JOURNAL OF CULTURAL ANALYSIS AND SOCIAL CHANGE

Journal of Cultural Analysis and Social Change,
2025, 10(3), 1396-1412
ISSN: 2589-1316

Humanist Intelligence in the Context of Modern Security: Between Operational Effectiveness and Respect for Human Values

Ami Prindani[1], Muhamad Syauqillah[2*], Khoirul Anam[3]

[1] *Indonesian National Police Headquarters (Mabes Polri), INDONESIA*
[2] *Graduate school of sustainable development, Terrorism Studies, Universitas Indonesia, Jakarta, INDONESIA*
[3] *Doctoral Candidate, Indonesian International Islamic University (UIII), INDONESIA*

*__Corresponding Author:__ muhamadsyauqillahhi@ui.ac.id

Citation: Prindani, A., Syauqillah, M. & Anam, K. (2025). Humanist Intelligence in the Context of Modern Security: Between Operational Effectiveness and Respect for Human Values, *Journal of Cultural Analysis and Social Change*, 10(3), 1396-1412. https://doi.org/10.64753/jcasc.v10i3.2612

Published: November 30, 2025

ABSTRACT

This narrative review synthesizes theoretical frameworks and empirical evidence to address persistent challenges in academic writing instruction for Chinese university EFL learners. Despite extensive English education, Chinese students struggle with extended academic writing, particularly when managing disciplinary content alongside language production. The review identifies constraints at linguistic, cognitive, and cultural-rhetorical levels, compounded by systemic issues including assessment misalignment and inadequate teacher preparation. The review advances a Metacognitive CLIL orientation that integrates three established traditions: Content and Language Integrated Learning for authentic purposes, the Cognitive Academic Language Learning Approach for explicit strategy instruction, and self-regulated learning for metacognitive development. This framework maps Coyle's Language Triptych directly to genre-specific moves while embedding planning, monitoring, and evaluation as routine lesson components rather than supplementary additions. The contribution is a theoretically coherent framework that addresses the fragmentation characterizing current practice, where content, strategies, and metacognition are treated separately. By providing operational principles for aligning content objectives, genre expectations, and process regulation, the framework offers practical guidance for curriculum design in Chinese universities. The research agenda prioritizes mixed-method evaluations capturing both writing products and composing processes to validate the integrated approach.

Keywords: Humanist Intelligence, Modern Security, Deradicalization, HUMINT, TECHINT, Human Rights, Indonesia

INTRODUCTION

Intelligence is one of the fundamental instruments to maintain a nation's stability and security. Historically, intelligence practices have been synonymous with coercive activities and covert operations focused on detecting and countering physical threats. This classical view positions intelligence primarily as *security intelligence* that is activities centered on preventing attacks, infiltration, or sabotage. The concept of the "archaeology of information," as introduced by Herman (2001), emphasizes the process of collecting, analyzing, and interpreting data to produce strategic decisions. However, in practice, traditional intelligence operations have often raised ethical concerns, particularly when they involve human rights violations or the disproportionate use of force.

The shifting global landscape of the 21st century demonstrates that security threats are no longer conventional. Terrorism, ideology-based radicalization, cybercrime, and the spread of digital propaganda have created a complex, asymmetric, and unpredictable configuration of threats. In this context, coercive approaches that rely solely on force are not always effective. In many cases, repressive operations have instead generated social resistance,

reinforced extremist narratives, and undermined the state's legitimacy in the eyes of both the public and the international community. This complexity of threats drives a new paradigm for intelligence practice—one that is more adaptive, inclusive, and sustainable.

A fundamental dilemma arises when a state attempts to maintain security but, on the other hand, becomes trapped in practices that have the potential to lead to injustice or violate democratic norms. Experience shows that intelligence that relies solely on eliminating threats tends to produce a cycle of violence without addressing the underlying social, economic, and psychological issues that fuel extremism. This is where the need for *humanistic intelligence* becomes relevant. This paradigm offers a balance between operational effectiveness and respect for human dignity, the law, and universal ethical values.

Humanist intelligence emphasizes that information gathering, analysis, and strategic intervention must be conducted within the bounds of legality and accountability. This approach seeks to understand the motivations, social factors, and ideological context behind threatening actions, rather than simply identifying targets for elimination. With this perspective, intelligence functions not merely as a coercive tool of the state, but as an instrument capable of building public trust, encouraging deradicalization, and strengthening societal resilience against the infiltration of violent ideologies.

Indonesia serves as an important context for discussing humanist intelligence. As Southeast Asia's largest democracy, Indonesia faces significant challenges related to terrorism, communal conflict, and socio-economic vulnerability. The application of humanist intelligence can be found in various initiatives, such as the deradicalization program run by Densus 88, the National Police's involvement in community-based mobilization, and the application of the "4K" principle (Communication, Comfort, Security, and Welfare) in field operations. These practices demonstrate how an intelligence approach can be implemented in a more empathetic, persuasive, and participatory manner without compromising national security objectives.

This article aims to analyse the concept and practice of humanist intelligence in the context of modern security, focusing on the Indonesian experience as a case study. Specifically, this paper will discuss the conceptual dimensions of humanist intelligence, its implementation in domestic security operations, and its relevance in addressing contemporary threats. Thus, this article is expected to enrich academic discourse on intelligence paradigms while providing practical contributions to the formulation of democratic, ethical, and sustainable security policies.

LITERATURE REVIEW

Intelligence has long been recognized as a vital component of national security and statecraft. Traditionally, intelligence activities were primarily directed toward safeguarding state sovereignty through espionage, counterintelligence, and covert operations (Herman, 2001). This classical conception aligns with what is termed security intelligence, focusing on the identification and neutralization of physical threats such as sabotage, infiltration, and terrorism. Herman's concept of the *archaeology of information* highlights the systematic process of gathering, analyzing, and interpreting information to support strategic decision-making—a process central to intelligence studies. Nevertheless, classical intelligence practices have often drawn criticism for ethical lapses, particularly concerning surveillance overreach, political manipulation, and violations of human rights (Gill & Phythian, 2020).

In the 21st century, security challenges have evolved from conventional warfare to more complex and asymmetric threats, including cyberattacks, terrorism, radicalization, and digital disinformation (Buzan & Hansen, 2020). These multifaceted risks blur the boundaries between internal and external security, demanding a more holistic approach to intelligence. Repressive or coercive responses, while sometimes effective in the short term, often produce counterproductive outcomes—fueling resentment, reinforcing extremist ideologies, and undermining state legitimacy (Neumann, 2013). Consequently, scholars have called for a paradigm shift toward more adaptive, preventive, and inclusive forms of intelligence work that emphasize societal engagement and resilience (Born, Caparini, & Wills, 2015).

The concept of humanist intelligence emerges as a theoretical response to the ethical dilemmas inherent in traditional intelligence practices. Rooted in human security theory, this paradigm emphasizes the protection of individual dignity and the upholding of democratic values alongside national stability (Booth, 2007). Humanist intelligence prioritizes understanding over coercion, focusing on the psychological, sociological, and ideological dimensions that motivate hostile actions. In this sense, intelligence is reframed not merely as an operational tool but as a form of social knowledge production that promotes empathy, participation, and justice (Gill, 2016). This perspective resonates with the principles of *ethical intelligence*, which advocate for transparency, accountability, and proportionality in information gathering and decision-making (Lowenthal, 2019).

Indonesia presents a compelling context for applying the humanist intelligence paradigm. As a pluralistic democracy facing persistent challenges of terrorism, communal tensions, and socio-economic disparity, the

country's security institutions have sought to balance firmness with humanity. Programs such as the *deradicalization initiative* by Densus 88 and the integration of the "4K" principle—Communication, Comfort, Security, and Welfare—illustrate the operationalization of human-centered intelligence (Sukma, 2020). These initiatives reflect a broader movement toward what can be termed empathetic intelligence, where engagement with local communities becomes a critical component of intelligence effectiveness. Through this model, intelligence functions not only as a shield against threats but also as a bridge that fosters social trust, legitimacy, and long-term resilience.

The humanist intelligence paradigm underscores that security and ethics need not be mutually exclusive. Rather, the integration of democratic accountability into intelligence operations enhances both effectiveness and legitimacy (Born & Wills, 2012). By shifting the focus from elimination to understanding, intelligence agencies can address the root causes of extremism and societal instability. This shift also aligns with global trends toward *intelligence democratization*, where civil oversight, human rights compliance, and community engagement become essential elements of national security governance (Phythian, 2021). In this regard, Indonesia's experience contributes valuable insights into how developing democracies can operationalize ethical intelligence without compromising their defensive capabilities.

Figure 1. Literature Review

THEORETICAL FRAMEWORK AND METHODOLOGY

Intelligence as Information Archaeology

Intelligence is essentially a complex epistemic process, involving a series of stages ranging from data collection and verification to analysis and distribution of information to support strategic decisions. Herman (2001) refers to intelligence as *archaeology of information*, a metaphor emphasizing that knowledge does not emerge instantly, but rather through careful, systematic, and patient "excavation." Like an archaeologist digging through layers of soil to

uncover artifacts, intelligence analysts must uncover layers of raw information, sort out the relevant from the misleading, and assemble them into a comprehensive picture of a phenomenon.

In modern intelligence literature, this definition is expanded by Gill & Phythian (2018) emphasizing the political and social dimensions of intelligence. According to them, intelligence is not simply a technical activity, but rather a practice fraught with interests, interpretations, and the construction of meaning. The information collected is never neutral; it is always influenced by who collects it, how the methods are used, and the political objectives behind its use. Thus, intelligence is both an epistemic and a social product.

This view is intertwined with a major debate in the study of international relations. Realists view intelligence as a state instrument for maintaining sovereignty, managing risk, and balancing power. In contrast, constructivists argue that intelligence should be understood as a social practice that shapes identities, perceptions, and definitions of threats, for example, a group can be viewed as an "enemy" or a "strategic partner" depending on how political discourse and intelligence analysis frame it. Intelligence is not merely a passive tool that records reality, but also an active actor that contributes to the creation of security realities (Lowenthal, 2017).

From this framework, a preliminary conclusion can be drawn that intelligence is a practice inseparable from values, norms, and political objectives. This serves as an important entry point to the idea of *humanistic intelligence*. If intelligence from the very beginning is the result of social construction, then ethical choices and a humanitarian orientation can and should be embedded in every part of the process, not merely at the final stage when decisions have already been made.

Limitations of the Coercive Paradigm

Historically, intelligence has often been practiced within a coercive framework that emphasizes secrecy, covert operations, and the elimination of threats through repressive means. This approach can be effective in certain situations—particularly when threats are immediate and demand swift responses. However, various studies highlight that the coercive paradigm carries serious limitations. Clark (2013), for instance, points out that excessive reliance on covert intelligence operations often leads to abuses of power, false targeting, and even violations of human rights. Such practices not only cause individual suffering but can also create a boomerang effect in the form of social resistance that strengthens the adversary's narrative.

In the context of domestic security, the coercive approach also risks eroding public trust in the state. Heuer (2009) emphasizes that intelligence efforts relying solely on repression tend to fail in understanding the social and psychological motivations behind threats. As a result, the security policies produced are often reactive, while the root causes remain unaddressed. Cases of extremism management in various countries demonstrate that purely repressive measures can actually trigger new waves of radicalization, as targeted groups feel alienated and are driven to seek legitimacy through violence (Borum, 2011).

The coercive paradigm, moreover, is inconsistent with international legal and ethical norms that increasingly emphasize accountability and respect for human rights. An ICRC (2021) study shows that intelligence operations violating humanitarian principles ultimately undermine a state's legitimacy in the long run. In this era of information transparency, human rights violations are difficult to conceal and can generate both international and domestic pressure. As a result, the state not only fails to achieve its security objectives but also loses public trust and its reputation in the eyes of the global community.

The limitation of the coercive paradigm lies in its tendency to prioritize short-term security at the expense of legitimacy, social trust, and policy sustainability. This is where the need to formulate a new approach becomes urgent, that is, a humanistic intelligence paradigm that balances operational effectiveness with respect for humanitarian values.

The Emergence of Humanist Intelligence

Criticism of the coercive paradigm has generated a need to formulate a new framework of intelligence that is not only effective but also ethical and sustainable. From this arises the concept of *humanistic intelligence,* a paradigm that places law, ethics, and humanitarian values at its core foundation. Humanistic intelligence is a conceptual response to traditional intelligence practices that often fail to build legitimacy and, in many cases, exacerbate cycles of violence.

The fundamental principle of humanistic intelligence is that true security cannot be achieved merely by eliminating threats, but also by building trust, strengthening social resilience, and preventing the regeneration of extremism. This approach emphasizes the importance of understanding the social, psychological, and ideological roots underlying a given threat (Horgan, 2009; Borum, 2011). Instead of solely targeting individuals involved in acts of violence, humanistic intelligence seeks to interpret the broader social context: how recruitment networks operate, how propaganda spreads, and what economic or political factors contribute to vulnerability.

The fundamental difference between traditional intelligence and humanistic intelligence lies in their ethical orientation. While traditional intelligence prioritizes tactical effectiveness often at the expense of moral values,

humanistic intelligence makes ethics a prerequisite for operational success. In this view, an intelligence operation is legitimate only when conducted within the framework of legality, institutional transparency, and respect for human dignity. Accordingly, success is measured not only by the threats that are prevented, but also by the enhancement of public safety, state legitimacy, and the willingness of society to cooperate (Tyler, 2006; Lowenthal, 2017).

Contemporary literature affirms that humanistic intelligence is not merely a normative ideal, but a practical necessity in addressing modern threats. Cronin (2009) argues that security strategies which disregard humanitarian factors tend to fail in the long term because they fail to address the roots of radicalization. Conversely, deradicalization and social reintegration programs based on dialogue, education, and economic empowerment have proven to be more effective in preventing perpetrators from returning to cycles of violence (Rabasa & Benard, 2015; Tribunnews, 2022). Thus, humanistic intelligence represents a paradigm that offers a balance between strategic effectiveness and social sustainability.

Human Security as a Normative Foundation

The concept of *human security* serves as an important normative foundation for humanistic intelligence. Introduced by the UNDP (1994), this idea shifts the focus of security from state protection to individual protection. Human security emphasizes seven dimensions of protection—from personal, political, and economic security to environmental security—all aimed at preserving human dignity. This shift marks a fundamental change: security is no longer solely about military defense, but also about guaranteeing individuals' basic rights to live safely and with dignity.

In subsequent literature, Paris (2001) asserts that *human security* is a normative framework that integrates development, human rights, and social stability. For intelligence work, this means that operations should not only aim to counter threats but also contribute to social justice and sustainability. In practice, humanistic intelligence draws inspiration from this framework by emphasizing that the success of an operation is measured by the protection of individuals and communities, not merely by the survival of the state.

Adherence to *human security* norms also carries significant implications for international legitimacy. A recent ICRC (2021) study shows that security operations violating humanitarian standards diminish a state's global reputation, weaken diplomacy, and increase the risk of political isolation. Conversely, states that demonstrate a strong commitment to human security values gain greater support from the international community—both in terms of security cooperation and diplomatic legitimacy (Lowenthal, 2017).

In the domestic context, human security reinforces the principle that intelligence must serve the people, not merely the interests of a regime. This is particularly important in democratic nations such as Indonesia, where state legitimacy is largely determined by public trust. Without a commitment to human security principles, intelligence practices risk being perceived as instruments of repression rather than tools of protection. Thus, the foundation of human security ensures that humanistic intelligence is not only normatively relevant but also strategically essential for the sustainability of democracy.

Research Methods

Research Design

This study adopts a qualitative descriptive research design with a focus on conceptual and contextual analysis. The qualitative approach is considered suitable for examining the paradigm of humanist intelligence, which involves abstract constructs such as ethics, human rights, and operational practices in security institutions. As Creswell (2018) notes, qualitative research seeks to understand the meaning individuals or groups ascribe to social phenomena, making it ideal for exploring the intersection of intelligence operations and human values.

The descriptive design aims to provide an in-depth account of how humanist intelligence operates within the Indonesian context, without attempting to manipulate variables or test causal hypotheses. Instead, it focuses on identifying conceptual patterns, policy implications, and best practices derived from secondary data sources and case studies.

Research Approach

The research uses a library-based analytical approach (*library research*) integrated with contextual interpretation. This method combines theoretical exploration and empirical review to link global intelligence theories with Indonesia's security practices. As suggested by Bowen (2009), document-based analysis enables the researcher to extract meaning and synthesize concepts from various written materials, including books, journal articles, policy documents, and institutional reports.

This study also draws upon constructivist epistemology, which assumes that knowledge about intelligence and security is socially constructed. This paradigm allows for interpreting intelligence as not merely technical but deeply embedded in cultural, political, and ethical contexts (Bryman, 2016).

Data Sources

Data for this research are entirely secondary and derived from a combination of academic, institutional, and policy-based documents. The sources include:

- ***Academic Literature:*** peer-reviewed journals, monographs, and theoretical works on intelligence studies, human security, and ethics (e.g., Herman, 2001; Gill & Phythian, 2020).
- ***Policy And Institutional Documents:*** Indonesian National Police reports, National Counterterrorism Agency (BNPT) publications, and official decrees related to deradicalization and intelligence reform.
- ***Case Documentation:*** reports and public analyses of the *Densus 88 deradicalization program*, the "4K" operational principle, and local community engagement projects.

The selection of these materials followed the criteria of credibility, relevance, and recency (Yin, 2018).

Data Collection Techniques

The main technique employed was documentary analysis, encompassing:

- Systematic review of theoretical and empirical literature through databases such as JSTOR, Scopus, and Taylor & Francis Online.
- Content analysis of relevant Indonesian policy documents, including regulations, operational guidelines, and field manuals related to intelligence ethics.
- Comparative analysis between international practices (e.g., UK and EU intelligence oversight models) and Indonesia's approaches to community-based intelligence operations.

Documents were coded thematically using keywords such as *humanist intelligence*, *ethical intelligence*, *HUMINT*, *deradicalization*, and *democratic accountability*.

Data Analysis Procedure

Data were analyzed using qualitative content analysis as developed by Mayring (2014), which involves three key stages:

- ***Reduction:*** selecting and condensing relevant information from various documents.
- ***Categorization:*** grouping themes into conceptual clusters—such as ethics, legality, operational effectiveness, and community engagement.
- ***Interpretation:*** connecting empirical evidence from Indonesia's intelligence practices with global theoretical frameworks on humanist intelligence.

Triangulation was performed through cross-verification between academic sources, policy texts, and empirical reports to ensure analytical validity (Flick, 2018). The analysis also applied critical discourse analysis to understand how language in policy texts reflects the ideological stance of humanist intelligence.

Research Validity and Reliability

To ensure rigor, the study followed the principles of **trustworthiness** proposed by Lincoln and Guba (1985):

- ***Credibility:*** achieved through data triangulation and referencing authoritative sources.
- ***Transferability:*** ensured by detailed contextual descriptions that allow replication in other democratic security systems.
- ***Dependability and Confirmability***: maintained through transparent documentation of the research process and consistent citation of data sources.

Ethical Considerations

Although this study relies solely on secondary data, ethical integrity remains essential. All information is cited properly to avoid plagiarism and intellectual misrepresentation. Sensitive institutional data—especially regarding intelligence operations—are discussed based only on publicly available documents. The research aligns with the ethical principles of academic integrity and the UNESCO Recommendation on Science and Scientific Researchers (2017), which emphasize respect for human rights, transparency, and responsible dissemination of knowledge.

RESEARCH RESULT

Humanistic Policing and Humanistic Intelligence

In addition to *human security*, the concept of *humanistic policing* offers important operational inspiration for humanistic intelligence. Rahardjo (2014) emphasizes that law enforcement officers should work not only with

"muscle" to exercise power, but also with "mind" to think strategically and "conscience" to uphold humanitarian values. This principle places empathy, dialogue, and respect for human rights at the core of law enforcement.

When the principles of *humanistic policing* are applied in intelligence practice, the orientation shifts from merely suppressing threats to building constructive relationships with communities. Humanistic intelligence emphasizes persuasive communication, public participation, and an understanding of local contexts as prerequisites for success. This aligns with the findings of Novriansyah (2017), which show that community-based policing approaches can enhance public trust, prevent recurring conflicts, and strengthen the legitimacy of security forces in conflict-prone areas.

This approach is also highly relevant in the context of counterterrorism. Indonesia's deradicalization programs led by Densus 88, for example, have shown greater success when employing methods of dialogue, education, and social empowerment rather than purely repressive actions (Rabasa & Benard, 2015). By viewing individuals involved in extremism not merely as threats but as human beings capable of change, humanistic intelligence adopts a more inclusive approach. This perspective aligns with the *community policing* model, which treats the public as partners rather than mere objects of surveillance.

Thus, *Humanistic policing* provides an applied framework for humanistic intelligence to develop strategies that are both effective and ethical. This orientation ensures that intelligence operations do not undermine social trust but instead strengthen the social capital necessary for long-term security.

Ethics in Humanistic Intelligence

The ethical dimension is an inseparable foundation of the humanistic intelligence framework. The classic debate between utilitarianism and deontology provides a rich normative basis for understanding dilemmas in intelligence practice. From a utilitarian perspective, intelligence activities are legitimate insofar as they produce the greatest benefit for the wider society—for instance, by preventing acts of terrorism, protecting civilians, or maintaining political stability (Borum, 2011). Within this framework, intelligence actions are evaluated based on their collective positive outcomes, even if they sometimes involve certain risks or sacrifices.

The utilitarian approach, however, faces criticism for its potential to overlook individual rights in favor of collective interests. The deontological perspective offers a corrective by emphasizing absolute moral obligations. Tyler (2006) asserts that intelligence practices must never violate fundamental principles of justice, such as the prohibition of torture, discrimination, or privacy abuse, even if such actions are believed to prevent major threats. From this standpoint, legal and ethical norms represent boundaries that cannot be compromised.

Humanistic intelligence seeks to integrate both approaches. Operational effectiveness is considered legitimate only when carried out within a strict legal and ethical framework. Thus, utilitarian and deontological orientations are not viewed as contradictory but as complementary dimensions. As Lowenthal (2017) notes, successful intelligence practice is not only about reducing threats but also about strengthening social legitimacy and public trust in the state.

Contemporary literature also highlights the importance of *ethical oversight* in intelligence work. Gill and Phythian (2018) argue that intelligence agencies must be subject to democratic accountability mechanisms to prevent abuses of power. Parliamentary supervision, independent oversight bodies, and judicial mechanisms are essential instruments to ensure that intelligence practices remain within legal and ethical boundaries. Through such oversight, public trust can be maintained while intelligence operations retain their political legitimacy.

Thus, ethics in humanistic intelligence should not be seen as a limitation that weakens effectiveness, but rather as an instrument that strengthens long-term success. Without ethics, intelligence risks losing its legitimacy; with ethics, it gains the social trust that serves as the primary foundation for sustaining security.

Ethical dilemmas in intelligence can be found in various real-world practices, one of the most widely debated examples is the U.S. National Security Agency (NSA)'s mass surveillance program, exposed through Edward Snowden's leaks in 2013. This practice was justified through utilitarian logic—monitoring the communications of billions of people to prevent global terrorism. However, from a deontological perspective, mass surveillance violates individual privacy rights protected under international law (Greenwald, 2014). This case illustrates how the absence of ethical boundaries can undermine the legitimacy of intelligence institutions, erode public trust, and ignite a global debate over privacy versus security.

In Indonesia, similar dilemmas arise in the use of informants within vulnerable communities, particularly in areas suspected of being radicalism bases. Operationally, infiltrating informants can yield valuable information to prevent attacks. However, if carried out without accountability, such practices can cause social trauma, stigmatize certain communities, and even reinforce extremist narratives that portray the state as unjust. Studies by Horgan (2009) and Borum (2011) emphasize that security strategies which generate a sense of injustice can, in fact, become catalysts for new forms of radicalization.

Several other studies also show that repressive actions against the families of terrorism suspects often produce the opposite effect: families feel alienated and subsequently become vulnerable to recruitment into new extremist

networks (ICG, 2017). From the perspective of humanistic intelligence, this represents both an ethical and strategic failure—achieving short-term security at the expense of long-term stability.

One example of an ethical dilemma in Indonesia can be found in the counterterrorism operations in Poso during the early 2000s. Operations involving Densus 88 successfully weakened local terrorist networks, but the predominantly repressive approach initially generated resistance among segments of the local population. Several reports indicate that violent arrests, intensive surveillance of Muslim communities, and stigmatization of suspects' families fostered feelings of injustice and distrust toward state authorities (ICG, 2007; IPAC, 2014). From the perspective of humanistic intelligence, such practices risk expanding the base of sympathy for extremist groups while simultaneously hindering deradicalization efforts.

However, over time, the approach of security forces began to shift. Subsequent operations in Poso were no longer solely focused on strict law enforcement, but started to emphasize dialogue, community engagement, and social reintegration programs for former terrorism convicts. This approach is reflected in the application of the "4K" principle (Communication, Comfort, Security, Welfare), which underscores that intelligence officers should not merely act as overseers, but as partners of the community in maintaining shared stability (BNPT, 2020). This transformation demonstrates that a security operation initially perceived as repressive can evolve into a practice of humanistic policing and humanist intelligence, when ethics, empathy, and social relations are placed at the core.

The Poso case demonstrates that ethics is not an obstacle to the success of intelligence operations, but rather a prerequisite. When security forces disregard the principles of justice and proportionality, the short-term outcomes they achieve often carry the risk of reproducing future violence. Conversely, when operations are conducted with respect for humanitarian values, public trust increases, communities become more willing to cooperate, and threats can be managed in a more sustainable manner.

These cases illustrate that ethical dilemmas are not abstract issues but real challenges faced by intelligence agencies. Integrating utilitarian and deontological frameworks within humanistic intelligence becomes essential to ensure that operational practices focus not only on immediate results but also on social, political, and moral consequences. In this way, intelligence work can maintain both effectiveness and long-term legitimacy.

HUMINT and the Role of Social Relations

Human Intelligence (HUMINT) represents the most fundamental dimension of intelligence practice, as it involves direct interaction with people as sources of information. HUMINT operates through agents, informants, and social networks capable of providing contextual data that cannot be obtained through technology alone. Within the framework of humanistic intelligence, HUMINT holds a strategic position because it creates space for dialogue, empathy, and a deeper understanding of the social dynamics underlying various threats.

Intelligence literature emphasizes that the quality of social relationships is the key to HUMINT's success. Heuer (2009) highlights the importance of building trust between intelligence agents and information sources. Without trust, the information provided tends to be partial, misleading, or even counterproductive. Therefore, HUMINT practice requires a persuasive approach that respects the informant's dignity, rather than mere exploitation for tactical gain. Within the humanistic framework, this relationship is understood as a partnership, not a subordination.

The humanistic approach in HUMINT is also highly relevant in the context of preventing radicalization. Borum (2011) found that social factors such as a sense of injustice, marginalization, and alienation are the main triggers of extremism. Through HUMINT, intelligence officers can detect early signs of radicalization, understand the narratives developing within communities, and design more precise intervention strategies. However, such strategies can only succeed if interactions are conducted with empathy and openness, rather than coercion.

In practice, HUMINT in Indonesia has proven effective when combined with community-based approaches. Community engagement programs involving religious leaders, families of former inmates, and civil society groups have succeeded in creating spaces for dialogue that narrow the influence of extremist propaganda (IPAC, 2017). This approach demonstrates that field intelligence becomes more accurate when communities feel included and respected, rather than when they live in fear.

From the perspective of humanistic intelligence, HUMINT is not merely a technique for gathering information, but also an instrument for building healthy social relations between the state and society. This relationship forms the foundation of legitimacy and the sustainability of security strategies, as a society that trusts the state will be more willing to act as a partner in maintaining shared stability.

TECHINT and Ethical Challenges

Technical intelligence (TECHINT) has advanced rapidly alongside the digital revolution and the progress of information technology. Its forms include signals intelligence (SIGINT), imagery intelligence (IMINT), measurement and signature intelligence (MASINT), and open-source intelligence (OSINT) analysis. Innovations in big data, artificial intelligence (AI), and machine learning now enable intelligence agencies to analyze billions of

data points—from communications, movements, to digital interactions—within a relatively short time. Rid and Buchanan (2015) assert that these capabilities have transformed the global intelligence landscape by significantly expanding the capacity for threat detection.

However, the expansion of technological capacity also presents serious ethical challenges. Chambers and Smith (2018) highlight that the use of algorithms to predict individual behavior can potentially violate privacy rights, reinforce discriminatory biases, and produce *false positives* that endanger civilians. The mass surveillance program conducted by the NSA, revealed by Edward Snowden, serves as concrete evidence of how technology use without accountability can trigger a public trust crisis (Greenwald, 2014). From a humanistic intelligence perspective, this illustrates that technology is not neutral—it is laden with moral implications.

Ethical challenges also arise in digital surveillance practices in developing countries, including Indonesia. The implementation of *lawful interception* systems, which grant authorities the power to monitor communications, often sparks debates over legal boundaries and potential misuse. Without independent oversight mechanisms, such technologies may be used not only to prevent terrorism but also to monitor political opposition or control public discourse. This, in turn, risks undermining democracy and fostering public distrust toward the state.

From the perspective of humanistic intelligence, technology is legitimate only when it adheres to the principles of legality, proportionality, and accountability. The principle of *legality* asserts that data collection must be governed by a clear legal framework. The principle of proportionality requires that technology be used in a limited manner, strictly in accordance with actual threats rather than arbitrarily. Meanwhile, the principle of accountability demands transparent oversight mechanisms to prevent abuse. Without these three principles, technology risks becoming a source of state delegitimization.

Within a humanistic framework, TECHINT is not viewed as a replacement for HUMINT, but rather as a *force multiplier* that enhances the scope and depth of analysis. Technological capabilities become truly effective only when combined with the contextual understanding derived from social relationships. Humanistic intelligence emphasizes that technology should serve humanity, not replace it. Only through this ethical orientation can TECHINT contribute positively to sustainable security.

HUMINT–TECHINT Integration in a Humanist Framework

One of the greatest challenges in modern intelligence work is integrating HUMINT and TECHINT within a single framework that is both ethical and effective. HUMINT provides depth of understanding, insight into motivation, perception, and social dynamics, while TECHINT offers speed, scale, and data precision. When separated, intelligence operations tend to become unbalanced: HUMINT alone is vulnerable to subjective bias, while TECHINT by itself risks generating *false positives* devoid of context. Therefore, the integration of both is a fundamental requirement for a balanced practice of humanistic intelligence.

Within a humanistic framework, the integration of HUMINT and TECHINT is not merely aimed at enhancing efficiency but also at preserving social legitimacy. HUMINT helps interpret technological data to prevent its misuse, while TECHINT expands the capacity of HUMINT by providing broader empirical evidence. For example, OSINT analysis can detect digital propaganda patterns of extremist groups, while HUMINT provides contextual insights into how these narratives are received within local communities. This synergy enables more accurate operations while reducing the risk of criminalizing innocent individuals.

Recent studies also support the importance of this integration. Rid and Buchanan (2015) emphasize that hybrid threats—combining physical and digital strategies—cannot be effectively addressed using only one type of intelligence. Meanwhile, research by IPAC (2017) in Indonesia shows that counterterrorism programs are more successful when digital data collection is complemented by dialogue with community leaders. This demonstrates that the integration of HUMINT and TECHINT within a humanistic framework is not merely a normative ideal, but also a practical necessity in the field.

In addition, this integration enables the application of the principle of *precision intelligence*, an effort to minimize civilian harm through higher accuracy in target identification. With the support of technological data and field verification, the risk of misidentification can be reduced, ensuring that intelligence operations remain both proportional and ethical. This approach is crucial for maintaining public trust, as failures in accuracy often have a direct impact on the state's legitimacy.

Thus, the integration of HUMINT and TECHINT within a humanistic framework is not merely about combining two methods, but about building an intelligence practice that is effective, legitimate, and accountable. The synergy between the two enables the state to confront contemporary threats more adaptively, while upholding human values as the core of long-term security.

The integration practice of HUMINT and TECHINT can be observed in the counter-terrorism operations of Densus 88 in Indonesia. In several cases, Densus 88 has utilized digital data (TECHINT) to track the online communications of extremist groups through social media, instant messaging applications, and closed forums. However, this digital data does not stand alone. HUMINT plays a crucial role in verifying information on the

ground—through networks of local informants, religious leaders, and the families of suspects. The combination of these approaches produces a more accurate picture of network structures, recruitment strategies, and potential attack threats.

One of the successes of this approach was evident in the arrest of the Jamaah Ansharut Daulah (JAD) network following the 2018 Surabaya attacks. OSINT and SIGINT analysis enabled authorities to detect digital communications between different cells, while HUMINT ensured that the obtained information aligned with on-the-ground realities. This dual approach helped the authorities avoid misidentification while accelerating the process of identifying and acting against key nodes within the network (IPAC, 2019).

Interestingly, this approach did not stop at enforcement. Densus 88 also integrated HUMINT with social engagement programs, in which former terrorism convicts were invited to collaborate by providing information, testimonials, or even participating in deradicalization initiatives. In this way, HUMINT functioned not only as a tool for threat detection but also as an instrument of social reintegration. The synergy with TECHINT made the process more systematic, as digital data could be used to monitor the dynamics of extremist narratives online, while HUMINT helped build bridges with communities in the real world.

This case illustrates that the integration of HUMINT–TECHINT within a humanist framework can achieve higher effectiveness while simultaneously reducing potential negative excesses. Rather than merely pursuing operational targets, this approach enables the attainment of a broader goal: sustainable security supported by community trust and participation.

Humanist Intelligence and Democracy

In a democratic system, the continuity of intelligence practices is determined not only by operational effectiveness but also by political legitimacy and public accountability. Gill & Phythian (2018) emphasize that intelligence agencies operating without democratic oversight risk abusing their authority, ultimately undermining public trust in the state. Thus, accountability is not merely an administrative procedure but a substantive prerequisite for the success of intelligence operations in a democratic nation.

Humanistic intelligence emphasizes that security and democracy are not opposing goals, but rather mutually reinforcing ones. Lowenthal (2017) notes that the public is more willing to cooperate with security agencies when they believe intelligence processes are conducted fairly and within the bounds of law. This aligns with Tyler's (2006) concept of *procedural justice*, which asserts that a state's legitimacy grows when citizens feel they are treated fairly—even in difficult circumstances. This principle is crucial in the context of intelligence operations, where public trust serves as the primary capital for obtaining information and securing social support.

In Indonesia, the democratization of intelligence can be seen in efforts to strengthen the legal framework and oversight mechanisms. Law No. 17 of 2011 on State Intelligence stipulates that intelligence operations must operate within the bounds of the law and adhere to the principles of human rights protection. Likewise, the 2023 National Police Intelligence and Security Agency (Baintelkam) Regulation emphasizes the importance of a humanistic approach in community engagement, including the application of the "4K" principles (Communication, Comfort, Security, and Welfare). These regulations reflect an institutional awareness that the success of intelligence work is measured not only by security outcomes but also by democratic legitimacy.

Oversight mechanisms are also a crucial component of humanistic intelligence. In many democratic countries, intelligence agencies are subject to supervision by parliamentary bodies, independent commissions, and judicial institutions. Gill (2020) emphasizes that *oversight* is the most effective way to prevent abuses of power while maintaining transparency. For Indonesia, strengthening intelligence oversight mechanisms is a strategic step to ensure that security operations remain aligned with democratic principles.

Thus, humanistic intelligence within a democratic framework is a paradigm that integrates operational effectiveness with political accountability. A democracy without security will be fragile, while security without democracy will be authoritarian. Humanistic intelligence offers a middle path by ensuring that intelligence practices contribute to stability while simultaneously strengthening democratic values.

Social and Psychological Dimensions in Radicalization Theory

Humanistic intelligence cannot be separated from an understanding of the social and psychological dimensions that drive radicalization. Horgan (2009) emphasizes that radicalization is not an instant process, but rather a gradual journey influenced by factors such as identity, a sense of injustice, and individual life experiences. Therefore, intelligence operations that focus solely on the physical elimination of perpetrators will not address the real root of the problem. Humanistic intelligence emerges to fill this gap by placing social and psychological analysis at the foundation of security strategy formulation.

Borum (2011) outlines four stages of radicalization: perceiving injustice, seeking an ideology of justification, adopting an extremist narrative, and ultimately committing acts of violence. These stages illustrate that psychological factors such as frustration, alienation, or the need for social recognition serve as key catalysts.

HUMINT plays a crucial role in detecting these dynamics through direct engagement with vulnerable communities, while TECHINT can monitor online communication patterns that reinforce extremist narratives. The combination of both enables authorities to conduct early interventions that are more humane and effective.

The social dimension of radicalization is also closely linked to economic and political factors. In many cases, extremist groups exploit economic inequality, discrimination, and weak public services to gain public sympathy. Research by IPAC (2017) on terrorist networks in Indonesia reveals that extremist propaganda often infiltrates through local issues of injustice, such as agrarian conflicts or ethnic marginalization. Therefore, humanistic intelligence is not only responsible for monitoring threats but also for understanding the social contexts that make a community vulnerable to the infiltration of violent ideologies.

The psychological aspect is also related to the process of social reintegration. Rabasa & Benard (2015) emphasize that deradicalization is more effective when it addresses the psychological needs of former extremists, such as restoring self-esteem, providing family support, and creating employment opportunities. In other words, the success of humanistic intelligence is measured not only by its ability to prevent attacks but also by its capacity to help individuals break free from the cycle of violence and rebuild a positive sense of identity.

By emphasizing social and psychological dimensions, humanistic intelligence ensures that security strategies do not merely treat the symptoms but also heal the root causes. This approach makes intelligence work more adaptive, as it can interpret societal dynamics and deliver responses that are not only repressive but also preventive and rehabilitative.

Procedural Justice and State Legitimacy

One of the key theoretical foundations of humanistic intelligence is the concept of *procedural justice*. Tyler (2006) emphasizes that a state's legitimacy is determined not only by policy outcomes but also by how those policies are implemented. In the context of intelligence work, this means that the public judges security agencies not merely by their success in preventing threats, but by how those preventive actions are carried out—whether they are fair, transparent, and respectful of fundamental rights.

Procedural justice has a direct impact on the public's willingness to cooperate with security agencies. UNDP (2016) highlights that citizens are more likely to share information, comply with regulations, and support security initiatives when they feel treated with respect and equality. Conversely, intelligence operations that violate due process, act discriminatorily, or use excessive measures tend to breed distrust and resistance. Within the framework of humanistic intelligence, fair procedures are not merely formalities, they are strategic tools that enhance long-term effectiveness.

In the context of democracy, legitimacy is a form of social capital that cannot be imposed through force. Gill (2020) emphasizes that intelligence agencies that fail to uphold accountability and procedural justice risk being perceived as instruments of political repression. Therefore, independent oversight mechanisms, civil society involvement, and institutional transparency are essential elements for maintaining legitimacy. Through proper oversight, the public can trust that intelligence operations serve the interests of society as a whole, rather than the narrow agenda of a ruling regime.

Hence, procedural justice serves as the key element that bridges operational practice and state legitimacy. Humanist intelligence ensures that every operation is not only lawful but also perceived as fair by the public. The trust that emerges from this process becomes the foundation that enables the state to implement security strategies that are more inclusive, sustainable, and effective.

In general, humanist intelligence is a paradigm that places law, ethics, and humanitarian values as its foundation. Success is measured not only by the number of threats eliminated, but also by the enhancement of legitimacy, social trust, and community resilience (Lowenthal, 2017; Tyler, 2006). This concept is rooted in the idea of *human security* (UNDP, 1994; Paris, 2001), which emphasizes that true security lies in the protection of human dignity—not merely in the stability of the state.

The principles of *humanistic policing* (Rahardjo, 2014; Novriansyah, 2017) demonstrate how security forces can operate with empathy, dialogue, and community participation. When adapted to the field of intelligence, these principles strengthen state–society relations while enhancing the accuracy of information. In the ethical dimension, humanist intelligence integrates utilitarianism (an orientation toward collective benefit) and deontology (adherence to absolute moral boundaries) to ensure that operations are both effective and legitimate.

A concrete example of ethical dilemmas can be seen in the NSA's mass surveillance case (Snowden, 2013) as well as in counterterrorism operations in Poso. These cases highlight that intelligence practices which ignore ethical principles risk exacerbating radicalization. In contrast, operations grounded in dialogue and community engagement have demonstrated long-term success.

In methodological terms, HUMINT and TECHINT are not viewed as two separate approaches but as complementary instruments. HUMINT provides contextual understanding, while TECHINT offers broad and precise data (Rid & Buchanan, 2015; Chambers & Smith, 2018). The integration of both within a humanistic

framework results in operations that are more accurate, ethical, and sustainable—as demonstrated by Densus 88's operations against the JAD network.

Humanistic intelligence is also closely linked to democracy. Accountability, independent oversight, and civil society involvement are essential to ensure that intelligence is not perceived as an instrument of repression, but rather as a tool of protection. The concept of *procedural justice* (Tyler, 2006) illustrates that legitimacy arises not only from outcomes but also from the manner in which policies are implemented.

Finally, the social and psychological dimensions of radicalization (Horgan, 2009; Borum, 2011) reinforce the argument that humanistic intelligence must place humans at the center of its analysis. Success is not only measured by preventing attacks, but also by rebuilding positive identities, strengthening community resilience, and fostering sustainable security.

Overall, this framework affirms that humanistic intelligence is a paradigm that integrates strategic effectiveness, ethical accountability, and democratic legitimacy. It shifts the orientation of intelligence from merely a tool of power to a tool of social trust that upholds long-term security.

The Context of Indonesia as an Applicative Ground

Indonesia represents both a significant challenge and a major opportunity for the application of humanistic intelligence. As the largest democracy in Southeast Asia, with a population exceeding 270 million and immense ethnic, religious, and cultural diversity, Indonesia's security complexities cannot be resolved through coercive measures alone. Threats such as terrorism, communal conflict, ideology-based radicalization, and cybercrime demand intelligence strategies that are adaptive, inclusive, and aligned with democratic values.

Indonesia's legal framework provides a normative foundation for a humanistic approach. Law No. 17 of 2011 on State Intelligence stipulates that intelligence operations must be conducted within the boundaries of the law, respect human rights, and serve the national interest. Furthermore, the 2023 Regulation of the National Police's Intelligence and Security Agency (Baintelkam) directs police intelligence functions to emphasize the "4K" principles (Communication, Comfort, Security, and Welfare) in community engagement. This principle aligns with the humanistic paradigm, in which the success of intelligence work is measured not only by enforcement outcomes but also by the growing public trust in state institutions.

The implementation of humanistic intelligence in Indonesia can be observed through various counterterrorism programs conducted by Densus 88. In its early phases, counterterrorism operations relied heavily on repressive enforcement. However, this approach generated resistance within certain communities, as seen in the Poso case. Learning from that experience, the strategy gradually shifted toward a more humanistic orientation, prioritizing dialogue, education, and the socio-economic empowerment of former terrorism convicts. Deradicalization programs, for instance, no longer focus solely on ideological transformation but also incorporate family support, economic empowerment, and engagement of religious leaders to facilitate social reintegration.

In addition, humanistic intelligence has increasingly been practiced through *community policing* programs that position the public as partners rather than subjects of surveillance. Community-based engagement enables security officers to obtain more accurate information while simultaneously fostering a sense of collective safety. Research by IPAC (2017) indicates that the success of counterterrorism operations in Indonesia is largely influenced by the quality of relationships between security forces and local communities. These relationships have proven far more effective when conducted through persuasive and participatory approaches rather than intimidation.

Indonesia also faces emerging challenges in the form of digital radicalization and cybercrime. In this context, the integration of HUMINT and TECHINT becomes crucial. Data derived from OSINT and SIGINT allow security agencies to map the online communication networks of extremist groups, while HUMINT ensures that the analysis remains grounded and free from technological bias. This integrative approach, exemplified in operations against Jamaah Ansharut Daulah following the 2018 Surabaya attacks, demonstrates how the humanistic paradigm can minimize the risk of misidentification while simultaneously strengthening the legitimacy of security operations.

Hence, the Indonesian context illustrates that humanistic intelligence is not merely a normative ideal but a practical necessity. The complexity of threats, the diversity of society, and the demands of democracy make the humanistic approach the most relevant option for maintaining security while fostering state legitimacy. Indonesia, therefore, has the potential to serve as an important laboratory for developing a model of humanistic intelligence that could inspire other nations facing similar challenges.

Dimensions and Practices of Humanistic Intelligence

In the context of operational practice, humanistic intelligence has two main dimensions: *security measures* and *influence operations*. These two dimensions complement each other in creating security that is both effective and ethical, with a long-term orientation toward state legitimacy and public trust.

1. Security Dimension (Security Measures)

The security dimension emphasizes the traditional function of intelligence—detecting, preventing, and responding to threats against national security. However, within the humanistic framework, security is not achieved solely through repression, but rather through proportional measures grounded in human rights principles. For instance, in counter-terrorism operations, humanistic intelligence rejects unlawful practices such as torture or detention without legal basis, as such actions ultimately undermine the legitimacy of the state (ICRC, 2021).

A humanistic security approach requires the application of the *precision intelligence* principle, ensuring that law enforcement actions are truly directed toward legitimate and relevant targets. This is achieved through the integration of HUMINT and TECHINT, which enhances accuracy and minimizes the impact on civilians. Moreover, security efforts do not end with enforcement actions; they also involve continuous monitoring of social factors that could give rise to renewed threats, such as discrimination, marginalization, or extremist propaganda (Borum, 2011).

2. Influence Dimension (Influence Operations)

In addition to security measures, the influence dimension is a defining feature of humanistic intelligence. This aspect focuses on efforts to build communication, persuasion, and partnerships with communities to strengthen social resilience. In modern policing literature, this aligns with the principles of *community policing*, where citizens are engaged as active partners in maintaining security (Rahardjo, 2014). In the intelligence context, influence operations include dialogues with religious leaders, community figures, and families of former terrorism convicts, with the goal of fostering trust and cooperation.

In Indonesia, the practice of influence operations can be observed in deradicalization and social reintegration programs. These initiatives focus not only on ideological rehabilitation but also on economic and social empowerment. Former terrorism convicts, for example, are involved in productive activities to help them rebuild a positive identity. This strategy demonstrates that influence operations are not merely a *soft approach*, but a strategic instrument capable of reducing recidivism while strengthening the legitimacy of the state (IPAC, 2017).

3. Security and Influence Synergy

These two dimensions must operate synergistically. If security measures are carried out without influence operations, intelligence efforts risk generating social resistance. Conversely, relying solely on influence without adequate security leaves the state vulnerable to serious threats and infiltration. Humanistic intelligence offers a balanced approach by integrating both dimensions, ensuring that security is achieved not merely through control, but through trust and participation.

4. Legal and Institutional Framework

The practice of humanistic intelligence also depends on a supportive legal and institutional framework. Law No. 17/2011 on State Intelligence and the 2023 Baintelkam Regulation serve as key instruments to ensure that intelligence operations are carried out in accordance with the law. In addition, oversight mechanisms from the Parliament (DPR), independent bodies, and civil society play a vital role in preventing abuse of power. With a strong institutional framework in place, both security enforcement and engagement efforts can operate consistently within democratic boundaries.

5. The Role of Technology in Humanistic Practice

Technology is a vital component in modern intelligence practice, but its use must align with humanistic principles. OSINT, big data, and AI can expand the scope of threat detection, but they are only legitimate when applied under the principles of legality, proportionality, and accountability. The integration of technology with HUMINT enables analyses that are both more accurate and ethical, as demonstrated by Densus 88's operations against the JAD network after 2018. Thus, technology serves as an *enabler* of humanistic practice, not as an instrument of repression.

Challenges and Opportunities in the Modern Era

Humanistic intelligence, despite its conceptual and practical advantages, still faces a number of serious challenges in its implementation. These challenges arise both from the dynamics of contemporary threats and from existing institutional limitations, yet at the same time they open opportunities to strengthen state legitimacy and operational effectiveness.

1. The Complexity of Contemporary Threats

Modern-era threats have become increasingly hybrid and transnational in nature. Transnational terrorism, cybercrime, and digital propaganda disseminated through social media present new challenges for intelligence

agencies. Extremist groups now exploit social media algorithms to expand the reach of their narratives, while cybercrime can disrupt a nation's critical infrastructure without any physical involvement (Weimann, 2016). In this context, humanistic intelligence must adapt swiftly to remain relevant, without compromising ethical and legal principles.

2. The Dilemma of Technology and Privacy

The utilization of big data, artificial intelligence, and *predictive analytics* holds great potential for enhancing intelligence effectiveness. However, these technologies also pose serious dilemmas related to privacy, algorithmic discrimination, and abuse of authority (Chambers & Smith, 2018). The NSA mass surveillance case demonstrated that the use of technology without proper oversight can trigger a global crisis of trust (Greenwald, 2014). For Indonesia, the key challenge lies in developing regulations and oversight mechanisms that can balance national security needs with the protection of civil rights.

3. Institutional and Supervisory Limitations

Although Law No. 17/2011 and its implementing regulations are already in place, intelligence practices in Indonesia still face accountability issues. Oversight mechanisms by the Parliament or independent bodies have not yet functioned effectively, leaving room for potential abuse of power. Gill (2020) emphasizes that *oversight* is an essential prerequisite for intelligence operations in a democratic state. Without strong supervision, humanist intelligence risks falling back into a coercive paradigm.

4. Bureaucratic Cultural Resistance

Another challenge lies in the bureaucratic cultural resistance that persists among some security personnel. Repressive approaches are often perceived as faster and more practical compared to humanist approaches, which require dialogue, empathy, and community participation. However, the experience in Poso demonstrated that repressive strategies actually prolonged the conflict and strengthened extremist narratives (IPAC, 2014). Organizational culture change thus remains a major challenge to ensure that the humanist paradigm can be genuinely institutionalized.

5. Opportunities for Multidisciplinary Integration

On the other hand, humanist intelligence holds great potential for development through the integration of multiple disciplines. Social psychology can help in understanding the process of radicalization, anthropology can provide insights into local community dynamics, while data science can enhance technical analysis. This multidisciplinary approach enables intelligence to function not only as a tool for threat detection but also as an instrument for sustainable social development.

6. Momentum of Reform and Global Norms

Another opportunity arises from the growing global demand for transparency, accountability, and respect for human rights in security operations. International norms, such as the ICRC standards and UN resolutions on human rights–based counterterrorism, encourage states, including Indonesia, to adopt more humanist approaches. This creates an opening for Indonesia to position itself as a pioneer in developing a model of humanist intelligence that could serve as an example for other regions.

Hence, these challenges and opportunities demonstrate that humanist intelligence is not merely a normative alternative, but a strategic necessity in the modern era. Its successful implementation will largely depend on the state's ability to balance technology with ethics, security with democracy, and operational effectiveness with social legitimacy.

POLICY RECOMMENDATION

To ensure that humanist intelligence can function optimally as a new paradigm in maintaining modern security, a series of strategic policy measures is required. These recommendations focus on strengthening regulations, enhancing institutional capacity, and integrating humanitarian values into operational practices.

1. Strengthening the Legal Framework and Oversight

The government needs to strengthen the legal framework to more specifically regulate the use of intelligence technologies, such as wiretapping, big data analysis, and *predictive analytics*. This regulation must be accompanied by an independent oversight mechanism, either through parliament or civil society. This way, the use of technology remains legitimate and accountable without violating citizens' privacy rights.

2. Organizational Culture Reform

Humanistic intelligence demands a shift in the bureaucratic culture of security forces from a coercive paradigm to a more persuasive and participatory one. This can be achieved through education, training, and specialized modules on intelligence ethics, *procedural justice*, and empathy-based communication skills. This cultural reform is crucial to ensure the humanist approach becomes more than just jargon and institutionalized practice.

3. Multidisciplinary Integration in Intelligence Analysis

Humanistic intelligence requires analysis that involves various disciplines. Therefore, intelligence agencies must be open to collaboration with academics, civil society organizations, and experts from various fields such as psychology, anthropology, and data science. This multidisciplinary approach allows for richer and more contextual analysis, resulting in more targeted strategies.

4. Strengthening the Community Mobilization Program

Deradicalization and social reintegration programs need to be expanded to include families, religious leaders, and local organizations. Intelligence should be viewed not as a watchdog, but as a partner in building security. A *community engagement strategy* based on the "4K" principle (Communication, Comfort, Security, and Welfare) can serve as a practical model for increasing public trust.

5. Ethical Use of Technology

Technology must be positioned as an *enabler* for a humanist approach, not as an instrument of repression. Therefore, any use of OSINT, big data, or AI must adhere to the principles of legality, proportionality, and accountability. Intelligence agencies need to develop specific ethical guidelines for the use of technology, including mitigating the risks of algorithmic discrimination and data misuse.

6. Security Diplomacy and Indonesia's Position in the World

Indonesia has the opportunity to emerge as a pioneer in developing a humanist intelligence model in Southeast Asia. By demonstrating a commitment to international human rights norms, Indonesia can strengthen its position in global security diplomacy while enhancing its international reputation as a stable democracy.

With these policy recommendations, humanist intelligence can be positioned not merely as a theoretical paradigm but as an operational strategy relevant to modern security needs. The integration of law, ethics, technology, and public participation will make intelligence more effective and strengthen the state's legitimacy.

CONCLUSION

Humanist intelligence is a new paradigm born from the need to balance operational effectiveness with respect for humanitarian, legal, and ethical values. Unlike the coercive paradigm, which emphasizes repression, humanist intelligence places public trust, democratic legitimacy, and social justice as the benchmarks of success. With a theoretical framework rooted *in human security, humanistic policing*, and principles of *procedural justice*, humanist intelligence offers a more inclusive, sustainable, and adaptive approach to contemporary threat dynamics.

In practice, humanist intelligence is implemented through two main dimensions: *security measures* and *influence operations*. Security focuses on threat detection and prevention while maintaining proportionality and accuracy, while influence operations emphasize dialogue, persuasion, and community participation as partners. The integration of HUMINT and TECHINT strengthens both, with the caveat that technology must be used ethically in accordance with the principles of legality, proportionality, and accountability.

The Indonesian context demonstrates that humanist intelligence is not merely a normative ideal, but a practical necessity. Experiences in counterterrorism operations, such as in Poso and after the 2018 Surabaya attacks, demonstrate that a solely repressive approach is ineffective in the long term. Shifting strategies toward a more humanist approach—through deradicalization, social reintegration, and community mobilization—can build public trust and strengthen societal resilience.

The implementation of humanistic intelligence, however, faces challenges such as the complexity of hybrid threats, technology and privacy dilemmas, limited oversight mechanisms, and bureaucratic cultural resistance. However, significant opportunities remain through the integration of multidisciplinary approaches, institutional reform, and a commitment to international norms. Policy recommendations, including strengthening the legal framework, reforming organizational culture, and ethically utilizing technology, are key to success.

Ultimately, humanist intelligence affirms that true security is not merely the absence of threats, but rather the presence of a sense of security, justice, and public trust. This paradigm allows intelligence to be viewed not merely as an instrument of power, but as an instrument of social legitimacy that underpins democracy and long-term

stability. With consistent commitment, Indonesia has the opportunity to become a pioneer in developing humanist intelligence practices that can serve as a global benchmark..

Funding Source

This research was conducted independently by the researcher but received support from the University of Indonesia in various non-financial forms. The support included access to the internet for data collection and analysis, computer facilities and software for data processing, as well as administrative assistance related to research legality and field data collection permits. All of this support enabled the research to proceed smoothly, even though the study did not receive external funding in the form of grants or sponsorships.

REFERENCES

Booth, K. (2007). *Theory of world security*. Cambridge University Press. https://doi.org/10.1017/CBO9780511491528

Born, H., & Wills, A. (2012). *Making intelligence accountable: Legal standards and best practice for oversight of intelligence agencies*. Geneva Centre for the Democratic Control of Armed Forces. https://www.dcaf.ch/making-intelligence-accountable

Born, H., Caparini, M., & Wills, A. (2015). *Intelligence oversight in the twenty-first century: Accountability in a changing world*. Routledge. https://doi.org/10.4324/9781315762979

Borum, R. (2011). *Radicalization into violent extremism I: A review of social science theories*. Journal of Strategic Security, 4(4), 7–36. https://doi.org/10.5038/1944-0472.4.4.1

Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal, 9*(2), 27–40. https://doi.org/10.3316/QRJ0902027

Bryman, A. (2016). *Social research methods* (5th ed.). Oxford University Press.

Buzan, B., & Hansen, L. (2020). *The evolution of international security studies*. Cambridge University Press. https://doi.org/10.1017/CBO9780511817762

Chambers, J., & Smith, A. (2018). Artificial intelligence, ethics, and the future of security. *Security Studies Review, 24*(2), 115–134.

Clark, R. M. (2013). *Intelligence analysis: A target-centric approach* (4th ed.). CQ Press.

Creswell, J. W. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). SAGE Publications.

Cronin, A. K. (2009). *How terrorism ends: Understanding the decline and demise of terrorist campaigns*. Princeton University Press.

Flick, U. (2018). *An introduction to qualitative research* (6th ed.). SAGE Publications.

Gill, P. (2016). *Intelligence ethics: A critical introduction*. Polity Press.

Gill, P. (2020). Intelligence oversight and accountability in democracies. *Intelligence and National Security, 35*(2), 153–170. https://doi.org/10.1080/02684527.2019.1700076

Gill, P., & Phythian, M. (2020). *Intelligence in an insecure world* (3rd ed.). Polity Press.

Greenwald, G. (2014). *No place to hide: Edward Snowden, the NSA, and the U.S. surveillance state*. Metropolitan Books.

Herman, M. (2001). *Intelligence power in peace and war*. Cambridge University Press. https://doi.org/10.1017/CBO9780511491573

Herman, M. (2001). *Intelligence power in peace and war*. Cambridge University Press. https://doi.org/10.1017/CBO9780511491573

Heuer, R. J. (2009). *Psychology of intelligence analysis*. Center for the Study of Intelligence, CIA.

Horgan, J. (2009). *Walking away from terrorism: Accounts of disengagement from radical and extremist movements*. Routledge.

Institute for Policy Analysis of Conflict (IPAC). (2014). *Indonesian jihadi plots and the "observer effect"*. IPAC Report No. 6.

Institute for Policy Analysis of Conflict (IPAC). (2017). *The rehabilitation of former jihadis in Indonesia*. IPAC Report No. 21.

Institute for Policy Analysis of Conflict (IPAC). (2019). *Jemaah Ansharut Daulah: Evolution and resilience*. IPAC Report No. 24.

International Committee of the Red Cross (ICRC). (2021). *International humanitarian law and challenges of contemporary armed conflicts*. ICRC Report.

International Crisis Group (ICG). (2007). *Jihadism in Indonesia: Poso on the edge*. Asia Report No. 127.

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry*. SAGE Publications.

Lowenthal, M. M. (2017). *Intelligence: From secrets to policy* (7th ed.). CQ Press.

Mayring, P. (2014). *Qualitative content analysis: Theoretical foundation, basic procedures and software solution*. Klagenfurt.

Neumann, P. R. (2013). The trouble with radicalization. *International Affairs, 89*(4), 873–893. https://doi.org/10.1111/1468-2346.12049

Novriansyah, A. (2017). Humanistic policing and conflict resolution in Indonesia. *Journal of Social Security Studies, 9*(1), 55–73.

Paris, R. (2001). Human security: Paradigm shift or hot air? *International Security, 26*(2), 87–102. https://doi.org/10.1162/016228801753191141

Phythian, M. (2021). *Understanding the intelligence cycle*. Routledge. https://doi.org/10.4324/9781003042333

Rabasa, A., & Benard, C. (2015). *Deradicalizing Islamist extremists*. RAND Corporation.

Rahardjo, S. (2014). *Membedah hukum progresif*. Kompas.

Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies, 38*(1–2), 4–37. https://doi.org/10.1080/01402390.2014.977382

Sukma, R. (2020). Counterterrorism and democracy in Indonesia: The need for a human security approach. *Contemporary Southeast Asia, 42*(2), 175–195. https://doi.org/10.1355/cs42-2a

Tyler, T. R. (2006). *Why people obey the law* (2nd ed.). Princeton University Press.

United Nations Development Programme (UNDP). (1994). *Human development report 1994: New dimensions of human security*. Oxford University Press.

Weimann, G. (2016). *Terrorism in cyberspace: The next generation*. Columbia University Press.

Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.). SAGE Publications

