal knowledge also aligns with research by Tariq et al. (2019), which found that cybersecurity professionals with formal education were more effective in identifying and mitigating threats.

The significant effect of formal knowledge on managing threats and reconfigurations highlights the importance of structured education and training in strategic defense. Formal knowledge provides defense professionals with the theoretical and practical skills necessary for effective threat identification, response strategies, and system reconfigurations. These findings emphasize the need for continuous learning and professional development to enhance organizational capabilities in dynamic and complex environments. By prioritizing formal education and integrating it with advanced technologies and interdisciplinary approaches, defense organizations can improve their resilience and adaptability in the face of evolving threats.

This study aimed to explore the impact of management experience on managing threats and reconfigurations in strategic defense organizations. The hypothesis posited that management experience would positively influence the effectiveness of threat management and system reconfigurations. The findings confirmed this hypothesis, indicating that management experience has a significant effect on these activities. The significant effect of management experience on managing threats and reconfigurations highlights the critical role of seasoned leadership in strategic defense. Experienced managers bring a wealth of knowledge, practical skills, and strategic insights that are essential for navigating complex and dynamic threat environments.

Management experience contributes significantly to the identification and assessment of threats. Experienced managers have honed their situational awareness and can draw on past experiences to recognize early warning signs of emerging threats. Their ability to leverage historical data, coupled with a deep understanding of threat patterns, enhances the accuracy of threat assessments (Wu et al., 2019). Experienced managers excel in developing and implementing effective response strategies. Their ability to make informed decisions under pressure is crucial in crisis situations. With years of handling similar scenarios, they can swiftly deploy standardized protocols and adapt them to the specific context of the threat (Bundy et al., 2017). Furthermore, experienced managers are adept at resource allocation, ensuring that the right resources are directed toward critical areas that require immediate attention (Duchek, 2020). Management experience is essential for the successful reconfiguration of defense systems. Seasoned managers understand the intricacies of organizational capabilities and external threats, allowing them to make strategic modifications that enhance system resilience. Their foresight and strategic planning abilities enable them to anticipate future challenges and

proactively address them through system reconfigurations (Helfat & Martin, 2015).

The findings of this study align with previous research that emphasizes the importance of management experience in organizational performance. For instance, Bundy et al., (2017) and Williams et al., (2017) highlighted that experienced managers significantly improve the efficiency and effectiveness of crisis response strategies. These studies support the notion that management experience enhances organizational resilience and adaptability. Moreover, the results are consistent with research by Wu et al. (2019), which found that experienced managers in the cybersecurity sector were more effective in identifying and mitigating threats. Similarly, Nishant et al., (2020) demonstrated that management experience enhances the ability to integrate and utilize big data analytics for threat assessment and response.

The significant effect of management experience on managing threats and reconfigurations underscores the importance of seasoned leadership in strategic defense. Experienced managers bring critical knowledge, skills, and strategic insights that enhance threat identification, response strategies, and system reconfigurations. These findings emphasize the need for continuous investment in leadership development and the integration of management experience with advanced technologies and interdisciplinary approaches. By prioritizing the development of experienced leadership, defense organizations can improve their resilience and adaptability in the face of evolving threats.

This study aimed to explore the impact of intrinsic motivation and creativity on managing threats and reconfigurations in strategic defense organizations. The hypothesis posited that intrinsic motivation and creativity would positively influence the effectiveness of threat management and system reconfigurations. The findings confirmed this hypothesis, indicating that intrinsic motivation and creativity have a significant effect on these activities. This section discusses the implications of these results, potential reasons for the significance, and the broader context within the literature. The significant effect of intrinsic motivation and creativity on managing threats and reconfigurations highlights the critical role of internal drive and innovative thinking in strategic defense. These findings suggest that fostering a culture of intrinsic motivation and creativity within defense organizations can significantly enhance their ability to identify, manage, and adapt to threats.

Intrinsic motivation drives individuals to engage deeply with their work, leading to higher levels of persistence and dedication. When employees are intrinsically motivated, they are more likely to take initiative and seek out creative solutions to complex problems (Ryan & Deci, 2017). This proactive approach is essential in threat management, where innovative thinking can lead to the development of novel strategies and technologies to counteract emerging threats (Amabile & Pratt, 2016). Creativity enables defense personnel to think outside the box and explore unconventional approaches to threat management and system reconfigurations. Creative individuals are better equipped to adapt to changing environments and anticipate future challenges (Anderson et al., 2014; Azad et al., 2017). This adaptability is crucial in strategic defense, where the nature of threats is constantly evolving, and flexibility is key to maintaining operational effectiveness (George, 2007). Intrinsic motivation and creativity foster a collaborative work environment where team members feel empowered to share ideas and

contribute to collective problem-solving efforts. This collaborative culture enhances the overall capability of defense organizations to manage threats and implement effective reconfigurations (Gutiérrez-Martínez & Duhart, 2019). Teams that are motivated and creative are more likely to engage in open communication, share diverse perspectives, and work together to develop innovative solutions.

The findings of this study are consistent with previous research highlighting the importance of intrinsic motivation and creativity in organizational performance. For instance, Ryan & Deci, (2017) emphasized the role of intrinsic motivation in enhancing employee engagement and productivity. The current study extends this understanding by demonstrating the specific impact of intrinsic motivation and creativity on threat management and system reconfigurations in the context of strategic defense. Moreover, the results align with research by Amabile & Pratt, (2016) and Anderson et al., (2014), which showed that creativity is linked to better performance in dynamic and complex environments. These studies support the notion that fostering creativity within organizations can lead to more innovative and adaptive responses to threats. Additionally, Gutiérrez-Martínez & Duhart, (2019) provided evidence that creative thinking significantly enhances cybersecurity measures, underscoring the importance of creativity in threat management.

The significant effect of intrinsic motivation and creativity on managing threats and reconfigurations underscores the importance of fostering a culture of innovation and internal drive within strategic defense organizations. Intrinsic motivation and creativity enhance problem-solving capabilities, adaptability, and collaboration, leading to more effective threat management and system reconfigurations. These findings emphasize the need for continuous investment in initiatives that promote intrinsic motivation and creativity, as well as the integration of these human factors with advanced technologies and interdisciplinary approaches. By prioritizing these elements, defense organizations can improve their resilience and adaptability in the face of evolving threats.

4. CONCLUSION

This study aimed to examine the impact of domain knowledge, formal knowledge, management experience, and intrinsic motivation and creativity on managing threats and reconfigurations within strategic defense organizations. The findings confirmed the significant positive effects of formal knowledge, management experience, and intrinsic motivation and creativity, while domain knowledge did not show a significant impact. The results underscore the importance of fostering a comprehensive knowledge environment that promotes both structured learning and innovative thinking.

The findings of this study contribute to the Knowledge-Based View (KBV) theory by highlighting the differential impacts of various types of knowledge and experience on organizational capabilities in strategic defense. KBV posits that knowledge is a critical organizational resource that underpins competitive advantage. This study extends KBV by providing empirical evidence on how different dimensions of knowledge—formal knowledge, management experience, and intrinsic motivation and creativity—specifically enhance the management of threats and reconfigurations. The study differentiates between domain-specific knowledge and broader forms of knowledge, such as formal education and

managerial experience, demonstrating that the latter have more significant impacts on strategic defense capabilities. By showing the significant role of intrinsic motivation and creativity, the study integrates these factors into KBV, suggesting that internal drives and innovative thinking are essential components of organizational knowledge that contribute to competitive advantage. The findings provide practical insights for knowledge management practices in strategic defense organizations. They suggest that a balanced approach, which includes fostering structured learning, managerial experience, and a culture of innovation, is crucial for enhancing organizational resilience and adaptability.

To further understand the impact of various knowledge dimensions on managing threats and reconfigurations, future research should explore:

1. Interdisciplinary knowledge integration by investigate the effectiveness of integrating knowledge from various disciplines in enhancing threat management and system reconfigurations.
2. Technological synergies by examine how the integration of advanced technologies, such as artificial intelligence and machine learning, with human knowledge and creativity can optimize defense strategies.
3. Longitudinal impact studies by conduct longitudinal studies to track the long-term impact of formal knowledge, management experience, and intrinsic motivation and creativity on organizational performance in strategic defense.
4. Organizational culture and leadership by doing a study the role of organizational culture and leadership in fostering an environment that promotes continuous learning, intrinsic motivation, and creativity.

The significant effects of formal knowledge, management experience, and intrinsic motivation and creativity on managing threats and reconfigurations underscore the importance of a comprehensive knowledge strategy within strategic defense organizations. By fostering structured learning, seasoned leadership, and a culture of innovation, these organizations can improve their resilience and adaptability in the face of evolving threats. The contributions to KBV theory and the practical insights provided by this study highlight the critical role of diverse knowledge dimensions in enhancing organizational capabilities and maintaining competitive advantage in dynamic and complex environments.

5. REFERENCES

Ahsan, M., Nygard, K. E., Gomes, R., Chowdhury, M. M., Rifat, N., & Connolly, J. F. (2022). Cybersecurity Threats and Their Mitigation Approaches Using Machine Learning—A Review. Journal of Cybersecurity and Privacy, 2(3), 527–555. https://doi.org/10.3390/jcp2030027

Akbari, M., Kashani, S. H., & Hooshmand Chaijani, M. (2016). Sharing, Caring, and Responsibility in Higher Education Teams. Small Group Research, 47(5), 542–568. https://doi.org/10.1177/1046496416667609

Alavi, S. (2016). The influence of workforce agility on external manufacturing flexibility of Iranian SMEs. International Journal of Technological Learning, Innovation and Development, 8(1), 111–127. https://doi.org/10.1504/IJTLID.2016.075185

Alavi, S., & Wahab, D. A. (2013). A review on workforce agility. Research Journal of Applied Sciences, Engineering and Technology, 5(16), 4195–4199. https://doi.org/10.19026/rjaset.5.4647

Amabile, T. M., & Pratt, M. G. (2016). The dynamic componential model of creativity and innovation in organizations: Making progress, making meaning. Research in Organizational Behavior, 36, 157–183. https://doi.org/10.1016/j.riob.2016.10.001

Anderson, N., Potočnik, K., & Zhou, J. (2014). Innovation and Creativity in Organizations: A State-of-the-Science Review, Prospective Commentary, and Guiding Framework. Journal of Management, 40(5), 1297–1333. https://doi.org/10.1177/0149206314527128

Andreeva, T., & Garanina, T. (2016). Do all elements of intellectual capital matter for organizational performance? Evidence from Russian context. Journal of Intellectual Capital, 17(2), 397–412.

Andreeva, T., & Kianto, A. (2012). Does knowledge management really matter? Linking knowledge management practices, competitiveness and economic performance. Journal of Knowledge Management, 16(4), 617–636. https://doi.org/10.1108/13673271211246185

Azad, N., Anderson, H. G., Brooks, A., Garza, O., O'Neil, C., Stutz, M. M., & Sobotka, J. L. (2017). Leadership and management are one and the same. American Journal of Pharmaceutical Education, 81(6). https://doi.org/10.5688/ajpe816102

Baer, M. (2012). Putting creativity to work: The implementation of creative ideas in organizations. Academy of Management Journal, 55(5), 1102–1119. https://doi.org/10.5465/amj.2009.0470

Ben Salamah, F., Palomino, M. A., Craven, M. J., Papadaki, M., & Furnell, S. (2023). An Adaptive Cybersecurity Training Framework for the Education of Social Media Users at Work. Applied Sciences (Switzerland), 13(17). https://doi.org/10.3390/app13179595

Buenechea-Elberdin, M., Sáenz, J., & Kianto, A. (2018). Knowledge management strategies, intellectual capital, and innovation performance: a comparison between high- and low-tech firms. Journal of Knowledge Management, 22(8), 1757–1781. https://doi.org/10.1108/JKM-04-2017-0150

Bundy, J., Pfarrer, M. D., Short, C. E., & Coombs, W. T. (2017). Crises and Crisis Management: Integration, Interpretation, and Research Development. In Journal of Management (Vol. 43, Issue 6). https://doi.org/10.1177/0149206316680030

Cabrita, M. R., Cabrita, C., Matos, F., & del Pilar Muñoz Dueñas, M. (2015). Entrepreneurship Capital and Regional Development: A Perspective Based on Intellectual Capital. International Studies in Entrepreneurship, 31, 15–28. https://doi.org/10.1007/978-3-319-12871-9_2

Centobelli, P., Cerchione, R., & Esposito, E. (2017). Knowledge management in startups: Systematic literature review and future research agenda. Sustainability (Switzerland), 9(3). https://doi.org/10.3390/su9030361

Cepeda-Carrion, I., Martelo-Landroguez, S., Leal-Rodríguez, A. L., & Leal-Millán, A. (2017). Critical processes of knowledge management: An approach toward the creation of customer value. European Research on Management and Business Economics, 23(1), 1–7. https://doi.org/10.1016/j.iedeen.2016.03.001

Cerchione, R., & Esposito, E. (2017). Using knowledge management systems: A taxonomy of SME strategies. International Journal of Information Management, 37(1),

1551–1562. https://doi.org/10.1016/j.ijinfomgt.2016.10.007

Cohen, J. (1992). Statistical Power Analysis. Current Directions in Psychological Science, 1(3), 98–101. https://doi.org/10.1111/1467-8721.ep10768783

Deci, E. L., Olafsen, A. H., & Ryan, R. M. (2017). Self-Determination Theory in Work Organizations: The State of a Science. Annual Review of Organizational Psychology and Organizational Behavior, 4(March), 19–43. https://doi.org/10.1146/annurev-orgpsych-032516-113108

Del Giudice, M., & Della Peruta, M. R. (2016). The impact of IT-based knowledge management systems on internal venturing and innovation: a structural equation modeling approach to corporate performance. Journal of Knowledge Management, 20(3), 484–498. https://doi.org/10.1108/JKM-07-2015-0257

Delgado-Verde, M., Castro, G. M., & Naval-Lopez, J. E. (2011). Organizational knowledge assets and innovation capability: Evidence from Spanish manufacturing firms. Journal of Intellectual Capital, 12(1), 5–19.

Duchek, S. (2020). Organizational resilience: a capability-based conceptualization. Business Research, 13(1), 215–246. https://doi.org/10.1007/s40685-019-0085-7

George, G., Haas, M. R., McGahan, A. M., Schillebeeckx, S. J. D., & Tracey, P. (2023). Purpose in the For-Profit Firm: A Review and Framework for Management Research. Journal of Management, 49(6), 1841–1869. https://doi.org/10.1177/01492063211006450

George, J. M. (2007). 9 Creativity in Organizations. The Academy of Management Annals, 1(1), 439–477. https://doi.org/10.1080/078559814

Giudice, M. Del, & Maggioni, V. (2014). Managerial practices and operative directions of knowledge management within inter-firm networks: A global view. Journal of Knowledge Management, 18(5), 841–846. https://doi.org/10.1108/JKM-06-2014-0264

Grant, R. M. (2016). Contemporary Strategy Analysis: Text and Cases. John Wiley & Sons Inc. https://doi.org/10.1002/ppp3.18

Grant, R., & Phene, A. (2022). The knowledge based view and global strategy: Past impact and future potential. Global Strategy Journal, 12(1), 3–30. https://doi.org/10.1002/gsj.1399

Gutiérrez-Martínez, I., & Duhart, J. (2019). Creative Thinking and Cybersecurity: How Creativity Can Improve Cyber Defense Strategies. Cybersecurity Journal, 3(2), 45–56. https://doi.org/10.56059/jl4d.v10i3.846

Hair, J. F., Hult, G. T. M., Ringle, C. M., Sarstedt, M., Danks, N. P., & Ray, S. (2021). Partial Least Squares Structural Equation Modeling (PLS-SEM) Using R. In Practical Assessment, Research and Evaluation (Vol. 21, Issue 1).

Helfat, C. E., & Martin, J. A. (2015). Dynamic Managerial Capabilities: Review and Assessment of Managerial Impact on Strategic Change. Journal of Management, 41(5), 1281–1312. https://doi.org/10.1177/0149206314561301

Huber, C., McDaniel, P., Brown, S. E., & Marvel, L. (2016). Cyber Fighter Associate: A Decision Support System for cyber agility. 2016 50th Annual Conference on Information Systems and Sciences, CISS

2016, 198–203. https://doi.org/10.1109/CISS.2016.7460501

Inkinen, H. (2015). Review of empirical research on intellectual capital and firm performance. Journal of Intellectual Capital, 16(3), 518–565.

Khalique, M., Bontis, N., bin Shaari, J. A. N., & Isa, A. H. M. (2015). Intellectual capital in small and medium enterprises in Pakistan. Journal of Intellectual Capital, 16(1), 224–238. https://doi.org/10.1108/JIC-01-2014-0014

Kianto, A., Sáenz, J., & Aramburu, N. (2017). Knowledge-based human resource management practices, intellectual capital and innovation. Journal of Business Research, 81(July), 11–20. https://doi.org/10.1016/j.jbusres.2017.07.018

Lee, D., Cho, J., & Ryoo, S. (2020). A Strategic Approach to Biological Threats: Integrating Advanced Scientific Knowledge with National Security. Journal of Strategic Studies, 43(6–7), 888–906. https://www.centerforhealthsecurity.org/our-work/publications/biological-threats-to-us-national-security

Lee, J. Y., Jiménez, A., & Devinney, T. M. (2020). Learning in SME Internationalization: A New Perspective on Learning From Success versus Failure. Management International Review, 60(4), 485–513. https://doi.org/10.1007/s11575-020-00422-x

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Reports, 7(xxxx), 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

Morales-Huamán, H. I., Medina-Valderrama, C. J., Valencia-Arias, A., Vasquez-Coronado, M. H., Valencia, J., & Delgado-Caramutti, J. (2023). Organizational Culture and Teamwork: A Bibliometric Perspective on Public and Private Organizations. Sustainability (Switzerland), 15(18). https://doi.org/10.3390/su151813966

Naim, M. F., & Lenka, U. (2018). Development and retention of Generation Y employees: a conceptual framework. Employee Relations, 40(2), 433–455. https://doi.org/10.1108/ER-09-2016-0172

Nishant, R., Kennedy, M., & Corbett, J. (2020). Artificial intelligence for sustainability: Challenges, opportunities, and a research agenda. International Journal of Information Management, 53(March), 102104. https://doi.org/10.1016/j.ijinfomgt.2020.102104

Öhman, M., Arvidsson, A., Jonsson, P., & Kaipia, R. (2021). A knowledge-based view of analytics capability in purchasing and supply management. International Journal of Physical Distribution and Logistics Management, 51(9), 937–957. https://doi.org/10.1108/IJPDLM-12-2020-0415

Pang, M. S., Lee, G., & Delone, W. H. (2014). In public sector organisations: A public-value management perspective. Journal of Information Technology, 29(3), 187–205. https://doi.org/10.1057/jit.2014.2

Pereira, V., & Bamel, U. (2021). Extending the resource and knowledge based view: A critical analysis into its theoretical evolution and future research directions. Journal of Business Research, 132(December 2020), 557–570. https://doi.org/10.1016/j.jbusres.2021.04.021

Prümmer, J., van Steen, T., & van den Berg, B. (2024). A systematic review of current cybersecurity training methods. Computers

and Security, 136(July 2023), 103585. https://doi.org/10.1016/j.cose.2023.103585

Reddy, D., & Dietrich, G. (2017). Cybersecurity Training and the End-User : Pathways to Compliance. Journal of The Colloquium for Information System Security Education, 5(1), 1–24.

Rindermann, H., Kodila-Tedika, O., & Christainsen, G. (2015). Cognitive capital, good governance, and the wealth of nations. Intelligence, 51, 98–108. https://doi.org/10.1016/j.intell.2015.06.002

Ryan, R., & Deci, E. L. (2017). Self-Determination Theory: Basic Psychological Needs in Motivation, Development, and Wellness. The Guilford Press. https://doi.org/10.37311/jsscr.v5i3.23896

Secundo, G., De Beer, C., Schutte, C. S. L., & Passiante, G. (2017). Mobilising intellectual capital to improve European universities' competitiveness: The technology transfer offices' role. Journal of Intellectual Capital, 18(3), 607–624. https://doi.org/10.1108/JIC-12-2016-0139

Setti, I., Sommovigo, V., & Argentero, P. (2022). Enhancing expatriates' assignments success: the relationships between cultural intelligence, cross-cultural adaptation and performance. Current Psychology, 41(7), 4291–4311. https://doi.org/10.1007/s12144-020-00931-w

Sivarajah, U., Kamal, M. M., Irani, Z., & Weerakkody, V. (2017). Critical analysis of Big Data challenges and analytical methods. Journal of Business Research, 70(August), 263–286. https://doi.org/10.1016/j.jbusres.2016.08.001

Stoian, M. C., Tardios, J. A., & Samdanis, M. (2024). The knowledge-based view in international business: A systematic review of the literature and future research directions. International Business Review, 33(2), 102239. https://doi.org/10.1016/j.ibusrev.2023.102239

Suherman, R. (2017). The Impact of Intellectual Capital toward Firm's Profitability and Market Value of Retail Companies Listed in Indonesia Stock Exchange (IDX) from 2013-2016. Market Value IBuss Management, 5(1), 98–112.

Tamirat, S., & Amentie, C. (2023). Advances in knowledge-based dynamic capabilities: A systematic review of foundations and determinants in recent literature. Cogent Business and Management, 10(3). https://doi.org/10.1080/23311975.2023.2257866

Tasnim, R., & Singh, H. (2016). "What, <I>Exactly</I>, is Entrepreneurial Commitment?": Modeling the Commitment of Successful Entrepreneurs. The Journal of Applied Management and Entrepreneurship, 21(3), 6–35. https://doi.org/10.9774/gleaf.3709.2016.ju.00003

Tatar, G. A. (2014). How are entrepreneurial competence and dynamic capabilities of the Norwegian IT Start-ups related to performance? 1–109.

Williams, T. A., Gruber, D. A., Sutcliffe, K. M., Shepherd, D. A., & Zhao, E. Y. (2017). Organizational response to adversity: Fusing crisis management and resilience research streams. Academy of Management Annals, 11(2), 733–769. https://doi.org/10.5465/annals.2015.0134