Formosa Journal of Multidisciplinary Research (FJMR)
Vol. 4 No. 8, 2025: 3733-3750

Psychological Dimensions of Sishanta for Societal Resilience and National Unity in the Digital Defense Era

Adi Putra Wibisono[1*], Susilo Adi Purwantoro[2], Editha Praditya Duarte[3]
Republic of Indonesia Defense University, Indonesia
Corresponding Author: Adi Putra Wibisono adiputraawibisono@gmail.com

A R T I C L E I N F O
Keywords: Digital Era, National Unity, Psychological Dimensions, Societal Resilience, Sishanta

Received : 16, July
Revised : 30, July
Accepted: 22, August

A B S T R A C T
This study examines the strategic application of Indonesia's Universal Defense System, Sishanta, in cultivating societal resilience and national unity against digital threats. Sishanta, a whole-of-nation defense strategy, is deeply rooted in Indonesia's collectivist culture, religiosity, and local wisdom, offering a unique psychological foundation unlike individualistic Western models. In the digital era, Sishanta can be reinterpreted to address disinformation and psychological operations by integrating digital literacy into "Bela Negara" education, leveraging AI for threat detection, and employing initiatives like the Digital House of Knowledge for cultural resilience. Challenges include slow regulatory adaptation and weak non-military coordination, necessitating flexible policies and interdisciplinary collaboration to ensure comprehensive national defense.

DOI: https://doi.org/10.55927/fjmr.v4i8.353
ISSN-E: 2829-8896
https://npaformosapublisher.org/index.php/fjmr

INTRODUCTION

A nation's defense strategy is vital in safeguarding its sovereignty and territorial integrity amid various threats. The evolving global landscape has brought both military and non-military challenges that have significantly reshaped national life. This evolution includes the rise of digital era threats, such as disinformation campaigns, which advancements in information technology can facilitate. These non-military threats often target the nation's mindset, promoting ideologies contrary to national values or aiming to diminish patriotism (Huda et al., 2024). The insidious nature of these threats, which attack societal thought processes, necessitates a comprehensive response.

Indonesia employs the Universal Defense System (Sistem Pertahanan Semesta) or Sishanta to address such complex and varied threats. This system is characterised by its comprehensive nature, involving all citizens, territories, and national resources, prepared in advance by the government and implemented in a total, integrated, directed, and sustainable manner to uphold state sovereignty, territorial integrity, and national safety from all forms of threats (Huda et al., 2024). Sishanta is not solely the military's (TNI) responsibility as the main component, but of all national resources. In the context of the digital era, where non-military threats like disinformation are prevalent, Sishanta's framework, which involves all citizens and empowers ideological, political, economic, socio-cultural, and technological factors, becomes particularly relevant in safeguarding the nation (Huda et al., 2024).

However, a potential gap exists in the current discourse and application of defence strategies against the backdrop of an increasingly digitised world. Specifically, current defense strategies may overly focus on technical cybersecurity measures, such as firewalls, encryption, and intrusion detection systems. While these technological safeguards are undoubtedly vital, overemphasising them risks potentially overlooking the crucial psychological vulnerabilities and the human element central to national defense in the digital age. Digital threats, particularly sophisticated disinformation campaigns and influence operations, often bypass technical defenses by directly targeting human cognition, emotions, and societal trust. This creates a critical need to look beyond purely technological solutions and consider the more nuanced aspects of psychological defense.

This observation leads to a critical inquiry that will guide this research: *How can the psychological dimensions inherent in Indonesia's Sistem Pertahanan Semesta (Sishanta) be effectively leveraged and adapted to cultivate societal resilience and strengthen national unity against modern digital threats, thereby ensuring comprehensive national defense in the digital era?* Answering this question is essential because it directly addresses the identified gap wherein the human element, often the primary target of digital era threats, may be under-addressed by technically-focused strategies. Understanding how Sishanta's psychological underpinnings can be mobilised is crucial for developing effective countermeasures beyond technological fixes, strengthening Indonesia's ability to withstand and recover from non-military attacks on its societal cohesion and national identity. Therefore, this study aims to analyse the strategic application of Sishanta's inherent psychological principles, which likely encompass

community cohesion, national identity, and collective responsibility, to enhance societal resilience and national unity in these pervasive non-military challenges.

The significance of this study is particularly pronounced as it addresses a pressing contemporary issue, given the world's escalating geopolitical tension and the weaponisation of information. Digital threats transcend physical borders, making robust, psychologically-informed national defence strategies more critical. By exploring these psychological dimensions within the Sishanta framework, this research seeks to contribute valuable insights towards developing a more holistic, adaptive, and ultimately effective national defense posture that empowers citizens and strengthens the societal fabric against insidious digital influences in an increasingly complex global environment.

LITERATURE REVIEW

Societal Resilience and National Unity

In an era marked by uncertainty and diverse threats, ranging from natural disasters to armed conflicts, societal resilience is vital (Rachmad, 2022). This concept encloses a community's capacity to endure, adapt, and respond constructively to crises, ensuring long-term stability (Maguire & Hagan, 2009). It encompasses resistance to disruption, recovery to normalcy, and the creativity to learn from adversity, improving future responses (Maguire & Hagan, 2009). While societal resilience levels vary among social groups, influenced by factors like socio-economic status and disaster type, contemporary perspectives emphasize its deliberate cultivation through proactive planning and intervention, rather than relying on its spontaneous emergence (Rachmad, 2022). Ultimately, societal resilience forms a crucial foundation for national unity and social cohesion, indispensable for a country's stability and defense readiness.

National unity and social resilience are fundamental to a nation's core interests, serving as essential pillars for its preservation and the safeguarding of its citizens' lives, rights, and freedoms (Trubavina et al., 2024). A "unity of purpose" and "social solidarity" are identified as intrinsic components of national resilience, deeply linked to a shared destiny and a collective commitment to the common good (Michael & Fishman, 2019). The absence of genuine cohesion critically undermines the state's and civil society's administrative structures. This vulnerability invites external propaganda, psychological operations, and internal conflicts, significantly diminishing a country's defense capabilities (Trubavina et al., 2024). Thus, national unity is a prerequisite for effective governance and societal stability.

During times of crisis, especially war, establishing a common goal or idea becomes paramount for uniting citizens, who often face diverse life experiences and traumatic circumstances. This unity can be effectively cultivated through community-level social, informative, and legal initiatives that transcend political manipulation. Such approaches strengthen mutual assistance, pool resources, and alleviate social tension (Trubavina et al., 2024). Historically, political parties have often exploited cohesion and unity for self-interest, leading to societal division rather than unification (Trubavina et al., 2024). However, a contemporary shift towards needs-based, human-centred social interventions at the community level fosters authentic connections. By directly addressing

citizens' basic needs and promoting genuine collective action, these interventions contribute profoundly to national unity, starkly contrasting the fragmenting effects of politically driven, self-serving strategies.

The relationship between societal resilience and national unity is mutually reinforcing, with social resilience consistently recognized as a key element of broader national resilience (Riabets, 2024). National resilience broadly refers to a state's capacity to withstand internal and external threats across political, economic, social, and environmental domains (Riabets, 2024). Social resilience is often measured through indicators such as patriotism, collective threat perception, and trust in institutions, and it directly underpins national stability (Michael & Fishman, 2019). A resilient society, actively supported by the state, is better equipped to endure crises and adapt to change, while national security, in turn, fosters an environment of trust and stability (Riabets, 2024). Furthermore, social capital plays a vital role in this dynamic, enabling communities to mobilize resources and strengthen cohesion during times of need.

Understanding this interdependence requires examining the key drivers that strengthen or weaken social and national resilience. Social resilience is robustly strengthened by factors such as trust, effective leadership, strong social cohesion, active community engagement, shared values, clear communication, and robust social support systems (Maguire & Hagan, 2009). Key indicators like life satisfaction, stress management capabilities, and interpersonal relationships also play a significant role (Rachmad, 2022). Conversely, national resilience heavily depends on the integrity of leadership, public trust, shared national values, comprehensive education, patriotism, and stable governance (Michael & Fishman, 2019). Major internal threats include economic instability, social division, and declining trust in leadership (Riabets, 2024). Externally, propaganda and psychological operations targeting civilians pose significant challenges. Critically, distrust in leaders, particularly when perceived as self-serving, directly erodes unity and weakens overall resilience (Michael & Fishman, 2019). Violations of equality and the perception of a one-sided state-citizen relationship further diminish public trust and cohesion. In essence, trust is the bedrock of resilience: its presence enables unity and strength, while its absence fundamentally undermines social and national capabilities.

For Indonesia, strengthening resilience and unity necessitates a strategic, multi-sectoral approach. Disaster management plans, for instance, should proactively leverage communities' inherent social strengths through comprehensive mitigation, preparedness, response, and recovery phases. Mitigation, in particular, should reflect a continuous learning process from past crises to enhance future responses. Societal resilience is notably supported by strong networks, effective stress management, adaptability, and learning derived from experience (Rachmad, 2022). Success in these endeavours is intrinsically linked to strong leadership, active community involvement, adequate resource availability, and effective conflict resolution mechanisms. Integrating social resilience considerations into broader security policy at the national level ensures a proactive shift towards long-term unity and preparedness (Riabets, 2024).

The concept of Sistem Pertahanan Semesta (Sishanta)

Sistem Pertahanan Semesta (*Sishanta*) represents Indonesia's overarching state defence system, a defensive framework designed to mobilise all national resources, including citizens, territories, artificial resources, natural resources, and infrastructure, for national security (Ismail & Priyanto, 2023). This comprehensive system is conceived for early preparation and continuous, integrated implementation, aiming to safeguard state sovereignty, maintain the territorial integrity of the Unitary State of the Republic of Indonesia (*Negara Kesatuan Republik Indonesia, NKRI*), and ensure the safety of the entire nation from all forms of threats (Susdarwono, 2020). Sishanta integrates both military and non-military defense capabilities to foster a robust and dignified national defense with high deterrence, addressing a broad spectrum of threats, including traditional military, non-military, and hybrid forms (Ismail & Priyanto, 2023). The "*semesta*" (universal) characteristic of Sishanta signifies the comprehensive involvement of the entire populace, all national resources, facilities, and the entirety of the national territory as a unified defense entity (Danga, 2023). This approach indicates a deliberate strategic choice by Indonesia to perceive national security threats as extending beyond conventional warfare, necessitating a society-wide response and a proactive, integrated approach to national resilience.

The legal foundation of Sishanta is deeply embedded within Indonesia's constitutional and legislative framework. The 1945 Constitution, particularly Article 30, declares defense and security to be the responsibility of all citizens, while Article 27(3) mandates every citizen's right and duty to participate in state defense (Nitit & Saksono, 2023). Law No. 3 of 2002 concerning National Defense further articulates Sishanta as a system involving all individuals, territories, and national resources in defending sovereignty, integrity, and safety (Ismail & Priyanto, 2023). Key components of this system include the Indonesian National Armed Forces (TNI) and the Police as the Main Components, with the People (*Rakyat*) serving as Supporting Components (Nitit & Saksono, 2023). The formation of "*Komponen Cadangan*" (reserve components) is also highlighted as a means to assist the TNI, particularly against non-military threats (Rusfiana, 2021). Citizen participation, known as "*Bela Negara*" (state defense education), is constitutionally mandated and implemented through civic education, compulsory basic military training, voluntary or compulsory TNI service, and professional service (Nitit & Saksono, 2023). This constitutionalisation of total defense and citizen duty ensures broad societal commitment and collective responsibility for national defense, providing long-term stability and legitimacy for this enduring characteristic of Indonesian statecraft.

Sishanta represents an evolution from its predecessor, the "*Sishankamrata*" (*Sistem Pertahanan Keamanan Rakyat Semesta*) (Danga, 2023). The foundational concept of "total people's defense" (*Pertahanan Rakyat Semesta or Perang Rakyat Semesta*) was initially formulated by General Abdul Haris Nasution, drawing from his extensive experiences in guerrilla warfare during Indonesia's independence struggle (Susdarwono, 2020). His seminal work, *Pokok Pokok Perang Gerilya* (1952-1955), became a cornerstone for Indonesian defense doctrine (Susdarwono, 2020). A significant doctrinal shift occurred in 2002, when

Sishankamrata was formally changed to Sishanta, notably omitting the words "*Keamanan*" (Security) and "*Rakyat*" (People) following constitutional amendments and the enactment of Law No. 3 of 2002 (Danga, 2023). This alteration was primarily driven by the desire to delineate the responsibilities of the TNI (defense) and the National Police (security). However, it faced criticism for potentially misinterpreting the broader concept of "National Security" versus localized "public order" (Danga, 2023). The removal of "*rakyat*" from the doctrine's name, despite "*semesta*" inherently implying comprehensive participation, highlighted a tension between the historical, organic "guerrilla ethos" of widespread involvement and the modern state's drive for formalized, structured, and professionalized defense.

In its strategic implementation, Sishanta is actively optimized to confront a diverse range of contemporary threats, including military, non-military, and hybrid forms, with particular attention to intangible threats such as information warfare, propaganda, economic attacks, and cyber warfare (Rusfiana, 2021). Cyberspace is now recognized as the fifth domain of warfare, alongside land, sea, air, and space (Ismail & Priyanto, 2023). Key optimization efforts, as outlined in the Indonesian Defense White Paper, include continuous modernization of military strength (e.g., C4I systems, strategic conventional weapons), robust development of science and technology, comprehensive strategic environment analysis (covering ideological, political, economic, socio-cultural, and homeland security aspects, including separatism and horizontal conflicts), proactive future threat forecasting, enhancement of international cooperation, and sustained development of state defense awareness among citizens (Ismail & Priyanto, 2023). The explicit focus on non-military, hybrid, and cyber threats demonstrates a clear recognition of the evolving nature of warfare beyond conventional military engagements, signifying a strategic pivot towards anticipating and preparing for asymmetric and non-traditional threats. A significant challenge to Sishanta's optimization is the constraint of limited defense budgets, which impedes modernization efforts and the ability to keep pace with the advanced military capabilities of other nations (Ismail & Priyanto, 2023).

Indonesia's unique archipelagic geography profoundly influences its defense doctrine and strategic planning (Susdarwono, 2020). The precursor to Sishanta, Sishankamrata, was explicitly formulated based on this Nusantara geography, characterized by its "*Kerakyatan, Kesemestaan, and Kewilayahan*" (populist, universal, and territorial) aspects (Danga, 2023). Defense geography is deemed indispensable for determining defense policies and strategies and the optimal utilization of natural resources and terrain for Sishanta's practical implementation, including meticulous spatial planning for static and dynamic defense areas (Susdarwono, 2020). This implies that Indonesia's vast and dispersed geography, which presents inherent challenges for a purely conventional defense, necessitates a "total" mobilization of all available resources and its population. The concept of total war, embodied by Sishanta, is deemed essential and must be maintained, particularly given Indonesia's recognition that it cannot conventionally overcome a superpower (Rusfiana, 2021). The "*semesta*" nature of Sishanta necessitates the comprehensive

mobilization of all national components: main, reserve, and supporting, to achieve its objectives (Nitit & Saksono, 2023). This geographical reality underpins the enduring relevance and strategic necessity of Sishanta, as a solely military defense would be insufficient for such a complex and expansive domain.

Psychological Operations (PSYOPs) and Strategic Communication in the Digital Era

Psychological operations (PSYOPs), historically termed psychological warfare, have consistently served as a core element of military strategy, aiming to shape perceptions, influence behavior, and steer decision-making (Saeed, 2024). Ancient theorists like Sun Tzu emphasized psychological manipulation as key to victory, illustrating the enduring relevance of such tactics (Ambrus, 2020). Over time, PSYOPs evolved alongside communication technologies, from printed pamphlets and rumors to the use of radio, cinema, and propaganda during the world wars (Ambrus, 2020). The Cold War further institutionalized disinformation and covert influence as strategic tools (Saeed, 2024).

Focused initially on battlefield morale, PSYOPs are now integral to national security policy, spanning peace and conflict alike. Definitions by the U.S. Department of Defense and NATO reflect this broader scope, highlighting the use of tailored messaging to affect perceptions, reasoning, and behavior in favor of political or military objectives (Ambrus, 2020). Information has thus emerged as a "fourth element of power," alongside diplomacy, economy, and military force (Ambrus, 2020).

Strategic PSYOPs today support long-term national objectives and often require interagency coordination (Lee, 2020). The digital age has radically transformed these operations, making them more systematic, personalized, and challenging to detect. Advances in AI, big data, deepfake technology, and social media have enabled both state and non-state actors to conduct targeted psychological profiling and execute large-scale influence campaigns, with cyberspace acting as a powerful force multiplier (Saeed, 2024). This shift from broad propaganda to hyper-targeted psychological manipulation is reflected in historical trends: deception and misinformation rose from 45% of conflicts pre-1900 to 70% in the 21st century, propaganda from 30% to 80%, cyber warfare from 0% to 85%, and AI-driven operations, nonexistent in previous centuries, now appear in 60% of modern conflicts (Saeed, 2024).

The digital information space is now a battleground where state and non-state actors conduct advanced psychological operations. Russia employs tactics reminiscent of Soviet-era "Active Measures", including disinformation and troll messaging, as seen in the 2016 U.S. election, using information warfare as a constant soft power tool (Lee, 2020). China manages a vast network of online trolls, estimated at two million, to suppress dissent, advance nationalist narratives, and support foreign policy, embedding "cognitive warfare" into its military doctrine (Lee, 2020, pp. 26–27). Iran, Venezuela, and several other U.S. adversaries collaborate to erode American influence globally (Lee, 2020). Meanwhile, non-state actors like ISIS and Al-Qaeda exploit social media for recruitment, propaganda, and intimidation, achieving broad reach and attracting foreign fighters (Lee, 2020).

A primary concern lies in the disparity of constraints: authoritarian regimes and extremist groups operate with fewer legal and moral boundaries, enabling them to deploy more aggressive and deceptive tactics (Henschke et al., 2024). This raises serious concerns over misinformation, democratic erosion, and declining public trust issues, worsened by the rise of deepfake technology (Saeed, 2024).

Despite the growing urgency, efforts to enhance PSYOP capabilities remain hindered by bureaucratic rivalries and a stigma surrounding the term. Proposals to establish a Joint PSYOP Centre have been stalled by inter-agency competition (Lee, 2020). The rapid dismantling of the Office of Strategic Influence post-9/11, triggered by negative media coverage and political infighting, illustrates how internal resistance can derail strategic initiatives (Lee, 2020). The term "PSYOP" itself is often linked to propaganda and manipulation, perceived as morally problematic, especially during peacetime, discouraging officials from supporting such programs (Lee, 2020).

METHODOLOGY

This study employed a literature review methodology to analyze the strategic application of Sishanta's inherent psychological principles in enhancing societal resilience and national unity amidst digital threats. This method is particularly appropriate for addressing research questions aimed at providing an overview of a specific issue or tracing the development of a topic over time (Snyder, 2019). The review drew upon various sources, including academic journals, government publications, and relevant reports, to comprehensively understand Sishanta and its psychological dimensions.

The search strategy used keywords related to Sishanta, national defense, psychological operations, digital threats, and societal resilience. Inclusion criteria focused on sources addressing the Indonesian context and examined the relationship between psychological factors and national defense strategies. The analysis synthesized key themes and arguments from the literature to explore how Sishanta's psychological foundations can be effectively utilized in the digital era, emphasizing interpretation and direction for future research (Schryen, 2015). This approach supported formulating policy recommendations to strengthen Indonesia's capacity to respond to evolving digital threats.

RESEARCH RESULT

Reinterpreting Sishanta for the Digital Age

Indonesia's defense doctrine, Sishanta, is a total defense system designed to mobilize all elements of national power, including citizens, territory, and resources, to respond to various threats (Huda et al., 2024). In the digital age, this doctrine remains conceptually robust. Rather than requiring a complete overhaul, Sishanta's inclusive and universal structure allows for its seamless extension into emerging domains such as cyberspace and information warfare. The proliferation of disinformation, digital propaganda, and cultural dilution through online platforms exemplifies threats no longer confined to conventional warfare. These new realities expand the defense scope to include safeguarding cultural identity and informational sovereignty as part of national security.

Large Language Models (LLMs) such as GPT-4 offer a sophisticated toolset to support national cybersecurity efforts in this evolving landscape (Cimmino, 2024). Through advanced natural language processing, LLMs can identify patterns in massive text volumes, detect cyber threat indicators, and automate real-time responses. Tools like Open Interpreter enhance these capabilities by allowing LLMs to directly interact with system terminals, run diagnostics, conduct penetration tests, and deploy code within secure parameters (Cimmino, 2024). This level of automation increases response speed and reduces the likelihood of human error. Furthermore, LLMs can be integrated into intelligent firewall systems that dynamically adapt to new threat vectors, strengthening resilience across digital infrastructure. However, the same capabilities that enable defensive innovation can also be weaponized. The dual-use nature of LLMs allows for the acceleration of malicious activities such as automated phishing, malware generation, and advanced intrusion techniques. This reality necessitates a proactive and anticipatory posture, including robust regulatory oversight, technical safeguards, and adherence to emerging standards like the OpenAI Model Specification and Constitutional AI.

In parallel, digital defense also demands attention to cultural resilience. The Digital House of Knowledge (DHOK), introduced as a framework for preserving and transmitting Indigenous knowledge, provides a compelling example of how cultural continuity can be maintained in digital spaces (Cordova, 2024). The DHOK concept originates from the United States, specifically the Oglala Lakota Oyate in South Dakota. Designed as a secure and community-driven repository, the DHOK offers a platform for intergenerational knowledge exchange, digital sovereignty, and the reinforcement of traditional lifeways (Cordova, 2024). Such a model is particularly relevant for culturally diverse nations like Indonesia. Amid the pressures of globalization, Indonesian youth engage heavily with global media while continuing to express respect for traditional norms through batik, participation in religious festivals, and preservation of local languages (Sanmee, 2024). The DHOK concept aligns with efforts to resist cultural erosion, serving as a digital safeguard for national identity and values.

Integrating advanced cybersecurity technologies and culturally rooted digital infrastructure can redefine Sishanta into a more comprehensive national defense paradigm. LLMs reinforce external digital defense through real-time threat mitigation, while initiatives like DHOK strengthen internal defense by preserving intangible cultural heritage. This dual-layered approach enhances technological capability and sustains the socio-cultural foundation of national resilience. Regulatory and ethical frameworks and community-driven data governance create the environment for responsibly deploying AI technologies. Institutional collaboration between cybersecurity experts, technology developers, and cultural stewards is essential for harmonizing technological progress with national integrity. Sishanta, as a living doctrine, evolves by embracing such innovations while remaining anchored in its foundational principles. In the digital era, this reinterpretation ensures that defense efforts protect physical sovereignty and the informational and cultural domains that define Indonesia's national identity.

Key Psychological Dimensions of Sishanta

The development of human resources within Sishanta is viewed as fundamentally intertwined with broader national development, encompassing human development as both "human capital" and "human resources". This perspective highlights a symbiotic relationship where investment in human development for national progress simultaneously strengthens defense capabilities. The psychological attributes cultivated for societal well-being, such as resilience, skills, and knowledge, directly contribute to a robust defense posture, blurring the lines between civilian and military preparedness. Developing the "resilience and well-being of human resources" is essential for preparing individuals to face potential threats. This implies that defense is not an isolated sector but deeply integrated into the fabric of national development and human flourishing, positioning a psychologically healthy, skilled, and resilient populace as the ultimate defense asset.

Thus, Sishanta, as a defense system, relies heavily on psychological dimensions extending beyond conventional military strength (Huda et al., 2024). A foundational psychological aspect is the "psychological arming" of individuals, achieved through the "cultivating the values of the Pancasila ideology" (Poespitohadi et al., 2019). This process is deeply intertwined with human resources development, which is "the most crucial resource and the element that determines the development of civilization, including the aspect of national defense" (Kurnia et al., 2023). Essential psychological qualities for these human resources include "reason, feelings, abilities, skills, and knowledge" (Kurnia et al., 2023), all contributing to a populace capable of supporting national defense efforts.

Beyond individual attributes, broader cultural orientations significantly shape the psychological landscape for national defense. Cultural psychology highlights the independent versus interdependent self and individualism versus collectivism (Kitayama & Salvador, 2024). These cultural dimensions influence collective psychological processes, with comparative culturology emphasizing that societal cultures are "wholes" whose internal logic differs from individual personality dynamics (Minkov et al., 2024). Within Sishanta, these societal-level psychological factors contribute to "psychological defense" and foster "national defense awareness" (Huda et al., 2024), indicating a collective psychological readiness for defense.

In Indonesia, a non-Western nation, the self-concept is predominantly "interdependent with others in their ingroups" (Kitayama & Salvador, 2024). This aligns seamlessly with the collective nature of Sishanta, where national defense is explicitly stated as the "responsibility of all elements of the nation" (Huda et al., 2024). Crucially, specific cultural values like "religiosity and local genius values" have been empirically shown to influence "the intention of learning Social Psychology" among Indonesian students (Murjito et al., 2024). Even among the urban middle class, these values influence consumer behavior, suggesting their pervasive impact on societal attitudes and actions (Murjito et al., 2024). The confluence of a general interdependent cultural orientation with these

specific local psychological drivers creates a robust, culturally resonant foundation for Sishanta in Indonesia.

The inherent interdependent self-construal of the Indonesian populace, coupled with the demonstrated influence of religiosity and local wisdom, provides a unique and robust psychological foundation for Sishanta. These deep-seated cultural traits foster a collective orientation that is highly conducive to the "universal" and "whole-of-nation" approach required for national defense (Huda et al., 2024). Therefore, understanding and strategically leveraging these culturally specific psychological dimensions are paramount for enhancing national defense awareness, building human resource resilience, and ultimately strengthening Indonesia's comprehensive defense system against military and non-military threats.

DISCUSSION

Cultural Psychology as the Foundation of Psychological Defense in Sishanta

The profound influence of culture on psychological processes, as highlighted by cultural psychology, directly applies to the domain of national defense (Kitayama & Salvador, 2024). The interdependent self-construal, prevalent in Indonesia as a non-Western nation, naturally aligns with the collective and universal nature of Sishanta. This contrasts with defense models rooted in Western individualistic approaches, which may not resonate as effectively in a collectivist context (Kitayama & Salvador, 2024). The emphasis on the "resilience and well-being of human resources" within Sishanta gains further depth when viewed through an interdependent lens, where collective well-being directly contributes to national resilience (Kurnia et al., 2023).

The significance of "religiosity and local wisdom" as specific cultural drivers of collective behavior and the "intention of learning" in Indonesia cannot be overstated (Murjito et al., 2024). These are not merely abstract values but tangible psychological factors that influence engagement with national defense. The "psychological arming" and "cultivating values" within Sishanta can be effectively implemented by integrating these deeply ingrained Indonesian cultural and religious frameworks (Poespitohadi et al., 2019).

Understanding Sishanta as a national system benefits significantly from the distinction between individual-level psychology and societal-level culturology (Minkov et al., 2024). Sishanta is best understood through a culturological lens, focusing on aggregated societal values and norms that shape collective defense efforts. This perspective acknowledges that "cultures are not king-size individuals" and possess their internal logic (Minkov et al., 2024). While interdependence forms a strong foundation, it is important to recognize that "interdependence takes on diverse forms within these cultural contexts" (Kitayama & Salvador, 2024), suggesting nuances in how Sishanta might be implemented across Indonesia's diverse regions.

Furthermore, the observation that Western societies are "psychologically atypical" due to their emphasis on independence carries a critical implication (Kitayama & Salvador, 2024): defense strategies and psychological interventions derived from Western, individualistic models may be ineffective or counterproductive in an interdependent, non-Western context like Indonesia.

The universal nature of Sishanta, while implying broad participation, must be culturally sensitive and leverage indigenous psychological strengths rather than imposing potentially misaligned foreign frameworks. The peculiar idea of the independent self (Kitayama & Salvador, 2024) is fundamentally at odds with the collective spirit required for Sishanta. For Sishanta to be truly effective, its psychological underpinnings must be indigenized, and Indonesia's unique cultural psychology must be acknowledged and built upon.

The cultural norms surrounding emotional expression and "feeling rules" also play a role in collective defense, particularly in countering non-military threats like disinformation (Huda et al., 2024). Suppose Indonesian culture, similar to other East and Southeast Asian cultures, is less influenced by highly arousing harmful content compared to Western contexts. In that case, spreading "hoaxes and intolerant issues" (Murjito et al., 2024) might operate through different emotional pathways or normative pressures. Understanding Indonesia's emotional climate and "feeling rules" is crucial for developing effective psychological defense mechanisms against non-military threats. Psychological defense strategies within Sishanta must be culturally attuned to how emotions are experienced, expressed, and regulated within Indonesian society to effectively counter threats like disinformation and radicalization (Murjito et al., 2024).

Sishanta Strategic Applications in the Digital Era for Societal Resilience and National Unity

The digital era has profoundly transformed warfare, enabling sophisticated PSYOPs that leverage social media, artificial intelligence (AI), and data analytics to influence perceptions, manipulate narratives, and destabilize societies (Nawaz, 2025). These non-physical threats, though intangible, wield impacts as significant as military incursions, eroding national identity, and fostering conflicting ideologies (Huda et al., 2024).

By design, the inherent comprehensiveness of Sishanta offers an asymmetric advantage against the pervasive and borderless nature of digital PSYOPs. While traditional defense systems often struggle to adapt their kinetic-centric frameworks to such ambiguous, non-physical attacks (Jaeni et al., 2025)Sishanta's foundational principle of mobilizing all societal components intrinsically extends defense into the social, cultural, and informational domains. This pre-existing holistic structure is conceptually agile, transforming the widespread reach of the digital realm from merely a vulnerability into a potential strength for national resilience.

The strategic application of Sishanta against digital PSYOPs critically depends on empowering its non-military components through targeted education and technological integration, thereby cultivating robust societal resilience. Sishanta's non-military defense is designed to enhance national welfare by leveraging ideological, political, economic, socio-cultural, informational, and technological factors through diverse professions and expertise (Huda et al., 2024). A cornerstone of this approach is "*Bela Negara*" (state defense education), which prepares citizens as the front line against non-military threats. This educational framework can be strategically reoriented to function as

a national cognitive inoculation program. By integrating explicit modules on digital literacy, critical evaluation of online content, and recognition of manipulation tactics, such as deepfakes, automated bots, and social engineering, into the "*Bela Negara*" curriculum, Indonesia can proactively fortify its populace against the psychological impacts of digital warfare.

This directly addresses the documented susceptibility of individuals with lower digital literacy to misinformation and mitigates the erosion of trust and potential for radicalization caused by PSYOPs (Nawaz, 2025). Furthermore, integrating advanced technologies like AI, big data, and the Internet of Things (IoT) offers opportunities to strengthen defense systems through enhanced detection and rapid response capabilities (Jaeni et al., 2025), with AI-driven content verification as a critical technological countermeasure.

Beyond individual resilience, Sishanta's emphasis on inter-ministerial coordination and the cultivation of national resilience provides a robust framework for a unified national response, directly countering the divisive aims of digital PSYOPs and strengthening national unity. PSYOPs are designed to "polarize societies, disrupt elections, and create cognitive biases" (Nawaz, 2025), ultimately aiming to damage national identity and introduce conflicting ideologies by trashing the information space with multiple truths (Rugge, 2018). In contrast, national resilience is defined as a dynamic condition that ensures the nation's identity, integrity, and survival by developing national strength across all dimensions (Huda et al., 2024).

This concept acts as a comprehensive counter-narrative to the fragmentation and cognitive hacking targeted by digital PSYOPs. By actively fostering this holistic national resilience across ideological, political, economic, socio-cultural, and technological spheres, Sishanta moves beyond merely reacting to disinformation. It proactively builds a shared national consciousness and strengthens collective identity, for instance, by promoting Pancasila as the national ideology.

This approach makes society inherently more resistant to manipulative narratives, ensuring national unity through top-down directives and a deeply ingrained societal ethos, reinforcing the collective responsibility of all national elements in maintaining cohesion. Moreover, the imperative for coordination and synergy between ministries and related institutions allows for early detection and rapid response mechanisms to counter emerging digital threats effectively (Nawaz, 2025).

Despite its inherent strengths, Sishanta faces significant challenges in the digital era, necessitating continuous adaptation, interdisciplinary collaboration, and flexible policy frameworks to safeguard Indonesia's information ecosystem and national cohesion effectively. A primary challenge is the persistent gap between rapid technological development and slow regulatory updates (Hwang & Rosen, 2017), which can compromise the effectiveness of the defense (Jaeni et al., 2025). The inherent "difficulty of attribution" in cyberspace and the transnational nature of cyber threats further complicate legal and policy responses, underscoring the need for robust international collaboration (Rugge, 2018).

For Sishanta to remain effective, Indonesia must prioritize developing a highly flexible and proactive legal and policy framework that can rapidly adapt to new digital threats, moving towards anticipatory governance. This is crucial given that the development and use of non-military defense forces is currently unclear and not well synergized (Huda et al., 2024). Such an agile regulatory environment must also carefully balance security imperatives with fundamental rights, as the use of advanced technologies, particularly AI, in defense raises significant ethical and human rights concerns regarding privacy and accountability (Jaeni et al., 2025). Interdisciplinary collaboration among governments, technology companies, researchers, and civil society, including public-private partnerships, is paramount for developing comprehensive countermeasures (Hwang & Rosen, 2017). Ultimately, by fostering adaptive governance and broad societal engagement, Indonesia can mitigate the risk of public trust erosion or rights violations, thereby preserving the societal resilience and national unity that Sishanta endeavors to build.

CONCLUSIONS AND RECOMMENDATIONS

Indonesia's Universal Defense System, Sishanta, is a culturally rooted, whole-of-nation strategy designed to protect national sovereignty from military and non-military threats, including digital-era challenges like disinformation and psychological operations (PSYOPs). Its strength lies in mobilizing all national elements, people, territory, and resources, and in its psychological dimension, grounded in Indonesia's collectivist culture, religiosity, and local wisdom.

Unlike Western individualistic models, Sishanta's communal values align naturally with defense efforts, fostering national awareness and psychological arming. To counter digital PSYOPs that erode identity and unity, Sishanta must strengthen non-military components. This includes updating Bela Negara education to include digital literacy and critical thinking, serving as a form of cognitive defense. AI and big data can further enhance threat detection and response, while initiatives like the Digital House of Knowledge (DHOK) reinforce cultural resilience.

However, Sishanta faces challenges: slow regulatory adaptation, cyber attribution difficulties, and weak coordination among non-military actors. Overcoming these requires flexible policies, interdisciplinary cooperation, public-private partnerships, and a balance between security and civil liberties.

Despite its strengths, Sishanta faces challenges, including rapid technological change versus slow regulatory adaptation, difficulty attributing cyber threats, and the need for clearer synergy among non-military defense forces. Therefore, continuous adaptation, flexible policy frameworks, robust interdisciplinary collaboration (including public-private partnerships), and a careful balance between security imperatives and fundamental rights are essential for Sishanta to effectively protect Indonesia's information ecosystem, preserve public trust, and ensure enduring national cohesion in an increasingly complex global environment. Understanding Sishanta's psychological and cultural dimensions yields several key policy recommendations for strengthening Indonesia's defense posture:

a. Leverage collectivism and interdependence

Policies should reinforce collective identity and community responsibility rather than rely on individualistic incentives. This aligns with Indonesia's non-Western cultural foundation, which naturally predisposes citizens toward collective action and participation in Sishanta.

b. Integrate religiosity and local wisdom

Religious values and local wisdom should be embedded in Sishanta's educational and awareness campaigns, as they significantly influence learning intention and behavior. Community-based initiatives—especially those led by religious or local leaders can help disseminate defense awareness in ways that resonate with local culture.

c. Culturally tailored psychological arming

Defense narratives must be framed through the lens of Pancasila and local cultural values to ensure they connect with Indonesia's collective psyche. This culturally attuned messaging enhances the internalization of national defense values.

d. Implement targeted psychological defense strategies

Non-military threats like disinformation and radicalization must be addressed through focused psychological defense. The rise of intolerance and radical behavior among youth, fueled by hoaxes and divisive content, represents a serious internal vulnerability. Sishanta must proactively counter these threats by using social psychology insights and researching the population's specific emotional and cultural responses to disinformation.

e. Foster interdisciplinary collaboration

A collaborative approach involving defense strategists, psychologists, sociologists, and cultural experts is essential to develop comprehensive, culturally grounded Sishanta policies that are both effective and sustainable.

Thus, Sishanta's success in the digital age depends on adapting its culturally grounded strengths to address complex, evolving non-military threats.

ADVANCED RESEARCH

While aiming to bridge the gap between Indonesia's traditional defense doctrine and modern digital threats, this study acknowledges several limitations. Primarily, its reliance on a literature review methodology means the findings are conceptual and theoretical, lacking empirical data or case studies to validate the proposed strategic applications of Sishanta's psychological dimensions. Furthermore, while it emphasizes the importance of cultural psychology, the study does not delve into the specific nuances of how the "interdependent self"

or "religiosity and local wisdom" would translate into actionable, measurable psychological defense strategies across Indonesia's diverse cultural landscape.

Future research could address these limitations by conducting empirical studies, such as surveys or experiments, to assess the effectiveness of proposed digital literacy and psychological inoculation programs within the "Bela Negara" framework. Additionally, comparative studies analyzing how different cultural groups within Indonesia respond to digital disinformation, coupled with qualitative research exploring community-led initiatives for cultural resilience in the digital sphere, would provide valuable insights for refining Sishanta's application in the digital era.

ACKNOWLEDGMENT

I extend my deepest gratitude to God for divine guidance, unwavering strength, and the countless blessings throughout my academic journey. Your grace has been my greatest motivation. To my friends, thank you for your invaluable companionship, understanding, and timely distractions that helped maintain my sanity. Finally, my sincerest appreciation goes to my journal supervisor, whose insightful suggestions, rigorous guidance, and unwavering patience were instrumental in shaping this paper. Your expertise and dedication have significantly enriched my research and writing.

REFERENCES

Ambrus, É. (2020). Of Ends and Means: The Integration of Psychological Operations and Cyber Operations. *Honvédségi Szemle – Hungarian Defence Review*, *148*(2), 102–111. https://doi.org/10.35926/HDR.2020.2.7

Cimmino, G. (2024). Large Language Models in Cybersecurity: Digital Defense and Ethical Challenges. *TechRxiv*. https://doi.org/10.36227/TECHRXIV.172417964.40874339/V2

Cordova, J. C. (2024). *Creating A Digital House of Knowledge Ensuring The Continuation and Integrity of Indigenous Knowledge Transfers in The Digital Era* [University of Alaska Fairbanks]. https://www.proquest.com/openview/6f9572abe1dda838d2aac7d0ae26d934/1?pq-origsite=gscholar&cbl=18750&diss=y

Danga, C. M. (2023). Perkembangan Doktrin Sistem dan Keamanan Negara Indonesia. *JUSTISI*, *9*(2), 104–115. https://doi.org/10.33506/JURNALJUSTISI.V9I2.2329

Henschke, A., Miller, S., Alexandra, A., Walsh, P. F., & Bradbury, R. (2024). The Ethics of National Security Intelligence Institutions. In *The Ethics of National Security Intelligence Institutions: Theory and Applications*. Taylor & Francis. https://doi.org/10.4324/9781003106449

Huda, A. V., Iswantono, I., & Kristin, L. (2024). Strategi Pertahanan pada Pengembangan Penggunaan Kekuatan Militer dan Non Militer. *JIIP - Jurnal Ilmiah Ilmu Pendidikan*, *7*(9), 10897–10901. https://doi.org/10.54371/JIIP.V7I9.5876

Hwang, T., & Rosen, L. (2017). *Harder, Better, Faster, Stronger: International Law and the Future of Online PsyOps*. https://demtech.oii.ox.ac.uk/wp-

content/uploads/sites/12/2017/02/Comprop-Working-Paper-Hwang-and-Rosen.pdf

Ismail, F., & Priyanto. (2023). Optimization of the Total Defense System in Facing National Securities Challenges to Defend State Sovereignty. *European Journal of Humanities and Social Sciences*, *3*(6), 49–54. https://doi.org/10.24018/EJSOCIAL.2023.3.6.499

Jaeni, A., Ignatius, S. B., & Karsoma, A. (2025). A Literature Review on The Transformation of Defense Law in The Digital Age and Advanced Technology. *TOFEDU: The Future of Education Journal*, *4*(4), 821–829. https://doi.org/10.61445/TOFEDU.V4I4.500

Kitayama, S., & Salvador, C. E. (2024). Cultural Psychology: Beyond East and West. *Annual Review of Psychology*, *75*(Volume 75, 2024), 495–526. https://doi.org/10.1146/ANNUREV-PSYCH-021723-063333/CITE/REFWORKS

Kurnia, R. R., Saputro, G. E., & Murtiana, S. (2023). Management of human resources in national defense depends on the defense economics point of view. *International Journal on Social Science, Economics and Art* , *13*(1), 1–11. https://doi.org/10.35335/IJOSEA.V13I1.201

Lee, S. (2020). *Strategic Psychological Operations Capability Development: Why Is It Taking So Long?* [Naval Postgraduate School]. https://hdl.handle.net/10945/66672

Maguire, B., & Hagan, P. (2009). Disasters and Communities: Understanding Social Resilience | The Australian Journal of Emergency Management. *The Australian Journal of Emergency Management*, *22*(2). https://search.informit.org/doi/abs/10.3316/informit.839750155412061

Michael, K., & Fishman, J. (2019). The Social Components of National Resilience: A Conceptualization of the Term. *National Resilience, Politics and Society*, *1*, 5–21. https://doi.org/10.26351/NRPS/1/1

Minkov, M., Vignoles, V. L., Welzel, C., Akaliyski, P., Bond, M. H., Kaasa, A., & Smith, P. B. (2024). Comparative Culturology and Cross-Cultural Psychology: How Comparing Societal Cultures Differs from Comparing Individuals' Minds Across Cultures. *Journal of Cross-Cultural Psychology*, *55*(2), 164–188. https://doi.org/10.1177/00220221231220027/ASSET/55B1AADA-0889-40A1-A09C-9B4DE8C2A4DE/ASSETS/IMAGES/LARGE/10.1177_00220221231220027-FIG4.JPG

Murjito, W. H., Nugroho, A. J. S., Pratomo, S. A., Prasetyo, J., Anisa, I., & Tasari, T. (2024). Relıgıosıty, Local Wısdom, And Socıal Psychology. *Asian Journal of Management, Entrepreneurship and Social Science*, *4*(01), 525–535. https://doi.org/10.63922/AJMESC.V4I01.622

Nawaz, F. (2025). Psychological Warfare in the Digital Age: Strategies, Impacts, and Countermeasures. *Journal of Future Building*, *2*(1), 21–30. https://www.researchcorridor.org/index.php/jfb/article/view/314

Nitit, Y. W., & Saksono, M. S. (2023). Prinsip dan Dinamika Sistem Pertahanan Negara Kesatuan Republik Indonesia Dalam Keikutsertaan Rakyat.

JURNAL MAHATVAVIRYA, *10*(1), 1–14. https://ojs.akmil.ac.id/index.php/mahatvavirya/article/view/62

Poespitohadi, W., Zauhar, S., Haryono, B. S., Amin, F., Fanani, Z., & Hermawan, R. (2019). The implementation of defense development policy with blended learning technology. *International Journal of Engineering and Advanced Technology*, *8*(6 Special Issue 3), 415–421. https://doi.org/10.35940/IJEAT.F1075.0986S319

Rachmad, Y. E. (2022). Social Resilience Theory. In *Aix-en-Provence Cézanne Éditions Internationales*. Aix-en-Provence Cézanne Éditions Internationales. https://doi.org/10.17605/OSF.IO/Z5ERQ

Riabets, K. (2024). Theoretical foundations of the interconnection between national and social resilience and state policy of national security. *Честь і Закон*, *89*(2).

Rugge, F. (2018). *"Mind Hacking" Information Warfare in The Cyber Age* (319). https://www.ispionline.it/sites/default/files/pubblicazioni/analisi319_rugge_11.01.2018_1.pdf

Rusfiana, Y. (2021). Aktualisasi Sistem Pertahanan Rakyat Semesta (SISHANTA) dan Dinamika Potensi Ancaman. *Moderat : Jurnal Ilmiah Ilmu Pemerintahan*, *7*(3), 483–492. https://doi.org/10.25157/MODERAT.V7I3.2482

Saeed, Prof. H. (2024). Minds at War: The Evolution of Psychological Tactics in Conflict Scenarios. *Journal of Future Building*, *1*(3), 32–41. https://www.researchcorridor.org/index.php/jfc/article/view/304

Sanmee, W. (2024). Cultural Identity and Globalization: Navigating Tradition and Modernity in Southeast Asia. *Journal of Exploration in Interdisciplinary Methodologies (JEIM)*, *1*(1), 11–20. https://so19.tci-thaijo.org/index.php/JEIM/article/view/605

Schryen, G. (2015). Writing Qualitative IS Literature Reviews—Guidelines for Synthesis, Interpretation, and Guidance of Research. *Communications of the Association for Information Systems*, *37*(1), 12. https://doi.org/10.17705/1CAIS.03712

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, *104*, 333–339. https://doi.org/10.1016/J.JBUSRES.2019.07.039

Susdarwono, E. T. (2020). Defense Geography and The Character of The Indonesian Total Defense System (SISHANTA). *JURNAL GEOGRAFI Geografi Dan Pengajarannya*, *18*(2), 129–138. https://doi.org/10.26740/JGGP.V18N2.P129-138

Trubavina, I., Cherednychenko, O., & Oliinyk, N. (2024). Integration Measures in Communities as a Way to National Unity, Cohesion and Ensuring the National Country Interests. *Educational Challenges*, *29*(1), 175–191. https://doi.org/10.34142/2709-7986.2024.29.1.12