

Building Pancasila-Based Cognitive Defense: A Conceptual Framework For Countering Cognitive Warfare In Indonesia

Gema Merdeka Goeryadi¹
Universitas Narotama, Surabaya Indonesia

Muhammad Yusuf²
Politeknik Praktisi Bandung

Correspondence : Gema Merdeka Goeryadi (gema.merdeka@narotama.ac.id)

ABSTRACT

Cognitive warfare has emerged as a new domain of conflict that targets human perception, belief, and decision-making through information manipulation, algorithmic amplification, and the exploitation of cognitive biases. Indonesia, with more than 200 million internet users and a highly plural society, is considerably exposed to disinformation, identity-based polarization, and foreign influence operations. This article aims to develop a conceptual framework of cognitive defense grounded in Pancasila as the ideological, ethical, and epistemic foundation of national resilience. Using a qualitative approach based on a semi-systematic narrative literature review and conceptual analysis, the study synthesizes literature on cognitive warfare, psychological inoculation, media literacy, and Pancasila studies. The results propose the *Pancasila Cognitive Defense Framework* (PCDF), consisting of three layers value foundation, cognitive capacity, and institutional ecosystem operationalized through five pillars derived from the five principles of Pancasila: spiritual-ethical integrity, critical humanism, inclusive national identity, deliberative reasoning, and digital social justice. The framework positions Pancasila not merely as a normative doctrine but as a living cognitive “immune system” that strengthens individual and collective resilience. The study recommends integrating the framework into state defense education, digital literacy programs, and inter-agency coordination within Indonesia’s Total People’s Defense System.

Keyword: cognitive warfare; cognitive defense; Pancasila; national resilience; disinformation

INTRODUCTION

Advances in information and communication technology have fundamentally transformed the character of conflict, both between states and within societies. Whereas conventional warfare relies on control over land, sea, and air, contemporary conflict is increasingly shifting toward an invisible domain: the human mind. The concept of *cognitive warfare* refers to systematic efforts to influence how individuals and groups perceive reality, form beliefs, and make decisions in order to gain strategic advantage without resorting to physical force (Bernal et al., 2020; Claverie & du Cluzel, 2022). Within this paradigm, the human brain is treated as the battlefield, while social media, algorithms, and narratives become its weapons.

Indonesia is among the countries most vulnerable to this phenomenon. An internet user base exceeding 200 million people, intensive social media use, and a high degree of ethnic, religious, racial, and inter-group diversity (known locally as SARA) make Indonesia’s information space fertile ground for disinformation and polarization. Electoral experiences over the past decade have shown how identity-based narratives, coordinated anonymous

accounts, and paid online influencers (*buzzers*) can deepen social segregation (Lim, 2017; Bradshaw & Howard, 2019). On a broader scale, geopolitical competition in the Indo-Pacific opens the possibility of foreign influence operations targeting Indonesian public opinion on issues of sovereignty, the economy, and foreign policy.

The state's response to threats in the information space has thus far tended to be reactive and technical, such as content blocking, hoax labeling, and law enforcement against those spreading false news. While these measures are important, they do not address the root of the problem, namely citizens' cognitive resilience in sorting, interpreting, and responding to information. Approaches focused solely on "content takedown" also risk conflicting with freedom of expression and may erode public trust. A defense paradigm that is preventive, value-based, and inclusive of all components of the nation is therefore required.

Pancasila, as the foundation of the state and the national ideology, holds significant potential to serve as the basis for such cognitive defense. To date, Pancasila has more often been positioned as material for indoctrination or as a normative symbol, rather than as an epistemic framework capable of equipping citizens with clear, critical, and unity-oriented ways of thinking. Yet the values embodied in its five principles—belief in God, humanity, unity, democracy guided by wisdom in deliberation, and social justice—substantively intersect with the principles of resilience against information manipulation, such as honesty, empathy, shared identity, deliberative reasoning, and equitable access (Latif, 2011; Kaelan, 2013).

Studies of cognitive warfare in Indonesia remain relatively limited and tend to borrow frameworks from NATO member states or Taiwan's experience without considering Indonesia's ideological and socio-cultural context. Conversely, Pancasila studies are rarely linked explicitly to the literature on cognitive psychology and information security. This article seeks to fill that gap. Accordingly, it addresses two research questions: (1) what are the characteristics of the cognitive warfare threat in the Indonesian context; and (2) how can the values of Pancasila be operationalized into a conceptual framework of cognitive defense? The contribution of this article lies in formulating a *Pancasila Cognitive Defense Framework* that integrates the dimensions of values, cognitive capacity, and institutions into a single coherent model.

LITERATURE REVIEW

The Concept of Cognitive Warfare

The term *cognitive warfare* gained wide attention after NATO Allied Command Transformation made it a focus of its concept development work. Bernal et al. (2020) define cognitive warfare as a form of conflict that seeks to change not only what people think but also

how they think and act. Claverie and du Cluzel (2022) emphasize that cognitive warfare goes beyond information warfare because its target is not merely the flow of information but mental processes themselves, including emotion, memory, and decision-making mechanisms. Cognitive warfare thus combines elements of psychological operations, propaganda, cyber warfare, and neuroscience along a single spectrum.

Historically, the idea of influencing an adversary's mind is not new. The concept of *netwar* proposed by Arquilla and Ronfeldt (1997) anticipated network-based conflict targeting what a society knows or believes. What distinguishes the present era, however, is scale, speed, and precision. Digital platforms enable microtargeting based on behavioral data, while recommendation algorithms foster *echo chambers* and *filter bubbles* that reinforce pre-existing beliefs (Pariser, 2011; Sunstein, 2017). Hung and Hung's (2022) study of Taiwan's experience shows that cognitive warfare can be waged continuously in peacetime, exploits domestic political divisions, and is difficult to attribute to a specific state actor.

Cognitive Vulnerability and Information Disorder

The effectiveness of cognitive warfare rests on inherent vulnerabilities in the way humans process information. Kahneman (2011) distinguishes between two systems of thinking: System 1, which is fast, intuitive, and emotional, and System 2, which is slow, analytical, and reflective. The fast-paced social media environment tends to activate System 1, making individuals more susceptible to confirmation bias, the availability heuristic, and reasoning motivated by group identity. Wardle and Derakhshan (2017) introduce the concept of *information disorder*, distinguishing misinformation (false information shared without intent to harm), disinformation (false information deliberately spread to cause harm), and malinformation (genuine information used to cause harm). This classification matters because cognitive warfare does not always rely on falsehoods; it often exploits partial truths framed manipulatively.

Lewandowsky, Ecker, and Cook (2017) show that correcting misinformation after it has spread is often ineffective due to the *continued influence effect*: false information continues to shape reasoning even after it has been corrected. This finding strengthens the argument that cognitive defense should emphasize prevention and resilience-building rather than post-attack remediation.

Cognitive Resilience and Psychological Inoculation

One of the most widely studied preventive approaches is inoculation theory, developed by McGuire (1961). Analogous to vaccination, individuals exposed to a weakened form of a persuasive argument together with its refutation develop cognitive "antibodies" against similar

persuasion in the future. Van der Linden et al. (2017) and Roozenbeek and van der Linden (2019) developed this approach into *prebunking*, which equips the public with an understanding of manipulation techniques such as emotional language, polarization, impersonation, conspiracy theories, and trolling before they encounter disinformation. Experimental results show that game-based interventions can significantly improve people's ability to recognize manipulative content.

Beyond inoculation, media and digital literacy are recognized as a foundation of cognitive resilience. Hobbs (2010) views digital literacy not merely as a technical skill but as the competence to access, analyze, create, reflect, and act responsibly within the information ecosystem. However, several studies caution that literacy that is purely cognitive-technical is insufficient if individuals remain emotionally bound to polarized group identities. This is where the dimensions of values and identity become relevant.

Pancasila as a Foundation of National Resilience

Pancasila was formulated by the nation's founders as the *philosophische grondslag*, or philosophical foundation of the state (Soekarno, 1945). Notonagoro (1975) emphasizes the hierarchical-pyramidal and unified-plural character of Pancasila, meaning that its five principles form an organic whole in which each principle animates the others. Latif (2011) reads Pancasila as a common denominator that enables a plural society to live together, as well as a guiding star for public ethics. Kaelan (2013) positions Pancasila not only as the foundation of the state but also as a philosophical system with ontological, epistemological, and axiological dimensions.

In defense doctrine, Law No. 3 of 2002 on State Defense establishes a total defense system involving all citizens, territory, and national resources. The Indonesian Defense White Paper (Ministry of Defense of the Republic of Indonesia, 2015) identifies non-military threats, including those with ideological, socio-cultural, and information technology dimensions, and positions awareness of state defense (*bela negara*) as part of non-military defense. However, the operationalization of Pancasila in countering digitally driven cognitive threats has not yet been systematically formulated. The concept of *soft power* (Nye, 2004) also suggests that the attractiveness of values and identity can be a source of strategic strength, including in shielding society from foreign narratives.

Research Gap

The review above reveals three main gaps. First, the cognitive warfare literature is dominated by Western and East Asian security perspectives that may not fit Indonesia's plural context grounded in the Pancasila ideology. Second, psychology-based studies of cognitive

resilience tend to focus on individuals and pay less attention to collective values and institutional dimensions. Third, Pancasila studies rarely engage with empirical findings from cognitive science and disinformation research. This article seeks to bridge these three gaps by formulating an integrative conceptual framework.

METHOD

This study employs a qualitative approach with a conceptual research design. Conceptual research aims to build a new theoretical framework by connecting concepts from various fields that were previously separate. The procedure follows the stages of conceptual framework analysis proposed by Jabareen (2009), combined with a semi-systematic or narrative literature review as outlined by Snyder (2019).

The research stages comprised: (1) mapping data sources, namely identifying relevant literature from international and national journal databases (Scopus, Google Scholar, and Garuda), policy documents (laws, defense white papers, institutional reports), and classic works on Pancasila; (2) selection and extensive reading, with inclusion criteria covering literature on cognitive warfare, influence operations, disinformation, cognitive resilience, media literacy, and the philosophy and ideology of Pancasila; (3) identifying and naming concepts, namely extracting key concepts from each body of literature; (4) deconstructing and categorizing concepts, namely outlining the attributes, functions, and roles of each concept; (5) integrating concepts, namely combining concepts with similarities into new categories; and (6) synthesis and logical validation, namely assembling these concepts into a coherent framework and testing its consistency through argumentative reasoning and comparison with practices in other countries.

Data were analyzed using qualitative content analysis and thematic synthesis. Concepts from the cognitive warfare and cognitive resilience literature were mapped against the values embodied in each principle of Pancasila to identify points of correspondence. The trustworthiness of the findings was maintained through source triangulation, comparing academic literature, policy documents, and empirical reports. As a conceptual study, its limitation lies in the absence of empirical testing of the resulting framework, which is left for future research.

RESULTS AND DISCUSSION

Characteristics of the Cognitive Warfare Threat in Indonesia

The literature synthesis identifies four main characteristics of the cognitive warfare threat in the Indonesian context. First, the exploitation of identity fault lines. Indonesia's plural society has fault lines based on religion, ethnicity, and region that can easily be activated by

provocative narratives. Lim (2017) shows how social media and *algorithmic enclaves* in Indonesia have fueled the rise of tribal nationalism and hate speech, particularly during electoral moments. Such narratives work by activating collective emotions such as a sense of threat, anger, and victimhood, thereby weakening critical reasoning.

Second, the industrialization of opinion manipulation. Bradshaw and Howard (2019) list Indonesia among the countries showing evidence of *cyber troops* used by political actors, employing strategies such as fake accounts, hashtag amplification, and campaigns attacking opponents. The phenomenon of paid buzzers normalizes manipulation in the digital public sphere and opens opportunities for foreign actors to exploit the same infrastructure.

Third, the erosion of trust in institutions. One of the strategic objectives of cognitive warfare is to reduce public trust in government, the media, science, and democratic institutions (Claverie & du Cluzel, 2022). The COVID-19 pandemic demonstrated how health hoaxes and conspiracy theories can disrupt public policy and weaken social cohesion. When trust collapses, society becomes more easily steered by alternative narratives that cannot be verified.

Fourth, ambiguous attribution and a peacetime character. As Taiwan's experience shows (Hung & Hung, 2022), cognitive warfare takes place in a "gray zone" between war and peace, often through domestic proxies, making it difficult to distinguish from ordinary political dynamics. Consequently, conventional military approaches are inadequate, and defense must rest on the resilience of society itself. These four characteristics confirm that the ultimate target of cognitive warfare in Indonesia is to weaken national unity and the legitimacy of the national consensus which is none other than Pancasila itself.

Pancasila as a Cognitive Immune System

The main finding of this study is that Pancasila can be understood as the nation's "cognitive immune system." This analogy aligns with inoculation theory (McGuire, 1961; van der Linden et al., 2017): just as the biological immune system recognizes and neutralizes pathogens, a well-internalized value system helps individuals recognize narratives that contradict fundamental values and reject them reflectively. Unlike indoctrinative approaches, a cognitive immune system requires dialogical and critical internalization, so that values are not merely memorized but become a lens for evaluating information.

From an epistemological standpoint, each principle of Pancasila contains elements relevant to cognitive defense. The first principle emphasizes honesty and moral responsibility as part of faith, forming the basis of media ethics and the rejection of slander. The second principle embodies just and civilized humanity, demanding empathy and the rejection of the dehumanization of other groups a technique commonly used in polarizing narratives. The third

principle provides a national identity that transcends ethnicity and religion, which can temper reasoning based on narrow identities. The fourth principle emphasizes wisdom and deliberation, corresponding directly to reflective thinking (System 2) and deliberative reasoning. The fifth principle demands social justice, including fairness in access to information and digital literacy, so that no group is left behind and becomes an easy target of manipulation.

The Pancasila Cognitive Defense Framework

Based on this synthesis, the study formulates the *Pancasila Cognitive Defense Framework* (PCDF), consisting of three layers and five pillars. The first layer, the value foundation, is the internalization of Pancasila values as an ethical reference and shared identity. This layer functions as an anchor that keeps individuals stable when confronted with narratives that unsettle their emotions and identity. The second layer, cognitive capacity, comprises critical thinking skills, digital literacy, awareness of cognitive biases, and the ability to recognize manipulation techniques through *prebunking*. The third layer, the institutional ecosystem, refers to structural support from the state, digital platforms, the media, educational institutions, civil society organizations, and religious communities to create a healthy information environment. The five pillars derived from the principles of Pancasila are presented in Table 1.

Table 1. Pillars of the Pancasila Cognitive Defense Framework

Principle of Pancasila	Cognitive Defense Pillar	Threats Countered	Operationalization
Belief in the One and Only God	Spiritual-ethical integrity	Slander, lies, politicization of religion	Religion-based media ethics; engaging religious leaders as trusted messengers
Just and Civilized Humanity	Critical humanism	Dehumanization, hate speech, trolling	Empathy education; <i>prebunking</i> of polarization and emotional manipulation techniques

Principle of Pancasila	Cognitive Defense Pillar	Threats Countered	Operationalization
The Unity of Indonesia	Inclusive national identity	Exploitation of SARA, separatist narratives, foreign influence operations	National counter-narratives; strengthening state defense awareness in digital spaces
Democracy Guided by the Inner Wisdom of Deliberations amongst Representatives	Deliberative reasoning	Confirmation bias, echo chambers, impulsive decisions	Critical thinking training; digital deliberation forums; a culture of verifying before sharing
Social Justice for All the People of Indonesia	Digital social justice	Literacy gaps, vulnerable groups as microtargeting victims	Equitable digital literacy; accountable platform governance; personal data protection

Source: Author's synthesis (2026).

The three layers of the PCDF operate simultaneously and reinforce one another. A value foundation without cognitive capacity risks producing fanaticism that is itself easily manipulated in the name of Pancasila; conversely, cognitive capacity without a value foundation may breed cynicism and relativism that leave individuals without moral bearings. The institutional ecosystem ensures that resilience is not borne by individuals alone but is also a structural responsibility of the state and digital platforms. Within the Total People's Defense System, the PCDF can be seen as a component of non-military defense that positions every citizen as an aware, critical, and principled "cognitive defender."

Policy Implications and Implementation Strategies

Implementing the PCDF requires a cross-sectoral strategy. In the education sector, Pancasila and civic education should be revitalized from rote memorization toward case-based and dialogical approaches, incorporating digital literacy, awareness of cognitive biases, and *prebunking* simulations. State defense education in universities and workplaces can be complemented with a module on "state defense in the cognitive domain" that covers influence operation techniques and how to counter them.

In the defense and security sector, analytical capacity must be strengthened to detect coordinated influence operations, including account network mapping, narrative analysis, and attribution. Inter-agency coordination for example among the Ministry of Defense, the Indonesian National Armed Forces (TNI), the National Cyber and Crypto Agency (BSSN), the State Intelligence Agency (BIN), the Agency for Pancasila Ideology Education (BPIP), and the ministry responsible for digital communication needs to be institutionalized so that responses are not fragmented. However, such strengthening must be grounded in democratic principles and human rights, as required by the second and fourth principles, so that cognitive defense does not become a tool for silencing criticism.

In the civil society sector, fact-checking organizations, digital literacy communities, religious organizations, and mainstream media can be positioned as nodes of cognitive resilience. This *whole-of-society* approach is in line with the spirit of *gotong royong* (mutual cooperation), which lies at the heart of Pancasila. Religious and community leaders hold strategic positions as trusted messengers capable of reaching groups with low trust in formal institutions. In the platform governance sector, the state should encourage algorithmic transparency, accountable content moderation, and personal data protection to reduce vulnerability to microtargeting.

Critical Discussion

The framework is not without challenges. First, there is a risk that Pancasila may be instrumentalized by those in power, as occurred in the past when a single official interpretation of the ideology was used to restrict freedom of expression. To prevent this, the PCDF positions Pancasila as an open ideology that can be interpreted dialogically and makes critical reasoning an integral part of defense rather than a threat to it. Second, the effectiveness of value internalization depends heavily on elite role models; when political elites themselves use buzzers and polarizing narratives, the message of Pancasila loses credibility. Third, the framework remains conceptual and requires empirical testing, for example through experiments with Pancasila-based *prebunking* interventions or surveys measuring the relationship between the internalization of national values and susceptibility to disinformation.

Nevertheless, compared with purely technical or repressive approaches, the PCDF offers the advantages of being preventive, rooted in national consensus, and able to address the emotional and identity dimensions that have long been the weak point of conventional digital literacy. This approach also enriches the global discourse on cognitive resilience with the perspective of a plural developing country, showing that local values can serve as strategic resources in confronting global threats.

CONCLUSION

Cognitive warfare poses a real threat to Indonesia because it targets the most fundamental elements of national resilience: unity, trust, and public reason. In Indonesia, this threat is characterized by the exploitation of identity fault lines, the industrialization of opinion manipulation, the erosion of trust in institutions, and its occurrence in the peacetime gray zone. This study concludes that Pancasila can be operationalized as the nation's "cognitive immune system" through the *Pancasila Cognitive Defense Framework*, consisting of three layers value foundation, cognitive capacity, and institutional ecosystem and five pillars: spiritual-ethical integrity, critical humanism, inclusive national identity, deliberative reasoning, and digital social justice.

In practical terms, this study recommends revitalizing Pancasila education to be dialogical and integrated with digital literacy and *prebunking*, institutionalizing inter-agency coordination against influence operations, engaging civil society and religious leaders as nodes of resilience, and promoting accountable digital platform governance. Future research should empirically test the framework, develop instruments to measure Pancasila-based cognitive resilience, and design intervention models applicable to diverse target groups.

REFERENCES

- Arquilla, J., & Ronfeldt, D. (Eds.). (1997). *In Athena's camp: Preparing for conflict in the information age*. RAND Corporation.
- Bernal, A., Carter, C., Singh, I., Cao, K., & Madreperla, O. (2020). *Cognitive warfare: An attack on truth and thought*. NATO Allied Command Transformation & Johns Hopkins University.
- Bradshaw, S., & Howard, P. N. (2019). *The global disinformation order: 2019 global inventory of organised social media manipulation*. Oxford Internet Institute, University of Oxford.
- Claverie, B., & du Cluzel, F. (2022). The cognitive warfare concept. In B. Claverie, B. Prébot, N. Buchler, & F. du Cluzel (Eds.), *Cognitive warfare: The future of cognitive dominance* (pp. 2-1–2-7). NATO Collaboration Support Office.
- Hobbs, R. (2010). *Digital and media literacy: A plan of action*. The Aspen Institute.
- Hung, T.-C., & Hung, T.-W. (2022). How China's cognitive warfare works: A frontline perspective of Taiwan's anti-disinformation wars. *Journal of Global Security Studies*, 7(4), ogac016.
- Jabareen, Y. (2009). Building a conceptual framework: Philosophy, definitions, and procedure. *International Journal of Qualitative Methods*, 8(4), 49–62.

- Kaelan. (2013). *Negara kebangsaan Pancasila: Kultural, historis, filosofis, yuridis, dan aktualisasinya* [The Pancasila nation-state: Cultural, historical, philosophical, juridical, and actualization aspects]. Paradigma.
- Kahneman, D. (2011). *Thinking, fast and slow*. Farrar, Straus and Giroux.
- Latif, Y. (2011). *Negara paripurna: Historisitas, rasionalitas, dan aktualitas Pancasila* [The consummate state: The historicity, rationality, and actuality of Pancasila]. Gramedia Pustaka Utama.
- Lewandowsky, S., Ecker, U. K. H., & Cook, J. (2017). Beyond misinformation: Understanding and coping with the “post-truth” era. *Journal of Applied Research in Memory and Cognition*, 6(4), 353–369.
- Lim, M. (2017). Freedom to hate: Social media, algorithmic enclaves, and the rise of tribal nationalism in Indonesia. *Critical Asian Studies*, 49(3), 411–427.
- McGuire, W. J. (1961). The effectiveness of supportive and refutational defenses in immunizing and restoring beliefs against persuasion. *Sociometry*, 24(2), 184–197.
- Ministry of Defense of the Republic of Indonesia. (2015). *Buku putih pertahanan Indonesia 2015* [Indonesian defense white paper 2015]. Ministry of Defense of the Republic of Indonesia.
- Notonagoro. (1975). *Pancasila secara ilmiah populer* [Pancasila: A popular scientific account]. Pantjuran Tujuh.
- Nye, J. S. (2004). *Soft power: The means to success in world politics*. PublicAffairs.
- Pariser, E. (2011). *The filter bubble: What the Internet is hiding from you*. Penguin Press.
- Republic of Indonesia. (2002). *Undang-Undang Nomor 3 Tahun 2002 tentang Pertahanan Negara* [Law No. 3 of 2002 on State Defense]. State Gazette of the Republic of Indonesia 2002 No. 3.
- Roozenbeek, J., & van der Linden, S. (2019). Fake news game confers psychological resistance against online misinformation. *Palgrave Communications*, 5, 65.
- Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, 104, 333–339.
- Soekarno. (1945). *Lahirnya Pancasila* [The birth of Pancasila] [Speech delivered at the session of the Investigating Committee for Preparatory Work for Independence (BPUPK), June 1, 1945].
- Sunstein, C. R. (2017). *#Republic: Divided democracy in the age of social media*. Princeton University Press.
- van der Linden, S., Leiserowitz, A., Rosenthal, S., & Maibach, E. (2017). Inoculating the public against misinformation about climate change. *Global Challenges*, 1(2), 1600008.
- Wardle, C., & Derakhshan, H. (2017). *Information disorder: Toward an interdisciplinary framework for research and policy making* (Council of Europe Report DGI(2017)09). Council of Europe.