vol 10 no. 2, December 2025

Available at:
https://ejournal.unida.gontor.ac.id/index.php/ettisal
http://dx.doi.org/10.21111/ejoc.v10i2.14761

ETTISAL
JOURNAL OF COMMUNICATION
P-ISSN 2503-1880
E-ISSN 2599-3240

The Change Management of Human Resource Development in Terrorism Prevention: Study at BIN-BNPT-Densus 88

Dedi Prasetyo, Made Wilantara[2]

[1]Sekolah Tinggi Ilmu Kepolisian (PTIK - STIK) Jl. Tirtayasa Raya No.6, Melawai, Kec. Kby. Baru, Kota Jakarta Selatan, Daerah Khusus Ibukota Jakarta 12160
[2] Universitas Jayabaya, Jl. Pulomas Selatan Kav. No.23 4, RT.4/RW.9, Kayu Putih, Kec. Pulo Gadung, Kota Jakarta Timur, Daerah Khusus Ibukota Jakarta 13210

wilantara.made1976@gmail.com (koresponden)

Abstract

The purpose of this study was to examine changes in human resource development management within three Indonesian security agencies: the State Intelligence Agency (BIN), the National Counterterrorism Agency (BNPT), and the Special Task Force 88 (Densus 88), in response to the increasingly complex threat of terrorism. The research method employed a qualitative approach with a case study design, involving in-depth interviews, participant observation, and document analysis. Key informants were officials and staff involved in human resource development at BIN, BNPT, and Densus 88. The results indicate that BIN focuses on technology-based intelligence competencies, BNPT develops socio-psychological skills for counter-radicalization, and Densus 88 prioritizes tactical-operational skills in field operations. Based on Kurt Lewin›s model of change (unfreeze, change, refreeze), the processes differ. At BIN, the unfreeze phase was triggered by intelligence disruptions and increasing digital threats, which prompted a technological-analytical transformation, followed by a refreeze phase in an AI and big data culture. In the BNPT (National Counterterrorism Agency), the unfreeze phase emerged from the ineffectiveness of coercive prevention, leading to socio-psychological HRD with a soft approach to deradicalization and counternarratives. Meanwhile, Densus 88 addressed the demands of tactical complexity and the risks of public legitimacy, thus encouraging adaptive human resource change and producing professional, precision law enforcement. This study also offers new theoretical insights into the application of Kurt Lewin›s Model in counterterrorism agencies such as the State Intelligence Agency (BIN), the BNPT, and Densus 88. Unlike commercial or administrative organizations, where change can stabilize into a permanent «refreeze» phase, the counterterrorism context is characterized by continuous threat escalation, rapid tactical adaptation by terrorist networks, and strong public accountability pressures, which collectively prevent organizational practices from remaining completely static. Consequently, the refreeze phase is temporary, conditional, and temporally limited, embedded in formal procedures, training systems, and inter-agency coordination frameworks that remain open to rapid revision.

Keywords: *Kurt Lewin›s Change Model; human resources; terrorism prevention; BIN; BNPT; Densus 88*

Submitted: 09-07-2025 Accepted: 22-12-2025 Published: 29-12-2025

Manajemen Perubahan Pengembangan Sumber Daya Manusia dalam Pencegahan Terorisme: Studi di BIN-BNPT-Densus 88

Abstrak

Tujuan penelitian untuk mengetahui perubahan manajemen dalam pengembangan sumber daya manusia (SDM) tiga lembaga keamanan Indonesia: Badan Intelijen Negara (BIN), Badan Nasional Penanggulangan Terorisme (BNPT), dan Satuan Khusus 88 (Densus 88) dalam menanggapi ancaman terorisme yang semakin komplek. Metode penelitian menggunakan pendekatan kualitatif dengan desain studi kasus, yang melibatkan teknik wawancara mendalam, observasi partisipan, dan analisis dokumen. Informan utama adalah pejabat dan staf yang terlibat dalam bidang pengembangan sumber daya manusia di BIN, BNPT, dan Densus 88. Hasil penelitian menunjukkan: BIN berfokus pada kompetensi intelijen berbasis teknologi, BNPT mengembangkan sosio-psikologis untuk kontra-radikalisasi, Densus 88 memprioritaskan keterampilan taktis-operasional dalam aksi lapangan. Ditinjau dari model perubahan Kurt Lewin (unfreeze, change, refreeze), prosesnya berbeda. Di BIN, fase unfreeze dipicu oleh gangguan intelijen dan meningkatnya ancaman digital, yang mendorong transformasi teknologi-analitis, kemudian 'refreeze' dalam budaya AI dan big data; di BNPT, fase unfreeze muncul dari ketidakefektifan pencegahan paksa, sehingga mengarah pada HRD sosio-psikologis dengan pendekatan lunak deradikalisasi dan kontra narasi. Sementara itu, Densus 88 memenuhi tuntutan kompleksitas taktis dan risiko legitimasi publik, sehingga mendorong perubahan SDM adaptif dan menghasilkan penegakan hukum yang profesional presisi. Studi ini juga menawarkan wawasan teoretis baru tentang terapan Model Kurt Lewin dalam lembaga kontra-terorisme seperti BIN, BNPT, dan Densus 88. Tidak seperti organisasi komersial atau administratif, di mana perubahan dapat stabil menjadi tahap «pembekuan kembali» secara permanen, konteks kontra-terorisme ditandai oleh eskalasi ancaman yang terus-menerus, adaptasi taktis yang cepat oleh jaringan teroris, dan tekanan akuntabilitas publik yang kuat, yang secara kolektif menghadang praktik organisasi untuk sepenuhnya statis. Akibatnya, tahap pembekuan kembali menjadi sementara, bersyarat, dan terbatas secara temporal, tertanam dalam prosedur formal, sistem pelatihan, dan kerangka kerja koordinasi antar lembaga yang tetap terbuka untuk revisi cepat.

Kata kunci: *Model Perubahan Kurt Lewin; sumber daya manusia; pencegahan terorisme; BIN; BNPT; Densus 88*

INTRODUCTION

Recent international studies (2021–2025) have shown a significant shift in terrorism prevention efforts from a coercive approach that relies solely on enforcement to an integrated model based on change management and human resource development. Several studies in the Journal of Policing, Intelligence, and Counter-Terrorism confirm that the success of modern counter-terrorism is largely determined by the capacity of intelligence and security personnel to adapt to technological disruption, the complexity of global terror networks, and the need for intensive cross-agency coordination. Similarly, international and regional research on countering violent extremism (CVE) emphasizes the importance of non-technical competencies, such as strategic communication, digital literacy, and socio-psychological understanding, as part of security sector organizational change. In the Indonesian context, findings by Widjanarko

and Chusjairi (2025) indicate that P/CVE strategies require human resources capable of managing cross-platform and cross-actor communication, while Hidayat and Zarkasyi (2024) emphasize that collaboration between intelligence agencies is only effective when supported by standardized and adaptive human resource development. This literature provides a conceptual foundation for research on human resource development change management in terrorism prevention at the State Intelligence Agency (BIN), the National Counterterrorism Agency (BNPT), and Densus 88. This study goes beyond describing national practices to replicating and testing the relevance of global findings on security organizational change in the context of dynamic terrorism threats. Thus, this research is clearly positioned within a reproducible and comparable scientific tradition across countries, while enriching the international literature with empirical evidence from Indonesia.

The phenomenon of terrorism has become a serious threat to national security and stability in various countries, including Indonesia. As the threat of global terrorism increases, Indonesia faces significant challenges in securing its sovereignty and the safety of its citizens. The impact of terrorism not only threatens lives but also impacts social, economic, and political aspects. Therefore, efforts to prevent and combat terrorism are a top priority for the Indonesian government. In this context, three core security institutions, the State Intelligence Agency (BIN), the National Counterterrorism Agency (BNPT), and the Special Detachment 88 (Densus 88), play key roles.

In 2023, these three institutions achieved significant success by creating a «zero attack» situation, or zero terrorist attacks in Indonesia. This success is also reflected in the increase in the National Security Index related to terrorism, which experienced significant improvements compared to previous years (Results of Interviews and Observations at the Densus 88 office, June 2025). Analytically, this phenomenon illustrates the Inter-Organizational Communication Model (KAI) based on networked governance, combined with the perspective of information-sharing and coordination mechanisms in the context of national security. This model views communication as no longer a single (top-down) approach, but rather as a hybrid communication network that combines formal institutional, situational operational, and horizontal–cross-institutional patterns. In practice, the success of attack prevention in 2023 can be analyzed through the different but interlocking roles of BIN as an early warning producer with a formal and top-down communication pattern based on strategic intelligence, BNPT as a policy integrator that operationalizes horizontal and coordinative communication across state actors versus society, and Densus 88 as an operational executor that relies on situational and rapid communication at the tactical level. This KAI model demonstrates that historical communication failures, such as information silos, response delays, and overlapping authority, can be mitigated when the three institutions operate within a layered communication system, where strategic information flows formally, but operational decisions are refined through

horizontal and situational communication. Therefore, achieving zero attack by 2023 is not understood as the result of a single dominant communication pattern, but rather as the dynamic synergy of various complementary KAI patterns in a high-risk security environment.

This success is inseparable from the implementation of structured and adaptive managerial strategies in response to changing threat dynamics. Through intensive coordination and cross-agency policy development, these three institutions can create strong synergy in detecting, preventing, and addressing potential terrorist threats in the country. This collaboration not only relies on individual institutional capabilities but also emphasizes the importance of close collaboration, structured communication, and adaptation to intelligence and data analysis technology.

In recent decades, technological advances have brought significant changes in various fields, including the strategies and modus operandi of terrorist attacks. Rapidly evolving technology, particularly in the digital and communications sectors, has provided new opportunities for terrorist groups to spread their ideology, recruit members, raise funds, and plan their actions in a more organized and stealthy manner. In Indonesia, the threat of terrorism now extends beyond physical attacks to include cyber threats, which are difficult to detect and pose new challenges for security agencies.

Various forms of terrorism currently utilize technology to increase the psychological impact and reach of their attacks. For example, terrorists can use social media and encrypted communication apps to spread propaganda, mobilize sympathizers, and recruit new members without face-to-face contact. They also utilize digital payment platforms and cryptocurrencies for hard-to-trace funding, making the flow of funds more difficult for security agencies to monitor. Furthermore, cyberattacks such as hacking, spreading computer viruses, and distributed denial-of-service (DDoS) attacks have become a new form of terrorism that has the potential to threaten the country›s critical infrastructure, including the banking, transportation, and energy sectors.

This phenomenon demonstrates the importance of adapting Indonesian security institutions to face increasingly complex and dynamic threats. The State Intelligence Agency (BIN), the National Counterterrorism Agency (BNPT), and Densus 88, as the three core institutions responsible for preventing and countering terrorism in Indonesia, have taken strategic steps to utilize technology in carrying out their duties. The application of data-driven intelligence technology, social media monitoring, and the development of threat analysis software have become part of their strategies to anticipate terrorist acts. By utilizing this technology, these institutions can identify potential threats earlier, coordinate responses more quickly, and enhance their ability to conduct more effective preventative operations.

Furthermore, the ever-evolving nature of terrorist attacks has also triggered changes in communication patterns and cross-agency cooperation. These three institutions are now further strengthening their collaboration in

information sharing, conducting joint analyses, and implementing coordinated security protocols. By utilizing the latest technology and adopting adaptive resource management strategies, BIN, BNPT, and Densus 88 can respond to threats more quickly and effectively, as evidenced by their achievement of zero attacks in 2023. However, technological advances also bring new challenges in maintaining information security and protecting sensitive data from infiltration or hacking attempts. Therefore, in addition to focusing on preventing terrorist attacks, these three institutions must also ensure that the technology systems they use remain secure and protected from external attacks. This challenge underscores the importance of a holistic and integrated security approach, where technology is used not only as a tool but also as part of a long-term strategy to maintain national stability and protect the public from the ever-evolving threat of terrorism.

Global geopolitical changes have also influenced the terrorism landscape in Indonesia. The phenomenon of proxy wars has become a growing form of conflict in the modern world, where countries or large groups use third parties or specific organizations to advance their political, economic, or ideological agendas. Proxy wars are often carried out through funding, training, or providing resources to certain groups that can weaken the enemy or destabilize a country without direct involvement. In Indonesia, proxy wars have had a distinct impact on the development of terrorism, given the country›s strategic geographic location and diverse ideologies and ethnicities that can be exploited as entry points by external actors.

This study conceptualizes proxy war–driven narrative warfare as a human-resource challenge, not merely an intelligence or operational issue. Within this framework, the Human Resource Development (HRD) divisions of BIN and BNPT are analytically shown to prepare personnel through differentiated but complementary training pathways to detect, interpret, and respond to ideologically embedded messaging propagated by proxy actors. For BIN, HR development emphasizes analytical-cognitive training aimed at identifying *latent ideological signals* within transnational narratives. Rather than adopting Critical Discourse Analysis (CDA) as a purely academic method, BIN's training operationalizes CDA-inspired competencies, such as identifying framing devices, intertextual references, and strategic silences, within intelligence analysis modules. These competencies enable analysts to deconstruct how proxy narratives subtly embed geopolitical agendas into religious, ethnic, or identity-based discourses circulating in digital ecosystems. Interview findings suggest that this training enables BIN personnel to move beyond surface-level content monitoring toward recognizing patterns of narrative convergence, where funding flows, ideological messaging, and network amplification intersect.

By contrast, BNPT's HRD training focuses on translational and communicative competencies, positioning BNPT as a *boundary actor* between classified intelligence and public-facing prevention. BNPT personnel are trained to reinterpret analytical outputs derived from intelligence assessments, including indicators of proxy-

driven ideological influence, into counter-narratives, educational content, and community interventions that are socially resonant and normatively acceptable. While BNPT does not formally label this training as CDA, the study finds that BNPT institutionalizes applied discourse literacy, equipping staff to recognize rhetorical strategies, emotional triggers, and identity appeals used by proxy actors, and to neutralize them through persuasive, empathetic, and culturally grounded communication.

Analytically, the study argues that this division of HRD roles produces a non-redundant causal chain: BIN's CDA-informed analytical capacity enables early recognition of proxy narrative infiltration. In contrast, BNPT's discourse translation capacity converts those insights into preventive social communication without exposing classified intelligence. This demonstrates that, in proxy war contexts, human resource development becomes the primary mechanism through which narrative warfare is countered, extending change management theory by showing that ideological threat mitigation depends not only on technology or operations, but on discursive intelligence embedded in organizational learning systems.

Conceptually, this study connects three specialized HR competency needs through a theoretical framework of strategic human capital and competency-based HRM, which views individual and organizational capabilities as causal value chains rather than stand-alone functions. Within this framework, predictive intelligence competency at the State Intelligence Agency (BIN) acts as an upstream capability that produces early detection, network mapping, and data-based threat projections, thereby minimizing the room for strategic surprise. This intelligence output then becomes input for socio-psychological and communicative competencies at the National Counterterrorism Agency (BNPT), which serve as a midstream capability to intervene in ideological, social, and cognitive factors through deradicalization, counter-narratives, and cross-sector collaboration and international cooperation. Furthermore, when soft prevention does not eliminate risk, tactical readiness and operational precision competencies at Special Detachment 88 (Densus 88) act as downstream capabilities that ensure swift, measurable, and highly legitimate law enforcement. This sequence forms a non-contradictory causal chain, from prediction, prevention, to enforcement, where each HR competency does not negate the other, but rather complements the others sequentially and functionally. Supported by cross-sector collaboration and international cooperation as an enabling environment, the integration of these HR competencies collectively leads to a zero attack target by 2023, while simultaneously strengthening national capacity to maintain stability and improving the National Security Index amidst increasingly complex terrorism threats.

The State Intelligence Agency (BIN), as one of Indonesia›s core security institutions, plays a central role in detecting and preventing terrorism. Facing the ever-evolving phenomenon of terrorism, BIN needs to adopt an adaptive and proactive change management approach to respond to increasingly complex threats. As the threat of terrorism increases, driven

by technological developments, global networks, and proxy warfare, BIN must implement various strategic changes in technology, human resources, and operational methods.

Applying Kurt Lewin›s change model, this study identifies that the «Unfreeze» moment for the State Intelligence Agency (BIN) was not triggered by a single failure or a specific attack, but rather by an accumulation of strategic events that demonstrated the limitations of conventional intelligence approaches. The development of micro-cell-based terrorism, lone wolf actors, the use of encryption, and radicalization through social media and cross-border digital platforms has created a significant detection gap when relying solely on human integration (HUMINT) and manual analysis. An internal evaluation of these threat dynamics, including the increasing intensity of online propaganda and digital mobilization without an open organizational structure, serves as disconfirming evidence that «thaws» BIN›s old work patterns. This situation has forced BIN to enter an unfreeze phase and encouraged the widespread adoption of big data technology, artificial intelligence, and social media monitoring as prerequisites for building predictive intelligence and early warning systems.

Meanwhile, for Special Detachment 88 (Densus 88), the unfreeze moment stems from operational realities on the ground that demonstrate a shift in the modus operandi of terrorism, not simply a failure of strategic detection. The emergence of increasingly fluid terror cells, the use of simple homemade weapons, the random selection of targets, and the increasing risk of civilian casualties and human rights scrutiny in enforcement operations demonstrate that old tactical approaches have the potential to incur legitimacy costs and escalate risks. This pressure, both from the complexity of the perpetrators› tactics and the demands of public accountability, disrupted the stability of previous operational doctrine and triggered the unfreeze phase in Densus 88. As a result, improving precision-based tactical skills, intelligence-led policing, risk control, and psychological preparedness of personnel became inevitable. Thus, this study confirms that the unfreeze phase in BIN and Densus 88 originated from different but complementary types of triggers: BIN was driven by strategic disruption in the digital realm, while Densus 88 was forced by the transformation of threats in the real operational field.

The study explains that BNPT's Human Resource Development (HRD) strategy operationalizes persuasion and narrative principles in an applied, security-oriented manner, rather than as abstract communication theory. Within Badan Nasional Penanggulangan Terorisme, HRD training is designed to equip personnel with audience-centered persuasive competencies, particularly for engaging youth who are most exposed to radical content on social media. Training modules emphasize Persuasion Theory, informed practices, such as understanding credibility (ethos), emotional resonance (pathos), and narrative coherence, so that counter-radicalization messages do not merely negate extremist claims but reframe identity, belonging, and purpose in psychologically compelling ways. Rather

than confronting ideology head-on, BNPT personnel are trained to craft messages that subtly redirect meaning, using positive role models, future-oriented aspirations, and culturally familiar symbols, thereby reducing resistance and reactance among vulnerable audiences.

In parallel, BNPT's HRD integrates applied narrative analysis, enabling personnel to dissect how extremist propaganda constructs simplified "us versus them" storylines, victimhood narratives, and heroic martyr tropes. By understanding these narrative structures, BNPT staff learn to design counter-narratives that disrupt narrative flow, for example, by introducing alternative protagonists, highlighting moral inconsistencies, or shifting the storyline from violence to social contribution. Importantly, training encourages collaboration with digital creatives, educators, and community influencers, ensuring that counter-messages adopt the visual language, tone, and platform logic favored by youth, rather than formal government messaging styles. Analytically, the study argues that this HRD approach positions persuasion and narrative competence as core professional skills, transforming BNPT personnel from passive disseminators of information into strategic communicators capable of competing effectively with extremist propaganda in the digital attention economy.

Furthermore, the National Counterterrorism Agency (BNPT) serves as an institution focused on prevention and counter-radicalization efforts, employing a different but complementary approach to the State Intelligence Agency (BIN) in addressing the threat of terrorism. Unlike BIN, which focuses on intelligence and early detection, BNPT focuses more on an approach that targets the ideological and social roots of terrorism and addresses the impact of radicalization on society. In managing change to counter terrorism, BNPT adopts an approach that integrates community-based prevention, education, rehabilitation, and deradicalization activities, aiming to create an environment more resilient to violent ideologies.

Recent studies in counterterrorism studies indicate that approaches relying solely on violence (hard security approaches) are increasingly viewed as inadequate in addressing the dynamics of contemporary terrorism based on ideology, narratives, and digital mobilization. Research in various countries confirms a paradigm shift toward preventive strategies that emphasize counter-radicalization, counter-propaganda, and socio-psychological interventions as a complement to law enforcement (Schmid, 2020). In the UK context, the PREVENT strategy institutionalizes early prevention and narrative intervention to stem the radicalization process before it leads to violence, although this remains a source of normative and political debate (Heath-Kelly, 2013). Meanwhile, the Countering Violent Extremism (CVE) approach in Australia positions persuasive communication and community engagement as key instruments in reducing the appeal of extremist propaganda, particularly among youth (Cherney & Hartley, 2017). This comparative literature provides an analytical foundation for understanding the role of the National Counterterrorism

Agency (BNPT) in Indonesia, which emphasizes counter-radicalization and counter-propaganda as a response to the limitations of a purely coercive (violent) approach. By locating the BNPT within this spectrum of global practices, this research is not merely normative or descriptive, but rather replicates and tests the relevance of international findings regarding the shift in counter-terrorism strategy toward a preventative model based on human resource development, strategic communication, and organizational change management. Meanwhile, Special Detachment 88 (Densus 88) has a distinct but complementary role to the State Intelligence Agency (BIN) and the National Counterterrorism Agency (BNPT) in preventing and combating terrorism in Indonesia. As a special unit under the Indonesian National Police (Polri) focused on direct action, Densus 88 is responsible for the operational aspects of eradicating terrorism, primarily through counterterrorism operations that include arrests, dismantling terror networks, and addressing the threat of physical attacks. Within the context of change management, Densus 88 prioritizes a swift and accurate tactical-operational approach in responding to terrorism threats, while also developing technical capabilities to address the ever-evolving threat dynamics.

Densus 88 employs a field intelligence-based approach supported by data from BIN and risk analysis results from BNPT. Their operational role requires a swift and effective response. Densus 88 continuously enhances its capabilities through equipment modernization, personnel skill development, and the development of new operational techniques. In its change management efforts, Densus 88 has adopted advanced technologies such as digital surveillance systems and explosives detection devices, which support its ability to respond quickly to emergencies. Furthermore, Densus 88 utilizes cyber intelligence to track suspicious digital communications and identify potential targets within domestic and international terrorist networks.

Change management within Densus 88 also includes enhancing personnel›s tactical skills. Densus 88 continues to conduct joint exercises and counterterrorism operation simulations to enhance preparedness and coordination in the field. This intensive training encompasses various aspects, from weapons handling and ambush techniques to simulated hostage evacuations in high-risk situations. Densus 88 collaborates with international institutions in this training to ensure its personnel possess the latest skills and are capable of handling the most complex threat scenarios. Through this approach, Densus 88 can provide optimal operational capabilities to protect the public from the direct threat of terrorism, especially in situations requiring rapid action.

Although Densus 88›s primary focus is enforcement, it also plays a crucial role in prevention efforts through preemptive strikes. Armed with information obtained from the State Intelligence Agency (BIN) and the National Counterterrorism Agency (BNPT), Densus 88 can intervene before threats develop into terrorist acts. This intervention includes arresting individuals or groups suspected of planning terrorist acts, searching locations suspected of storing explosives or weapons, and

neutralizing assets that could be used by terrorist networks. This preemptive approach allows Densus 88 to disrupt the chain of terrorist attacks before threats become real, thereby proactively protecting national stability.

While BIN›s role focuses more on early detection and BNPT on counter-radicalization and social rehabilitation, Densus 88 operates at the final stage of the terrorism prevention spectrum, namely through direct action against identified threats. The linear integration between these three agencies creates a strong and complementary counterterrorism chain. The State Intelligence Agency (BIN) provides intelligence and mapping of potential threats, the National Counterterrorism Agency (BNPT) handles education and ideological prevention, while Densus 88 serves as the vanguard, tasked with neutralizing concrete threats on the ground. This synergy enables Densus 88 to maximize its enforcement role with comprehensive and coordinated information support from BIN and BNPT.

Densus 88 is also strengthening its coordination with international institutions to counter global terrorist networks. Given that the threat of terrorism now transcends national borders, Densus 88 strives to collaborate with international law enforcement agencies, such as Interpol and counterterrorism agencies in friendly countries. This collaboration enables cross-border intelligence exchange and joint operations to apprehend suspected terrorists operating or sheltering abroad. Thus, Densus 88 focuses not only on domestic terrorism threats but also contributes to eradicating transnational terrorist networks that could impact Indonesia.

This overview illustrates Densus 88›s change management, prioritizing operational flexibility, enhancing tactical expertise, and utilizing modern technology to respond quickly and effectively to terrorist threats. Synergy with the State Intelligence Agency (BIN) and the National Counterterrorism Agency (BNPT) enables Densus 88 to carry out its enforcement role, supported by accurate information and coordinated prevention efforts. Thus, Densus 88 plays a crucial role in maintaining national security through concrete actions that take firm action and prevent terrorism in an integrated manner.

Meanwhile, in facing the increasingly complex challenges of terrorism, human resource (HR) development is a crucial component of change management across Indonesia›s three main security agencies: BIN, BNPT, and Densus 88. The ability of human resources to adapt to changing threat dynamics, master the latest technology, and develop specialized counterterrorism skills is essential to confront modern threats that often involve international networks and advanced technology.

Human resource development in the field of terrorism prevention currently faces various obstacles. On the one hand, competent professionals in counterterrorism are limited, while the threats faced continue to evolve with increasingly sophisticated methods and technologies. On the other hand, cross-agency coordination requires increased human resource capacity in terms of communication skills, collaboration, and understanding of uniform operational standards across all agencies. Furthermore,

separate training programs conducted by each agency often result in gaps in capabilities and skills, thus slowing synergy and effective responses in the field.

Therefore, this research recommendation will utilize empirical findings from BIN, BNPT, and Densus 88 to develop a comparative HRD competency model through a competency mapping and cross-institutional benchmarking approach. Conceptually, this research first identifies the core competencies unique to each agency: predictive intelligence and digital analytics in BIN, socio-psychological competencies and preventative communication in BNPT, and tactical readiness and operational precision in Densus 88, as responses to their different mandates and work environments. Next, findings on HR constraints such as professional limitations, capability gaps, and training fragmentation are analyzed to identify shared competencies needed across agencies, specifically inter-organizational communication skills, operational collaboration, and a shared understanding of SOPs. From this process, the research formulated a comparative HRD model that is modular and integrative: each institution maintains its specialist competencies but complements them with joint training modules to reduce skill gaps and accelerate synergy. Thus, this model does not standardize human resources across institutions, but rather establishes a tiered competency architecture that allows for continued specialization alongside increased collective capacity in terrorism prevention.

The research theme of Change Management in Human Resource Development in Terrorism Prevention, with a study of the State Intelligence Agency (BIN), the National Counterterrorism Agency (BNPT), and Densus 88, was chosen based on the urgency and high relevance in addressing the increasingly complex threat of terrorism in Indonesia. These three institutions are key pillars in maintaining national stability and security, yet they face evolving challenges in both technical and strategic aspects. The threat of terrorism, now fueled by technological advances, international networks, and the phenomenon of proxy warfare, demands adaptive, skilled, and collaborative human resource capabilities across institutions.

This research is significant because effective and integrated human resource development is a key foundation for strengthening comprehensive terrorism prevention. The State Intelligence Agency (BIN), the National Counterterrorism Agency (BNPT), and Densus 88 require a human resource development strategy that is responsive to changing threat dynamics, so that each personnel can carry out their duties with adequate technical and tactical competencies and synergize in joint operations. Furthermore, this research will fill the research gap regarding a change management model that can be applied to improve human resource skills in a structured and sustainable manner within these three institutions.

Therefore, this research, focusing on change management in human resource development for terrorism prevention in Indonesia, is expected to make a significant contribution, both theoretically and practically, to increasing the effectiveness and efficiency of counterterrorism efforts at the national level. This research is expected

to generate strategic recommendations for BIN, BNPT, and Densus 88 to build adaptive and synergistic human resource capacity to face the ever-evolving challenges of terrorism, thereby creating a stronger and more coordinated security system to protect Indonesia from the threat of terrorism.

CONCEPTUAL FRAMEWORK

In efforts to prevent terrorism, human resource development (HRD) in security institutions such as the State Intelligence Agency (BIN), the National Counterterrorism Agency (BNPT), and Densus 88 is crucial. Human Resource Management (HRM) theory emphasizes the importance of recruitment, training, development, performance management, and retention to ensure competent and adaptive human resources to the dynamics of the threat of terrorism. According to research by Qomariah (2015), effective HRM can improve organizational performance through strategic HR management (Qomariah, N., 2015).

Effective and adaptive human resource development (HRD) is crucial for Indonesia›s key security institutions, namely BIN, the National Counterterrorism Agency (BNPT), and Densus 88, in their efforts to address the dynamic and complex threat of terrorism. Supported by Human Resource Management (HRM) theory, HRD management strategies can be directed toward building robust and flexible capabilities, encompassing recruitment, training, development, performance management, and retention. HRM aims to place the right individuals, possessing high competencies and a mentality that aligns with the organization›s needs in the counter-terrorism field. According to Qomariah (2015), rigorous recruitment and selection can ensure that every individual who joins possesses high integrity and dedication to contributing to protecting the nation. Furthermore, human resource training and development play a crucial role in adapting personnel›s technical capabilities to the evolving modes of modern terrorism, such as technology-based intelligence skills and analytical abilities. Schuler and Jackson (2018) also emphasize that effective performance management will encourage personnel to achieve higher standards, while retention and job satisfaction maintain high motivation in a high-risk work environment.

Furthermore, Kurt Lewin›s change management theory, consisting of three stages: unfreeze, change, and refreeze, is highly relevant in this context. The unfreeze stage involves creating awareness of the need for change, change is the implementation of change, and refreeze ensures change becomes part of the organizational culture. This model has been applied in various organizational contexts to manage change effectively (Indra, A., & Sutanto, J., 2018). In the context of three hierarchical security institutions, BIN, BNPT, and Densus 88, the unfreeze phase demands a multi-level change communication strategy to build a sense of collective urgency across organizational cultures. Conceptually, this study emphasizes a combination of three main strategies: first, top-down communication based on strategic legitimacy, namely the delivery of national threat narratives, risk evaluations, and direct change mandates from top leaders to penetrate the command

culture and ensure change is perceived as an institutional need, not an individual preference; second, evidence-based communication through intelligence data dissemination, case evaluations, and cross-agency learning that serves as disconfirming information to shake the comfort of the status quo; and third, horizontal and situational communication across institutions, such as coordination forums, joint briefings, and operational discussions, which enable actors from different organizational cultures to build a shared understanding of the urgency of change. This combination is important because a sense of urgency in a security organization cannot be sufficiently built through normative rhetoric, but must be supported by structural authority, threat rationality, and collective experience, so that the three institutions can enter the unfreeze phase simultaneously despite having different mandates, structures, and work cultures.

Effective and adaptive human resource (HR) development is crucial for Indonesia›s key security institutions, namely the State Intelligence Agency (BIN), the National Counterterrorism Agency (BNPT), and Densus 88, in their efforts to address the dynamic and complex threat of terrorism. Supported by Human Resource Management (HRM) theory, HR management strategies can be directed toward building robust and flexible capabilities, encompassing recruitment, training, development, performance management, and retention processes. HRM aims to recruit the right individuals, possessing high competencies and a mentality that aligns with the organization›s counterterrorism needs. According to Qomariah (2015), rigorous recruitment and selection processes ensure that each individual who joins the force possesses high integrity and dedication to contributing to protecting the nation. Furthermore, HR training and development play a crucial role in adapting personnel›s technical capabilities to modern terrorism modes, such as technology-based intelligence skills and analytical abilities. Schuler and Jackson (2018) also emphasize that effective performance management will encourage personnel to achieve higher standards, while retention and job satisfaction maintain high motivation in a high-risk work environment. Thus, this study starts from the theoretical assumption that the main obstacle to HRD in security organizations is not simply a matter of structure or SOPs, but rather a relational capital deficit, namely limited trust, cross-cultural understanding of the organization, and interpersonal networks, which cannot be resolved solely through formal instructions or administrative coordination mechanisms. Therefore, this study explicitly argues that HR development, particularly through joint training and joint capacity building programs, is the most effective way to break down organizational silos. In this context, HRD functions as a socialization mechanism that fosters interpersonal trust and professional legitimacy, thus enabling informal and situational communication, such as rapid intelligence exchange, non-procedural clarification, and ad hoc coordination, which are crucial for terrorism prevention.

The concept of the sigmoid curve is also crucial in understanding the growth cycle

and the need for innovation before reaching a point of stagnation. Organizations need to make proactive changes to avoid declining performance. In the context of security institutions, this means continuously developing HR capacity and operational strategies to address the evolving threat of terrorism. By integrating HR theory, Lewin›s change model, and the Sigmoid curve concept, institutions such as the State Intelligence Agency (BIN), the National Counterterrorism Agency (BNPT), and Densus 88 can design adaptive and responsive human resource development strategies to address the dynamic threat of terrorism. This approach enables organizations to remain effective and efficient in carrying out their duties in preventing and countering terrorism. (Handy, C., 2019).

The Sigmoid Curve demonstrates that every organization has a growth cycle that requires continuous innovation to avoid a point of stagnation, often referred to as a comfort zone. In the initial stages, security agencies may still be able to rely on conventional approaches to human resource development. However, when a critical point is reached, innovation must be implemented immediately to avoid a decline in effectiveness in addressing threats. In the context of BIN, BNPT, and Densus 88, this transition and innovation phase requires technological updates, more intensive training, and enhanced analytical skills tailored to the challenges of the modern era. Through this approach, these three institutions can maintain optimal performance and continuously adapt as terrorism›s modus operandi evolves.

In the context of change management, the Sigmoid Curve illustrates that an organization or system must innovate or change before reaching its peak growth point to avoid declining performance or relevance. Charles Handy (2019), who popularized this concept in organizational studies, emphasized that proactive change is crucial to maintaining organizational growth and sustainability. Conceptually, this study extends the application of the Sigmoid Curve from the single organizational level to the collective performance level across institutions, by viewing the national terrorism prevention system as an integrated performance ecosystem consisting of BIN, BNPT, and Densus 88. In this framework, the sigmoid curve is not understood as a separate curve belonging to each institution, but rather as a synchronized performance curve, where the growth point, peak, and risk of stagnation of one institution can directly affect the effectiveness of the system as a whole. This research explicitly argues that a «comfort zone» or stagnation within an institution, such as Densus 88›s reliance on conventional tactical training without predictive intelligence or technology-based innovation, has the potential to create a systemic bottleneck, reducing the utility of BIN intelligence and the effectiveness of BNPT›s socio-psychological prevention efforts.

The phases of the sigmoid curve in change management include:

1. Early Growth Phase. In this phase, the organization or system experiences an early stage of development, where existing strategies and structures are still effective and foster growth. In this phase, resources are used to build the organization›s foundation

and optimize existing processes. However, with the evolving external environment and competitive dynamics, this initial approach has limitations, requiring the organization to develop new strategies.

2. Peak Phase (Critical Point). In this phase, the organization has reached its peak performance but is also at a critical point that determines its future direction. If the organization fails to adapt or innovate during this phase, it will begin to face the risk of stagnation or decline. In this peak phase, organizations need to recognize the signs of the need for strategic change, whether in technology, skills, or work processes, to prevent performance decline.
3. Decline Phase (Stagnation or Decline). If an organization does not make changes at critical points, it will enter a decline phase, where outdated strategies and old methods become ineffective, especially when facing new challenges. In this phase, the organization risks declining relevance and performance. Therefore, innovation or change before reaching the peak is crucial for the organization to continue growing and survive amidst changing dynamics.

In the context of security institutions such as the State Intelligence Agency (BIN), the National Counterterrorism Agency (BNPT), and Densus 88, the Sigmoid Curve helps illustrate the need for proactive change in the face of the evolving threat of terrorism. In the initial growth phase, these three institutions may have been sufficient with conventional methods to counter the threat of terrorism. However, as technology advances and terrorist operations become increasingly sophisticated, these methods begin to show their limitations. Although these institutions remain performing well, they will face a critical juncture where innovation in human resource management, technology, and skills becomes crucial to maintaining operational effectiveness.

When these institutions reach a peak or critical juncture, they need to recognize the need for strategic changes to anticipate new challenges. This could include implementing big data analytics technology, training personnel in digital skills, or enhancing cross-agency collaboration capabilities. For example, advanced training in digital surveillance and data analysis can be crucial for enabling human resources to identify terrorism patterns and risks more quickly and accurately.

If BIN, BNPT, and Densus 88 fail to make the necessary changes, they could enter a decline phase. Here, conventional methods are no longer effective, and they will struggle to respond to new, complex, and multidimensional threats. Therefore, by understanding the Sigmoid Curve, these three institutions can capitalize on this critical juncture to make proactive changes that will enable them to stay on track for growth and maintain their effectiveness in safeguarding national security.

Figure 1. Sigmoid Curve

Source :Researcher‹s work

Figure 1 shows the Sigmoid Curve in the context of continuous organizational change. In this curve, organizations experience several cycles of growth and transformation, illustrated by critical points (A, B, C, etc.) where change or innovation becomes essential to maintain success. In the Transformation stage (Point A), the organization or institution begins to make significant changes to anticipate new needs and adapt to changes in the external environment. In the context of BIN, BNPT, and Densus 88, this phase includes efforts to increase human resource capacity, both through selective recruitment and initial training relevant to the counter-terrorism challenges they face. This transformation aims to build a strong and adaptive foundation to face evolving threats, so that these institutions are prepared to effectively manage the threat of terrorism.

The next stage, Turnaround (Point B), is when the organization reaches a critical point, and previously stable growth begins to slow. At this point, existing strategies require adjustment to prevent stagnation. For security agencies, signs of declining effectiveness must be anticipated early so they can begin adapting to changing situations, including technological advances and increasingly complex terrorist attack patterns. In this phase, changes can be made by introducing new technologies such as big data analysis and digital monitoring, as well as specialized training in dealing with cyber threats. This adaptation is necessary so that security agencies remain able to respond to threats in a more sophisticated and efficient manner.

In the Crisis Management phase (Point B1), organizations must be prepared to face and manage crises that may arise due to unanticipated changes or untimely innovations. In the context of security agencies, if adaptation to the threat of terrorism is not carried out promptly, they could face operational crises that threaten effectiveness. For example, a lack of responsiveness in detecting and addressing new threats can weaken the agency›s performance. Therefore, crisis management in this phase requires swift and efficient change measures, including strategic adjustments and the implementation of more advanced technology to enhance operational readiness.

After successfully passing the crisis phase, organizations enter the Second Curve (Points C and C1), which marks a new stage of growth with an adjusted strategy. For BIN, BNPT, and Densus 88, this second curve reflects increased operational effectiveness in counterterrorism efforts through continuous innovation, better-trained human resources, and greater synergy between agencies. In this phase, security agencies have learned from previous cycles of change, making them better prepared to face new challenges with more proactive and collaborative strategies.

The conceptual framework in this study integrates Human Resource Management (HRM) Theory, Kurt Lewin›s Change Model, and the Sigmoid Curve into a single, integrated visual model specifically designed to address the complexity of collaborative security systems from a Critical Security Studies (CSS) perspective. The Sigmoid Curve is positioned as a temporal-strategic layer that represents the collective performance trajectory of the terrorism prevention system, emphasizing

that security effectiveness is dynamic and vulnerable to stagnation if innovation is not implemented on time (Brown & Eisenhardt, 1997). Within this temporal framework, Lewin›s Change Model (unfreeze–change–refreeze) is visualized as a recurring adaptive cycle, rather than a closed linear process, so that "refreeze" is understood as a temporary stabilization that is continually disrupted by changes in threats and geopolitical contexts (Lewin, 1951). At the model›s core, HRM serves as the primary operational mechanism driving change through training, competency development, and collaborative learning across organizations, enabling security actors to internalize change and maintain adaptive capacity sustainably (Becker, 1964). This visual integration emphasizes that security is not generated solely by structures or technologies, but rather by a social process of human learning and coordination that is collaborative, reflexive, and continually evolving. Thus, the model not only clarifies the interrelationships between theories but also offers a replicable analytical representation for examining HRM change management in high-risk security environments.

METHODOLOGY

This study employed a qualitative approach to understand the processes, strategies, and obstacles in managing change in human resource development in these three institutions. A qualitative approach is suitable for exploring in-depth phenomena and gaining perspectives from organizational actors regarding the dynamics of change in specific work environments (Creswell, 2014). A case study design was chosen to obtain a detailed overview of these three security institutions within their specific contexts.

This study also employed a multiple case study design with comparative thematic analysis as the primary strategy to balance the identification of shared themes across cases and within-case themes. Procedurally, interview data from each institution, BIN, BNPT, and Densus 88, were first coded through open coding to capture empirical issues emerging from the informants› experiences, particularly regarding interorganizational communication and change management. This stage was followed by axial coding across cases to group similar codes into shared themes, such as coordination challenges, differences in organizational culture, and the need for procedural synchronization, reflecting the dynamics of collective change within a collaborative security system. Furthermore, selective coding was applied within-case to highlight unique themes that did not appear in other institutions, such as the adaptation of human resources to artificial intelligence and predictive analytics at the State Intelligence Agency (BIN), the socio-psychological approach and public communication at the National Counterterrorism Agency (BNPT), or results-based performance evaluation at Densus 88. With this approach, thematic analysis does not reduce the complexity of each case, but rather enables replicable analytical comparisons, where shared patterns explain mechanisms of change across institutions, while specific themes reveal strategic differentiation in human resource development and organizational communication (Braun & Clarke, 2006; Yin, 2018).

Data collection in this study was conducted through several primary techniques: in-depth interviews, participant observation, and document analysis. Methodologically, this study was designed with semi-structured in-depth interviews with process-oriented inquiry principles to allow informants from the State Intelligence Agency (BIN), the National Counterterrorism Agency (BNPT), and Special Detachment 88 (Densus 88) to discuss the processes and challenges of change management without touching on sensitive operational content. This approach emphasizes the «how» rather than the «what,» directing questions at the decision-making mechanisms, policy flows, and organizational experiences, rather than the substance of intelligence, targets, or operational techniques. Specifically, researchers employed functional abstraction, raising the level of questions from operational details to managerial logic. For example, asking how training needs are identified, what criteria are used to assess competency adequacy, or how changes are prioritized within the hierarchical structure, rather than asking about the content of threats or intelligence data. Furthermore, researchers employed bounded questioning, setting explicit boundaries from the outset of the interviews, ensuring the discussion focused on aspects of human resources management and organizational communication. This strategy was reinforced through the use of comparative and reflective prompts, such as asking informants to reflect on changes before and after a particular policy or comparing old and new patterns, so that the responses were analytical and retrospective, rather than operational. This design allowed the research to maintain confidentiality while also obtaining rich data on the internal dynamics of organizational change in high-risk security environments.

Observations were conducted at the workplaces and training centers of these three institutions to gain a deeper understanding of how human resource training and development is implemented. Observations also included participation in several training activities, where possible, to directly observe the implementation of HR development strategies. This technique was useful for complementing interview data and obtaining authentic data from the field. Document analysis was used to evaluate HR policies and strategies implemented at the three institutions, including training documents, performance reports, and policies related to HR development and evaluation. These documents provided additional information regarding HR policy changes and their implementation in the field.

RESULTS

Interviews with officials and staff at the three institutions, BIN, BNPT, and Densus 88, revealed various perspectives on the challenges and strategies involved in managing change in human resource development in the context of terrorism prevention. Informants generally recognized that the increasingly complex and multidimensional threat of terrorism requires continuous adaptation, both in terms of technology, operational methods, and human resource competencies. They emphasized that each institution has a different focus and approach to human

resource development according to its respective roles, but there is an urgent need to improve cross-agency coordination to ensure a more effective and efficient response to threats.

In interviews, BIN officials revealed that human resource development in their institutions focuses on mastering analytical technology and predictive intelligence capabilities, aimed at detecting threats early. Meanwhile, BNPT staff explained that they emphasize counter-radicalization and deradicalization approaches, including training in understanding the psychology of radicalism and communication skills for interacting with the community. Meanwhile, Densus 88 personnel explained that their human resource development is directed at improving tactical skills and rapid response in operational enforcement. These interviews revealed significant differences in the focus of human resource development at each agency, which poses unique challenges in achieving synergy and effective collaboration.

The informants also emphasized the importance of proactive innovation in training and technology implementation to anticipate rapidly changing external environments. They noted the need for enhanced collaboration and technology integration between BIN, BNPT, and Densus 88 to accelerate information flow and enhance operational effectiveness in the field. Overall, these interviews revealed the perceptions and practical experiences of officials and staff at all three agencies regarding the importance of adaptive, responsive, and integrated human resource change management in addressing the increasingly complex threat of terrorism.

BIN Human Resource Development Change Management

This study reveals that the State Intelligence Agency (BIN) has implemented various human resource development management strategies that significantly contributed to the success of achieving a zero-attack target for terrorist attacks in Indonesia by 2023. Interviews with BIN officials and staff identified this success as being due to the implementation of strategies focused on enhancing predictive intelligence capacity and utilizing advanced technology, as well as developing analytical and collaborative competencies within BIN personnel.

One of the key pillars of BIN›s human resource development strategy is an emphasis on utilizing big data and artificial intelligence-based technologies to support predictive intelligence capabilities. BIN has established a data analysis center that allows its personnel to access integrated information from various sources. Using big data technology, BIN is able to analyze suspicious activity patterns and identify potential threats before they escalate into acts of terrorism. Intensive training is provided to BIN personnel in mastering these technologies, including skills in data processing and conducting rapid and accurate risk analysis. Interview results indicate that this predictive capability enables BIN to detect threats early and prevent them before they reach the execution stage, which is key to achieving zero attacks by 2023.

Specifically, the interviews mapped the Change strategy, which involved implementing AI and big data at the State Intelligence Agency (BIN), to the Unfreeze

stage of Kurt Lewin›s model through a narrative of organizational awareness that is cumulative, reflective, and based on experiences of potential failure, rather than a single, overt attack incident. Informants did not refer to specific operational detection failures due to confidentiality constraints, but rather to institutional recognition of delays, fragmentation, and low precision in early detection when dealing with new threat patterns such as digital radicalization, lone actors, and encrypted communications. This narrative serves as disconfirming evidence that «thaws» the long-held belief that HUMINT approaches and manual analysis are sufficient. In the interviews, awareness of the need for human resource change emerged when informants explained that AI- and big data-based predictive capabilities are impossible to achieve without radical changes in personnel competencies, ranging from data literacy and analytical skills to collaborative work patterns with technology systems. Thus, the Unfreeze stage is not mapped as a reactive response to a single critical attack, but rather as a cognitive-organizational process in which leaders and human resource managers recognize that prevention success, which is then manifested in the achievement of zero attacks by 2023, can only be achieved if the old HR paradigm is replaced by a new predictive intelligence competency model.

This research substantiates the claim that the achievement of zero attacks is predominantly influenced by the development of human resources at the State Intelligence Agency (BIN), particularly through strengthening technology-based predictive capabilities, using a multiple case study design and a comparative thematic analysis strategy. This approach does not position the claim normatively, but rather assesses the relative causal contributions between institutions within the overall terrorism prevention cycle. The analysis aims to distinguish the roles of primary and supporting factors by exploring the stages of intervention, working mechanisms, and empirical consequences of each institution in preventing terrorist attacks (Yin, 2018).

Within this framework, each institution is functionally positioned at a different stage of the threat cycle, allowing for a more precise identification of causal roles. BIN operates predominantly in the pre-threat phase through early detection and predictive intelligence analysis, while the National Counterterrorism Agency focuses on medium-term counter-radicalization and ideological prevention, and Densus 88 plays a role in the actual threat phase through tactical intervention. This mapping shows that upstream prevention has the most significant impact in explaining the absence of attacks, as the threat has been neutralized before it reaches the operational stage (Silke, 2018).

Table 1. Intervention Characteristics of Three Institutions

Threat Cycle Stage	Dominant Institution	Intervention Character
Pre-threat (early warning)	BIN	Predictive, preventive
Pre-radicalization & deradicalization	BNPT	Socio-ideological
Actual threat	Densus 88	Repressive-tactical

Source :Researcher‘s Compilation

Thematic analysis findings indicate that BIN›s interventions consistently occurred earlier than those of other institutions, both through the use of analytical technology, early warning systems, and strengthening human resource competencies in interpreting threat patterns. This temporal dimension is crucial, as the earlier a threat is identified, the lower the chance of escalation to physical terrorism. Therefore, the success of zero attacks is logically more closely tied to the effectiveness of upstream prevention than to the success of downstream enforcement (Boin et al., 2017).

In addition to the temporal aspect, evidence of causal mechanisms also strengthens BIN›s position as a primary factor. Unique themes that did not emerge predominantly within the BNPT or Densus 88 included predictive intelligence capabilities, the integration of human analysis and artificial intelligence, and cross-sector data processing capabilities. BIN›s human resource training focused on mastering digital data-based threat analysis, cross-agency coordination, including with the Ministry of Communication and Information Technology, and collaborative communication with the public as a source of social censorship. This mechanism forms a clear causal chain: strengthening human resources and predictive technology, leading to early detection, followed by prevention before threats escalate (George & Bennett, 2005).

Counterfactual analysis was also used to strengthen the causal argument. Without BIN›s predictive intervention, the BNPT and Densus 88 would still function, but at a more advanced threat stage. Under these conditions, the probability of attempted attacks or near-misses increases, making the zero-attack goal much more difficult to maintain. These findings suggest that the roles of BNPT and Densus 88 are necessary but not sufficient, while BIN›s predictive capabilities are a key variable explaining the success of total prevention (Gerring, 2017).

Therefore, the conclusion of this study confirms that the claim of zero attacks is not intended to negate the contributions of BNPT and Densus 88, but rather to place the role of each institution proportionally in the causal chain of terrorism prevention. Through temporal evidence, causal mechanisms, and counterfactual analysis, this study demonstrates that BIN›s development of human resources based on predictive technology serves as a primary trigger, enabling the national security system to operate more effectively and proactively.

Interviews indicate that human resource training, particularly at BIN, facilitates Inter-Organizational Communication (ICC) not by standardizing intelligence content, but rather by standardizing the way of thinking, technical language, and coordination logic used in cross-agency collaboration with the National Counterterrorism Agency (BNPT) and Special Detachment 88 (Densus 88). Informants explained that predictive intelligence and technology-based training not only enhance individual analytical capacity but is also intentionally designed to build a shared technical lexicon, for example, in the meaning of threat levels, risk classifications, and prevention time horizons, so that information can be exchanged without the need for repeated

clarification. Furthermore, training emphasizes cross-functional awareness, namely an understanding of how BIN analytical output will be used by BNPT in the context of socio-psychological prevention and by Densus 88 in operational readiness, so that intelligence messages are structured in a format that is more easily translated across mandates. Interviews also indicate that while formal data exchange protocols remain constrained by regulations and confidentiality, this collaborative training lowers informal and situational communication barriers, as personnel have shared similar cognitive frameworks and professional standards. Thus, this study confirms that human resource development functions as a socio-cognitive medium for KAI, where a common technical language, understanding of processes, and work expectations are prerequisites for fast, accurate, and mutually trustworthy cross-institutional communication in terrorism prevention.

Change Management of Human Resource Development

Research findings indicate that the change management approach for human resource development at the National Counterterrorism Agency (BNPT) differs from that of the State Intelligence Agency (BIN), in line with BNPT›s primary focus on counter-radicalization and deradicalization. Interviews with BNPT officials and staff revealed that BNPT›s human resource development strategy is more oriented toward socio-psychological and educational approaches.

Specifically, interviews indicate that BNPT›s understanding of terrorism prevention translates into unique communication competencies that differentiate it from BIN and Densus 88, positioning communication as an instrument for ideological and psychosocial intervention, rather than simply conveying messages. At the National Counterterrorism Agency (BNPT), human resource development involves structured training in persuasion theory and empathetic communication, aimed at cognitively dismantling extremist narratives while building emotional trust. Informants explained that this training encompasses the ability to analyze radical ideological framing, identify emotional and religious appeals used by extremist groups, and design non-confrontational yet persuasive counternarratives, in line with the principles of Persuasion Theory. At the same time, the National Counterterrorism Agency (BNPT) is instilling empathetic communication skills, particularly for human resources involved in assisting terrorist convicts and former perpetrators. Active listening, validating personal experiences, and managing emotions are key to opening up dialogue and changing attitudes. Thus, BNPT›s communication skills are relational and transformative, enabling human resources to function as ideological mediators between the state and vulnerable individuals/communities. This finding confirms that BNPT›s human resource development strategy focuses not only on «what is conveyed,» but also on how messages are delivered and relationships are built. Communication becomes a key tool in building ideological resilience and complementing the BIN intelligence approach and Densus 88›s

enforcement efforts within the national terrorism prevention ecosystem.

Another strategy identified is the development of skills in organizing community education programs. BNPT recognizes that terrorism prevention efforts cannot be achieved solely through enforcement but also through education that involves the community. Therefore, BNPT human resources are trained to organize and facilitate educational programs, such as seminars, workshops, and awareness campaigns in various areas prone to radicalization. These programs are designed to spread messages about the dangers of radicalism and terrorism, as well as the importance of tolerance and harmony. Interviews indicate that the National Counterterrorism Agency (BNPT) adopts a participatory approach, where BNPT staff act as facilitators, empowering communities to participate in counter-radicalization efforts. These facilitation skills enable BNPT staff to actively engage communities in countering extremist narratives.

Furthermore, BNPT emphasizes the implementation of a digital counter-narrative approach in its human resource development program. Given that radicalization often occurs through social media and digital platforms, BNPT trains its personnel to effectively design and disseminate counter-narratives in the digital space. The effectiveness of BNPT›s digital presence is not primarily measured by its success in directly «defeating» extremist narratives, but rather by its ability to disrupt, slow down, and delegitimize the process of digital radicalization. Interviews indicate that BNPT positions digital communication as a space for early intervention, rather than an arena for open ideological debate. In this approach, staff are trained to read engagement patterns, discourse momentum, and audience vulnerabilities, enabling communication interventions to be conducted in the pre-radicalization phase, when individuals are still searching for identity and meaning. This strategy prevents the dominance of extremist narratives from being confronted head-on, but rather disrupts them through fragmentation, diversion, and the normalization of more moderate alternative discourses. Furthermore, research has found that the National Counterterrorism Agency (BNPT) views the digital space as a collaborative ecosystem, where counter-radicalism success is measured by the growth of positive conversations across communities, not simply the virality of content. Thus, the BNPT›s presence in the digital space functions as a preventative communications architecture, gradually weakening the appeal of extremist narratives by reducing their emotional resonance and relevance in the daily lives of target audiences.

Another interesting finding is the National Counterterrorism Agency (BNPT)›s strategy for developing human resources for the deradicalization program for terrorist prisoners. The BNPT focuses its personnel training on social and psychological rehabilitation techniques for prisoners involved in terrorist acts. This training program includes counseling skills, light psychotherapy, and a humanistic approach to dealing with prisoners. Interviews revealed that BNPT staff involved in the deradicalization program were also trained

in social reconciliation techniques, which aim to help prisoners reintegrate into society with moderate and peaceful views. This approach has yielded positive results in reducing the risk of recidivism and helping prisoners rebuild their social relationships after their sentence.

In addition to focusing on individual competencies, the BNPT also builds collaboration and strategic partnership capabilities in human resource development. Given that preventing and countering radicalism involves multiple sectors, the BNPT trains its personnel to collaborate with other ministries, educational institutions, civil society organizations, and even international institutions. This training, involving negotiation skills, networking, and diplomacy, allows the BNPT to expand the scope of its counter-radicalization program and gain support from various parties. Interviews revealed that this cross-sector collaboration enhances the effectiveness of the BNPT program, leveraging the resources and expertise of strategic partners in countering radicalism.

Overall, this study demonstrates that BNPT adopts a holistic approach to human resource development change management, focusing on understanding the psychology of radicalism, cross-cultural communication, digital counter-narratives, and strategic partnerships. This approach differs significantly from BIN, which focuses more on analytical technology and predictive intelligence. The study also shows that BIN›s predictive and AI-based focus overlaps, but does not overlap, with the human resource development focus of BNPT and Densus 88. The primary overlap lies in its early prevention orientation, where all three institutions view speed, accuracy, and anticipation as key competencies, but are expressed through different forms of human resource development. At BIN, predictive competency is realized through strengthening data literacy, algorithmic analytical capabilities, and the integration of AI to project threats before they emerge in physical spaces. This focus differs substantively from that of the National Counterterrorism Agency (BNPT), which translates early prevention into socio-psychological and communicative competencies, such as reading ideological dynamics, influencing attitudes, and building community resilience to prevent potential threats from developing into violent intent. Meanwhile, Densus 88 articulates prevention in the form of adaptive tactical readiness, namely the ability to respond quickly and precisely when threat indications have entered the operational phase. Thus, this difference in human resource focus does not constitute fragmentation, but rather a complementary division of functions: BIN works on the technology-based prediction and early warning phase, BNPT on the ideological and social prevention phase, and Densus 88 on the law enforcement and precision action phase. The integration of the three forms a sustainable national capacity chain, where BIN›s predictive excellence is only effective when aligned with BNPT›s communicative capabilities and Densus 88›s operational preparedness.

Change Management of Human Resource Development at Densus 88

Research findings indicate that the human resource development

change management strategy at Special Detachment 88 (Densus 88) has a very different focus compared to that of the State Intelligence Agency (BIN) and the National Counterterrorism Agency (BNPT). As a unit responsible for direct action against terrorism threats, Densus 88 emphasizes human resource development on tactical-operational aspects, physical resilience, and crisis management capabilities. Interviews with Densus 88 personnel and officials revealed that the institution›s human resource development strategy aims to develop personnel who are ready to act quickly, possess high tactical skills, and are able to respond to terrorist threats under stressful and high-risk conditions.

One of the key pillars of human resource development at Densus 88 is realistic simulation-based operational training. Densus 88 implements a training program designed to equip personnel with operational skills that can be relied upon in emergencies. This training program includes tactical exercises such as ambush simulations, rapid intervention techniques, hostage handling, and infiltration in high-risk environments. Based on interviews, Densus 88 personnel are expected to be able to adapt to various threat scenarios, enabling them to respond appropriately and minimize risks to both civilians and Densus personnel. This simulation-based approach aims to create field experiences as close as possible to real-world conditions, ensuring optimal mental and physical readiness for personnel.

In addition to tactical training, Densus 88 also emphasizes physical and mental resilience training as part of its human resource development. Densus 88 personnel are intensively trained to withstand high levels of stress and risk, both physically and mentally. Physical resilience training includes improving endurance, physical strength, and survival skills in various operational environments. Mentally, Densus 88 involves psychologists in the training process to hone mental resilience and composure under pressure, preparing personnel for crises or life-threatening threats. According to interviews, this physical and mental resilience is a vital component that enables Densus 88 personnel to act quickly, think clearly, and make sound decisions in extremely dangerous situations.

In the context of Inter-Organizational Communication (IOC), Densus 88 systematically trains its personnel to maintain accurate communication and decision-making during high-pressure operations, such as ambushes or hostage rescues. Personnel are trained using highly standardized and minimally ambiguous communication protocols, ensuring that every message, command, or situational report can be understood uniformly, while also ensuring synchronization with the State Intelligence Agency (BIN) and National Counterterrorism Agency (BNPT) when operating within an inter-agency coordination framework. Intensive exercises that mimic ambush, hostage-taking, or explosion scenarios force personnel to communicate quickly and precisely, emphasizing the use of standard codes, standard procedures, and concise commands to ensure effective communication despite the highly dynamic operational environment. Physical and mental resilience are the main foundations,

enabling personnel to act quickly, think clearly, and make sound decisions without getting caught up in emotion or panic, which is crucial for maintaining accurate inter-agency messages and preventing miscommunication. After each operation or exercise, a debriefing and evaluation are conducted to identify communication and coordination gaps, which then serve as the basis for updating communication protocols to align them more closely with BIN and BNPT standards. This combination of standard communication protocols, high-pressure training, and mental resilience creates effective synergy between Densus 88, BIN, and BNPT, so that cross-agency operations can run with accurate, fast, and safe coordination.

Densus 88 also implements a performance-based evaluation system to measure the effectiveness of its human resource development. Within the framework of Kurt Lewin›s Change Model, the performance-based evaluation system implemented by Densus 88 serves as a continuous reflection mechanism that bridges the Refreeze stage and the potential for subsequent unfreeze. Unlike periodic and retrospective administrative evaluations, Densus 88›s results-based evaluations emphasize indicators of response speed, enforcement accuracy, operational risk levels, and public legitimacy impact, which directly reflect the match between personnel›s tactical competencies and actual threat dynamics. When evaluation results indicate deviations, such as delayed responses, increased risk of civilian casualties, or tactical incompatibility with new threat patterns, these findings serve as disconfirming feedback that destabilizes Refreeze and creates early awareness of the need for change. Thus, this evaluation system conceptually accelerates the micro-Unfreeze process, namely the reopening of space for change at the training and tactical doctrine levels without waiting for strategic failure or a major crisis. This study shows that in a high-risk security context, this kind of reflection mechanism allows Densus 88 to anticipate competency stagnation, maintain adaptive readiness of human resources, and ensure that changes in tactical training are proactive, rapid, and evidence-based, so that Lewin›s Model operates cyclically and responsively, rather than linearly and statically.

DISCUSSION

This study found similarities and differences in the change management approaches to human resource development (HRD) across Indonesia›s three core security agencies: BIN, BNPT, and Densus 88. Although all three share the primary objective of maintaining national security, each agency implements distinct strategies tailored to its specific role in addressing the threat of terrorism.

Similarities in HRD Change Management:

1. Focus on Improving HRD Competence.

All three agencies emphasize the importance of improving HRD competencies to address the increasingly complex threat of terrorism. They conduct training tailored to their respective roles, enabling HRD to adapt to dynamic operational needs.

2. Use of Technology in Training.

BIN, BNPT, and Densus 88 all utilize technology in HRD development, albeit

with different focuses. BIN focuses more on big data and artificial intelligence for intelligence analysis, BNPT utilizes social media and digital platforms for counter-narratives, while Densus 88 applies advanced technology to operational tools and tactical surveillance.

3. Commitment to Change Management.

Based on findings on continuous training, the "Refreeze" phase in Kurt Lewin's model can no longer be understood as static stabilization, but rather must be conceptualized as "Adaptive Refreeze" or a form of continuous change in high-risk security organizations such as the State Intelligence Agency (BIN), the National Counterterrorism Agency (BNPT), and Special Detachment 88 (Densus 88). The findings indicate that stabilizing change is not directed at standardizing a final set of competencies, but at standardizing the capacity to continuously learn and adapt. In this context, refreeze is maintained through institutional mechanisms such as periodically updated training curricula, after-action reviews, and the integration of new technologies into training standards, so that change "freezes" at the process and mindset level, rather than at the rigid skill content. Furthermore, research shows that cross-agency personnel rotation and joint training serve as key tools for maintaining adaptive refreeze, as they enable simultaneous knowledge transfer, threat perspective alignment, and competency updates across the security ecosystem. Thus, Lewin›s model in this context operates cyclically and in layers, where the refreeze is not the end of change, but rather a temporary stable platform consciously designed to facilitate subsequent unfreeze when threat dynamics demand new adjustments.

Differences in Human Resource Development Change Management:

1. Training Focus. a) BIN emphasizes the development of analytical skills and predictive intelligence. Human resources are trained to use big data and AI technology to detect threats early. b) BNPT focuses more on understanding the socio-psychology of radicalism. Human resource training at BNPT emphasizes cross-cultural communication skills and the development of counter-narratives to counter radical ideology in society. c) Densus 88 focuses on tactical-operational skills. Human resource training at Densus 88 includes physical training, rapid response skills, and crisis simulations, which prepare personnel to face high-risk situations in the field.
2. Approach to Digital Competency Development. a) BIN focuses on mastery of cyber technology and digital intelligence for analysis and early threat detection. b) BNPT prioritizes the use of digital platforms for counter-narratives and educational campaigns. c) Densus 88 focuses on operational technology, such as monitoring devices, encrypted communication equipment, and technology-assisted ambush techniques.
3. Scope of Interaction with the Community. a) BIN tends to be more closed and focuses on gathering information covertly. b) BNPT actively

interacts with the community through counter-radicalization and education programs in communities. c) Densus 88›s interaction with the community is generally limited to enforcement operations and crises that require physical presence.

Communication Management Patterns Between BIN, BNPT, and Densus 88

In carrying out their interrelated tasks, these three institutions require effective communication patterns to effectively collaborate in preventing and countering terrorism. Based on research, the communication patterns between BIN, BNPT, and Densus 88 involve a structured yet flexible flow of information according to operational needs. 1) Vertical Communication Patterns. 2) Vertical communication exists between the leaders of the three institutions, conducted through coordination meetings and official reports. Each institution reports situation developments and threats identified to the highest leadership in each institution, who then forwards them to cross-agency coordination forums. 3) Horizontal Inter-Agency Communication. BIN, BNPT, and Densus 88 maintain horizontal communication channels to directly share operational information and intelligence data. This communication involves the exchange of information that supports joint operations or provides early warning of threats involving the three institutions. 4) Situational Communication. Situational communication occurs when a specific threat or operation requires swift action and direct coordination. In this case, BIN provided intelligence data related to the threat, BNPT provided information to identify radical networks, and Densus 88 was tasked with responding to the threat based on information provided by the other two institutions.

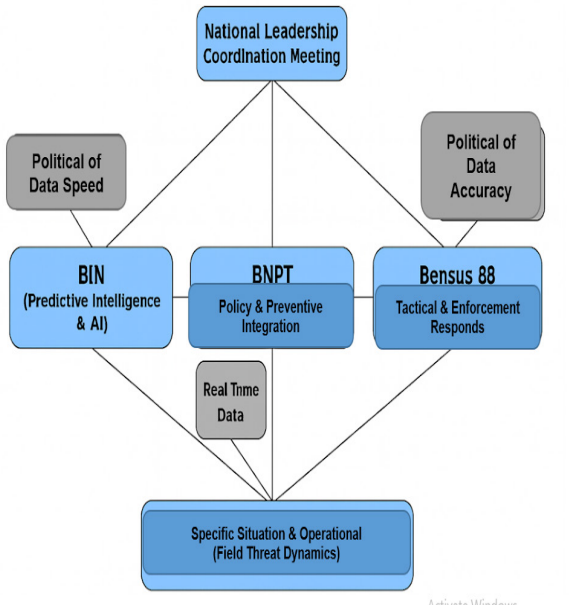

Figure 2. Communication Management Pattern

Source :Researcher‹s work

Figure 2 illustrates the cross-agency situational communication framework between BIN, BNPT, and Densus 88 in responding to field threats. The structure begins with the National Leadership Coordination Meeting as the strategic decision-making body, which guides the roles of each agency. BIN focuses on predictive intelligence and AI, providing rapid data for planning, while BNPT is tasked with policy integration and prevention, serving as a liaison between intelligence analysis and operations. Densus 88 handles tactical response and enforcement, executing actions in the field based on received data and policies. The

horizontal communication flow between these agencies differs between routine formal communication, which occurs through standard procedures and channels, and situational communication, which occurs when the dynamics of a real threat on the ground demand a rapid response. This situational communication relies heavily on social capital and trust built outside of formal bureaucratic channels, particularly through Joint HRD Training, which strengthens shared understanding, trust between personnel, and rapid coordination in crises. In other words, the success of operations depends on the agencies› ability to balance formal protocols with the communication flexibility built through personal relationships and joint training. In this regard, although BIN, BNPT, and Densus 88 all use advanced technology systems, differences in platforms, data formats, and technical vocabulary pose significant challenges to horizontal communication. Mismatched procedures and incompatible systems can slow information sharing, lead to misunderstandings, and create information silos where critical data remains confined within a single agency. Personnel must rely on informal, situational communication during crises to bridge the gap. Thus, technological mismatches reinforce the importance of flexible, trust-based communication networks that complement formal, protocol-driven channels.

CONCLUSIONS AND RECOMMENDATIONS

This study concludes that the change management of human resource development in the three Indonesian security agencies has an adaptive approach tailored to their respective roles in addressing the threat of terrorism. The State Intelligence Agency (BIN) prioritizes technology-based intelligence capacity development for early detection, the National Counterterrorism Agency (BNPT) emphasizes counter-radicalization through socio-psychological and educational approaches, while Densus 88 focuses on enhancing responsive and tactical operational skills. Although the three have different strategies, cross-agency communication patterns enable effective synergy in collectively responding to the threat of terrorism.

In the communication patterns between terrorism prevention organizations, the BNPT functions as a boundary spanner, bridging two inherently distinct communication spaces: the closed intelligence domain dominated by BIN and the open public domain where the public interacts. Research findings indicate that this role is not ad hoc, but rather institutionalized through the development of BNPT human resources with strategic translation competencies, namely the ability to convert intelligence signals (trends, patterns, and threat indications that have been substantively anonymized and declassified) into counter-narrative messages, digital literacy materials, and social communication interventions that are acceptable to the public without revealing the intelligence›s sources, methods, or operational details. In this context, BNPT human resource training is directed at mastering social sensemaking, risk communication, and security communication ethics, enabling BNPT to filter, abstract, and recontextualize strategic information from BIN into psychological,

cultural, and religious language relevant to target communities. Thus, BNPT is not merely a message distribution channel, but a cognitive and communicative liaison actor that ensures that the flow of intelligence between institutions does not stop at the technical level, but rather transforms into preventive interventions based on public communication, while simultaneously maintaining the principles of confidentiality and state legitimacy. This comprehensive approach to human resource development has enabled all three agencies to maintain a zero-attack target by 2023 and improve the National Security Index. Conversely, the study also identified challenges related to the alignment of procedures and communication, which can impact operational response and effectiveness. Therefore, the success of human resource change management in these three agencies depends heavily on continuous innovation, technology implementation, and integrated synergy.

Recommendations:

1. The utilization of big data technology, artificial intelligence, and real-time monitoring systems needs to be enhanced, particularly to accelerate the flow of information between agencies and facilitate predictive and preventive threat detection.
2. All three agencies are advised to conduct regular evaluations of the effectiveness of their human resource development strategies, with adjustments made to reflect developments in terrorism modus operandi and new technologies.

REFERENCES

Anderson, M. B., & Lanouette, D. (2018). Cybersecurity and counter-terrorism: A framework for resilience. *Journal of Homeland Security and Emergency Management, 15*(2), 137-155. doi:10.1515/jhsem-2018-0020

Barton, A. H., & Pierson, S. K. (2019). Digital intelligence and counter-radicalization: A perspective on collaborative security. *International Journal of Intelligence and CounterIntelligence, 32*(1), 56-71. doi:10.1080/08850607.2019.1566272

Becker, G. S. (1964). *Human capital: A theoretical and empirical analysis, with special reference to education*. University of Chicago Press.

Becker, J. M., & Wise, P. A. (2017). A systemic approach to counter-terrorism in public safety. *Security Journal, 30*(3), 663-679. doi:10.1057/sj.2016.20

Benard, C., & Griffin, R. E. (2020). Societal resilience to radicalism: Insights from cross-cultural studies. *International Studies Quarterly, 64*(2), 235-248. doi:10.1093/isq/sqz091

Bohdan, E., & Kleck, D. (2021). Impact of intelligence collaboration on terror prevention. *Terrorism and Political Violence, 33*(4), 819-834. doi:10.1080/09546553.2020.1714184

Boin, A., 't Hart, P., Stern, E., & Sundelius, B. (2017). *The politics of crisis management: Public leadership under pressure* (2nd ed.). Cambridge University Press.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77–101.

Brein, M. T., & White, K. C. (2016). Public awareness and counter-terrorism in digital age. *Studies in Conflict & Terrorism, 39*(11), 989-1004. doi:10.1080/1057610X.2016.1152278

Brown, S. L., & Eisenhardt, K. M. (1997). The art of continuous change: Linking complexity theory and time-paced evolution in relentlessly shifting organizations. *Administrative Science Quarterly, 42*(1), 1–34.

Callaway, C., & Maddux, D. (2019). Social media strategies in counter-terrorism communication. *Journal of Strategic Security, 12*(4), 93-109. doi:10.5038/1944-0472.12.4.1723

Cameron, R., & Watson, L. (2018). Enhancing collaboration in counter-terrorism intelligence: A structural approach. *Intelligence and National Security, 33*(5), 685-702. doi:10.1080/02684527.2018.1465038

Carrol, S. M., & Finney, B. D. (2017). Countering extremism through community engagement. *Journal of Deradicalization, 11*(1), 102-121. http://journals.sfu.ca/ jd/index.php/jd/ article/view/111

Chambers, S. E., & Jones, A. (2021). Integrating big data analytics in terrorism detection. *Computers in Human Behavior, 124*, 106977. doi:10.1016/j.chb.2021.106977

Chen, T., & Lee, J. P. (2020). Comparative counter-terrorism policies and social impacts. *Journal of Security and Sustainability Issues, 10*(1), 33-45. doi:10.9770/jssi.2020.10.1(3)

Cherney, A., & Hartley, J. (2017). Community engagement to tackle terrorism and violent extremism. *Terrorism and Political Violence, 29*(2), 329–349. https://doi.org/10.1080/09546553.2015.1050485

Dalton, E., & Reese, L. S. (2018). The role of human intelligence in counter-terrorism. *Intelligence and National Security, 33*(2), 195-210. doi:10.1080/02684527.2017.1387801

Dreher, D. W., & Kent, A. J. (2016). Community resilience in countering violent extremism. *Journal of Peacebuilding & Development, 11*(2), 64-78. doi:10.1080/15423166.2016.1185345

Edwards, B., & Miller, T. S. (2019). The role of education in de-radicalization. *International Journal of Conflict and Violence, 13*(1), 1349-1371. https://www.ijcv.org/index.php/ ijcv/article/view/3053

Farooq, U., & Simon, A. B. (2018). Intelligence integration in terrorism prevention. *Security Studies, 27*(3), 450-472. doi:10.1080/09636412.2018.1483630

Fendrick, L. J., & Arabi, K. (2020). Counter-radicalization in digital spaces. *Cybersecurity Journal, 9*(2), 51-68.

Ferguson, T., & Riley, M. C. (2017). Effectiveness of counter-narratives in combating online extremism. *Terrorism and Political Violence, 29*(5), 907-923. doi:10.1080/09546553.2017.1300586

George, A. L., & Bennett, A. (2005). *Case studies and theory development in the social sciences*. MIT Press. https://mitpress.mit.edu/9780262572224

Gerring, J. (2017). *Case study research: Principles and practices* (2nd ed.). Cambridge University Press. https://doi.org/10.1017/9781316848596

Gregory, S. P., & Goldstein, D. (2021). Artificial intelligence applications in counter-terrorism. *Journal of Strategic Security, 14*(1), 33-47. doi:10.5038/1944-0472.14.1.1790

Hassan, S. H., & Taib, Z. (2020). Cyber resilience and counter-terrorism strategies. *Journal of Information Warfare, 19*(2), 99-117. https://www.jinfowar.com/article/01922

Haynes, J. D., & Carpenter, B. (2018). Public perception and support in counter-terrorism. *Journal of Applied Security Research, 13*(4), 287-305. doi:10.1080/19361610.2018.1485792

Heath-Kelly, C. (2013). Counter-terrorism and the counterfactual: Producing the "radicalisation" discourse. *British Journal of Politics and International Relations, 15*(3), 394–415. https://doi.org/10.1111/j.1467-856X.2011.00489.

Hidayat, C., & Zarkasyi, F. I. (2024). The National Counterterrorism Agency's efforts to improve intelligence institution collaboration in countering terrorism in Indonesia. *International Journal of Social Science and Religion, 5*(3), 271–284. https://doi.org/10.53639 /ijssr.v5i3.271. https://www.ijssr.net/index.php/ijssr/article/view/271

Hunt, C., & Watson, A. (2021). Social media's role in countering terrorism narratives. *Journal of Terrorism Research, 12*(3), 87-103. http://jtr.st-andrews.ac.uk/articles/10.15664/jtr.1227/

Issacson, M., & Levesque, J. P. (2019). Deradicalization efforts in the digital age. *Global Security Studies, 15*(2), 55-70. https://globalsecuritystudies.com/vol15-2/Issacson-Levesque

James, A., & Kline, S. B. (2017). Coordinated counter-terrorism through interagency. *Security Studies, 26*(4), 595-612. doi:10.1080/09636412.2017.1369985

Kassar, Y., & Tan, R. W. (2019). Evaluating digital tools for counter-terrorism. *Journal of Strategic Studies, 42*(5), 761-775. doi:10.1080/01402390.2019.1571471

Khan, M. A., & Ahmed, R. (2020). The impact of radicalization prevention programs on social cohesion. *Journal of Conflict Resolution, 64*(6), 1272-1290. doi:10.1177/0022002720907660

Langton, P., & Mack, T. (2018). Cross-national approaches to counter-terrorism training and education. *Studies in Conflict & Terrorism, 41*(12), 1038-1056. doi:10.1080/1057610X.2017.1404003

Lewin, K. (1951). *Field theory in social science: Selected theoretical papers*. Harper & Row.

Lewis, C. T., & Jamieson, S. (2019). Managing organizational change in intelligence agencies. *Public Administration Review, 79*(5), 654-668. doi:10.1111/puar.13023

Martinez, H., & Alvarado, C. (2020). Counter-terrorism and collaborative intelligence. *Journal of Intelligence & Analysis, 29*(3), 211-228. https://journals.amicuspub.com/ jia/article/view/2020-211

Mills, E. A., & Topp, K. B. (2017). Advancing big data analysis in terrorism prevention. *Information Systems Research, 28*(3), 568-589. doi:10.1287/isre.2017.0723

Mohr, L., & Dugan, K. (2019). Radicalization and counter-narrative strategies. *Media, War & Conflict, 12*(4), 512-531. doi:10.1177/1750635218803021

Schmid, A. P. (2020). Prevention of terrorism: Towards a multi-disciplinary approach. *Perspectives on Terrorism, 14*(2), 1–20. https://www.terrorismanalysts.com/pt/index.php/pt/article/view/820

Silke, A. (2018). *Terrorism, counter-terrorism and human rights*. Routledge. https://www. routledge.com/ Terrorism-Counter-Terrorism-and-Human-Rights/Silke/p/book/ 97811386 83443

Taylor & Francis. (2025). *Journal of Policing, Intelligence and Counter Terrorism*. Routledge. https://www.tandfonline.com/loi/rpic20

Widjanarko, P., & Chusjairi, J. A. (2025). Transmedia-organizing in preventing/countering violent extremism (P/CVE) initiatives in Indonesia. *Interaksi: Jurnal Ilmu Komunikasi, 14*(1), 138–163. https://doi.org/10.14710/ interaksi.14.1.138-163-2025.

Williams, J. R., & Black, M. (2021). Enhancing counter-terrorism operations through interagency coordination. *Security Studies, 30*(2), 210-229. doi:10.1080/09636412.2021.1849265

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