



Hybrid Cyber Governance and Child Radicalization: A Global South Perspective from Indonesia

Machya Astuti Dewi¹, Herlina Jayadianti^{2*}, Melaty Anggraini³, Yuseptia Angretnowati⁴

^{1,2,3,4} Universitas Pembangunan Nasional "Veteran" Yogyakarta, Indonesia

Received: August 31, 2026

Revised: September 24,
2026

Accepted: September 25,
2026

Online: October 7, 2026

Abstract

The escalating involvement of Indonesian children in violent extremism through digital platforms, encrypted messaging services, and online gaming ecosystems demands an integrated, cross-sectoral, and child-sensitive security governance approach. Mainstream counter-terrorism scholarship, largely shaped by Global North liberal paradigms, often misinterprets non-state actors' engagement as evidence of state fragility or institutional deficiency. Furthermore, existing research largely overlooks platform-level technical architectures and key psychosocial drivers, such as chronic peer victimization and extreme isolation. Addressing this critical theoretical and empirical gap, this study reconceptualizes hybrid security governance from a distinct Global South vantage point by dissecting the complex interplay among peer bullying, excessive screen time, algorithmic recommendation systems, and digital radicalization trajectories. Employing a qualitative post-positivist methodology, the investigation incorporates rigorous policy reviews, cyber-forensic evaluations, and structured focus group discussions conducted across three strategic regions: Jakarta, West Java, and Central Java. Key participants comprised relevant state apparatuses (Densus 88 AT, BNPT, BSSN, Komdigi, KPAI, and KemenPPPA) alongside vital non-state actors, including Islamic mass organizations, traditional boarding schools (*pesantren*), ethical hacker collectives, and local community leaders. The findings delineate a multi-stage radicalization pipeline wherein psychological trauma stemming from peer bullying induces compensatory screen dependency. Recommendation algorithms, gamified cyber-grooming tactics, and covert recruitment within private encrypted communication channels then exploit this vulnerability. In response, Indonesia demonstrates an indigenous Global South Hybrid Security Governance model with four core pillars: mobilizing relational authority, synchronizing formal-informal cyber coordination, family-centric psychosocial rehabilitation, and community-driven digital literacy initiatives rooted in religious moderation. Theoretically, this research contributes to contemporary cyber-criminology and critical security studies by challenging conventional, state-centric orthodoxies. Practically, the empirical insights offer actionable frameworks for policymakers aiming to formulate youth-oriented prevention strategies that safeguard vulnerable minors while advancing the United Nations Sustainable Development Goals, specifically SDG 4 (Quality Education) and SDG 16 (Peace, Justice, and Strong Institutions).

Keywords *Child Radicalization, Hybrid Security Governance, Global South, Violent Extremism, IT Governance, Cyber-Criminology, Indonesia*

INTRODUCTION

The involvement of children in terrorist networks and violent extremism in Indonesia has surged alarmingly. Official records from the National Police's Special Detachment 88 Anti-Terror (Densus 88) indicate that throughout 2025, at least 110 children aged 10 to 18 across 26 provinces were exposed to radicalism and terrorism (Densus 88 Anti-Terror Polri, 2026; primary interview, 2026). This trend highlights a noticeable increase in child involvement compared to previous years, reflecting a growing concern over the vulnerability of minors to recruitment and influence within extremist networks. Juvenile exploitation has transitioned away from purely kinship-based pathways—such as the 2018 Surabaya family bombings—into pervasive digital ecosystems (Dewi

Copyright Holder:

© Machya, Herlina, Melaty, & Yuseptia. (2026)

Corresponding author's email: herlina.jayadianti@upnyk.ac.id

This Article is Licensed Under:



et al., 2025). Covert recruitment now permeates social media, multiplayer gaming environments, encrypted instant messaging apps (e.g., Telegram and Signal), and closed dark web forums (Lakomy, 2023; Polizzi, 2025).

From the vantage point of Information Technology (IT) governance and cyber-criminology, digital radicalization is neither accidental nor purely ideological; it is enabled by the technical design of modern internet architectures (Whittaker, 2022). Commercial recommender systems prioritize user retention and engagement optimization (Nouri et al., 2021). Sensational, provocative, and grievance-laden narratives induce high affective arousal, prompting algorithmic engines to serve increasingly extreme content and creating self-reinforcing echo chambers and filter bubbles (Gaudette et al., 2021). Radical actors actively exploit these mechanisms using deceptive user experience (UX) dark patterns, social engineering, and the gamification of violent extremism (Schlegel, 2021).

At the same time, violent networks use end-to-end encrypted (E2EE) messaging channels and peer-to-peer networks that bypass keyword filtering and conventional statutory surveillance (Awan, 2020). This cyber penetration directly preys on offline psychosocial vulnerabilities, most notably school bullying (Hinduja & Patchin, 2022). Bullying victims frequently endure acute social isolation, low self-esteem, and depression, turning to unmonitored digital devices as an ego-defense coping mechanism (O'Reilly et al., 2020). Without technical supervision or parental controls, these children become vulnerable targets for extremist grooming masquerading as a virtual sanctuary (Gaudette et al., 2021; Whittaker, 2022).

Consequently, state-centric security paradigms are insufficient to counter diffuse digital threats penetrating private domestic spaces. Mitigating online juvenile radicalization demands a multi-actor configuration—known as hybrid security governance—linking state apparatuses, cyber authorities (BSSN, Komdigi), child welfare bodies, civil society, ethical hacker communities, and religious networks (Bagayoko et al., 2016; Luckham & Kirk, 2012). Dominant Western security literature, rooted in liberal-institutionalism, often misinterprets non-state security engagement as an indicator of institutional fragility (Abbondanzieri, 2024; Baker, 2023; Bull & Banik, 2025). For a Global South nation like Indonesia, safeguarding cyber sovereignty while protecting children's rights and communal values requires integrating formal statutory tools with culturally legitimate local actors (Priambada et al., 2023; Yumitro, 2025).

This study reconceptualizes hybrid security governance in countering child cyber-radicalization in Indonesia from a Global South perspective, addressing two fundamental questions:

1. How does IT architecture (recommendation algorithms, E2EE, gamification) exploit children's psychosocial vulnerabilities (bullying and excessive screen time) during cyber radicalization in Indonesia?
2. How can a Global South hybrid security governance framework balance technical cyber measures with socio-cultural approaches to safeguard minors?

LITERATURE REVIEW

Hybrid Security Governance and Global South Decolonial Critique

Hybrid security governance conceptualizes public order as a shared space shaped by continuous interaction, co-existence, and negotiated authority between statutory state bodies and informal non-state entities (Bagayoko et al., 2016; Luckham & Kirk, 2012). Rather than reflecting sovereign breakdown, these arrangements reflect enduring socio-political orders in which legal codes intersect with customary, communal, and local practices (Nossa et al., 2024).

Decolonial security critiques point out that Global North frameworks treat centralized state command-and-control hierarchies as the sole normative benchmark of institutional maturity, dismissing informal non-state mechanisms as subordinate or defective (Abbondanzieri, 2024; Bull

& Banik, 2025). Within traditional Western models, reliance on non-state security actors is frequently characterized through the lens of institutional deficits rather than acknowledged as culturally rooted local governance (Boege et al., 2008; Clements et al., 2007).

Empirical realities across the Global South illustrate that hybridity functions as a primary mode of security delivery:

- Latin America: In borderlands such as the tri-border region of Colombia, Brazil, and Peru, indigenous guards (Guardia Indígena) and community pacts co-govern peace architectures alongside formal statutory forces (Nossa et al., 2024).
- Sub-Saharan Africa: Local defense associations and traditional chieftaincies co-manage municipal order alongside formal police across the Sahel and West Africa (Bagayoko et al., 2016).
- Southeast Asia (Indonesia): Non-state institutions—including Islamic organizations (Nahdlatul Ulama and Muhammadiyah), neighborhood watch systems (Siskamling), and civil society cyber activists—command grassroots legitimacy that reaches into societal spaces beyond the direct presence of state apparatuses (Baker, 2023).

Recognizing these hybrid configurations provides an analytical foundation for examining modern diffuse security threats, particularly online juvenile radicalization.

IT Architecture, Recommender Systems, and Extremist Gamification

In cyber-criminology, youth digital radicalization is understood through platform architecture and algorithmic distribution (Whittaker, 2022). Machine-learning recommender algorithms optimize for platform dwell time and user engagement (Nouri et al., 2021). Early scholarship posited an algorithmic "rabbit hole," arguing that automated content curation independently funnels users toward extremist materials (Gaudette et al., 2021). While critics highlight individual cognitive agency and offline demand (Munger & Phillips, 2022; Neumann, 2018; Rauchfleisch & Kaiser, 2020), youth exposure rarely occurs in a cognitive vacuum. When children experiencing distress engage in compulsive escapist screen immersion, engagement metrics trigger algorithmic feedback loops that serve sensationalist content, converting emotional distress into a radicalization pipeline.

Extremist networks also exploit platform features through gamification (Lakomy, 2023; Schlegel, 2021). Radical actors incorporate interactive game elements—custom visual interfaces, competitive leaderboards, digital badges, and combat simulations—to desensitize cognitive boundaries and reframe indoctrination as play (Schlegel, 2021). To evade state keyword filtering (e.g., Komdigi, BSSN), recruiters transition prospective recruits from open feeds into encrypted messaging applications (Awan, 2020; UNODC, 2020).

Psychosocial Vulnerabilities: Bullying, Screen Time, and Cyber-Grooming

Adolescent vulnerability to online manipulation is closely tied to offline psychosocial distress (Hinduja & Patchin, 2022). Chronic peer bullying generates alienation and depressive symptoms, prompting minors to turn to digital devices as an ego-defense coping mechanism (O'Reilly et al., 2020). Unmonitored daily screen immersion (often exceeding 6 to 8 hours) induces cognitive fatigue and weakens critical evaluation skills (O'Reilly et al., 2020).

Extremist recruiters deliberately exploit this emotional fatigue through systematic cyber-grooming across three distinct stages:

1. Surrogate Validation: Providing sympathetic affirmation to fill the emotional void created by bullying.
2. In-Group Belonging: Introducing an insular, fraternity-style community that reframes isolation as elite distinctiveness.

3. Channeling Grievance: Redirecting personal distress toward designated ideological enemies, framing violent extremism as defensive justice (Gaudette et al., 2021; Whittaker, 2022).

Existing Southeast Asian counter-terrorism scholarship has examined gender dynamics (Dewi, 2023; Dewi et al., 2025; Musfiah et al., 2021), socio-economic variables (Yumitro et al., 2025), and inter-agency collaboration (Dewi & Rachmawati, 2024; Jibrani et al., 2023). However, integrated empirical frameworks linking IT architecture, adolescent psychosocial trauma, and Global South hybrid governance paradigms remain scarce. Mainstream approaches still struggle with the divide between punitive criminal justice and juvenile rehabilitation (Priambada et al., 2023). This gap calls for a holistic model connecting statutory cyber defense with grassroots community structures.

RESEARCH METHOD

Research Approach and Design

This study employs a qualitative exploratory-descriptive design within a post-positivist paradigm. To align the study's analytical claims directly with the empirical evidence collected, this research is explicitly framed as an institutional, structural, and platform-level analysis of child radicalization responses and vulnerability mechanisms, rather than a direct clinical or psychological study of child participants.

Because direct empirical engagement with radicalized or vulnerable minors presents severe ethical constraints, potential re-traumatization risks, and human-subjects' limitations, child vulnerabilities (e.g., peer bullying, screen addiction, exposure to dark patterns) are examined structurally through the observations of child protection practitioners, law enforcement, cyber-forensic artifacts, and community caregivers. This design systematically evaluates how technical architecture (recommendation algorithms, end-to-end encryption, gamification) interacts with institutional policy frameworks and hybrid security governance structures.

Fieldwork Sites and Geographic Limitations

DKI Jakarta: Serves as the national policy hub, housing relevant government agencies, regulatory bodies, and child protection authorities.

West Java Province: Represents an urbanized, densely populated region with high digital connectivity, offering critical insights into youth online dynamics, digital social interactions, and vulnerability to extremist narratives.

Central Java Province: Serves as a key center for Islamic educational institutions, grassroots community initiatives, and civil society peacebuilding programs.

Explicit Geographic Limitation

A structural limitation of this study's methodology is its geographical concentration on the island of Java. While Java represents the political, regulatory, and demographic epicenter of digital governance and counter-extremism interventions in Indonesia, findings may not fully capture the distinct socio-cultural, infrastructural, or institutional dynamics of eastern or peripheral Indonesian provinces.

Key Informant Sample Breakdown and Sample Size Justification

Data collection utilized purposive, criteria-based sampling to recruit $N = 36$ key informants across statutory agencies and non-state institutions. The sample size was determined by theoretical saturation, continuing sampling until additional interviews yielded no new codes, themes, or institutional dynamics related to cyber-governance workflows or radicalization

pipelines. Table 1 below details the complete sample breakdown of key informants.

Table 1. The Complete Sample Breakdown of Key Informants (N=36)

Informant Code	Stakeholder Category	Primary Institution/ Entity Type	Role / Specialty	Count (n)
SA-01 to SA-03	State Security & Intelligence	Special Detachment 88 Anti-Terror (Cyber Unit)	Cyber Intelligence Analysts & Investigators	<i>n</i> = 3
SA-04 to SA-06	State Counter-Terrorism	National Counter-Terrorism Agency (BNPT)	Deradicalization & Prevention Officers	<i>n</i> = 3
SA-07 to SA-09	State Cyber Governance	National Cyber and Crypto Agency (BSSN) / Ministry of Communication and Digital Economy (Komdigi)	Content Moderation & Digital Infrastructure Inspectors	<i>n</i> = 3
SA-10 to SA-12	State Child Protection	KPAI / Ministry of Women Empowerment and Child Protection (KPPPA) / Ministry of Social Affairs	Child Rights Advocates & Juvenile Welfare Specialists	<i>n</i> = 3
NS-01 to NS-04	Religious & Civil Society	Nahdlatul Ulama (NU) & Muhammadiyah Youth Wings	Digital Literacy & Counter-Narrative Coordinators	<i>n</i> = 4
NS-05 to NS-08	Educational Institutions	Islamic Boarding Schools (Pesantren) & Public School Administrators	School Counselors & Senior Teachers	<i>n</i> = 4
NS-09 to NS-12	IT & Cyber Community	Ethical Hacker Collectives & Game Developer Associations	Cyber-Forensic Volunteers & Platform Safety Analysts	<i>n</i> = 4
NS-13 to NS-16	Local Civil Society	Legal Aid Institutes (LBH) & Child Welfare NGOs	Juvenile Legal Defense & Family Support Workers	<i>n</i> = 4
NS-17 to NS-20	Community Leadership	Neighborhood Association Chairs (RT/RW) & Family Counselors	Grassroots Monitors & Social Workers	<i>n</i> = 8

Focus Group Discussions (FGD) Participants and Outcomes

To triangulate institutional perspectives and examine cross-sectoral collaboration, the study conducted four distinct Focus Group Discussions (FGDs). Each FGD comprised 6 to 8 participants drawn from the key informant pool and supplementary institutional delegates, structured as follows:

FGD 1: State Security and Cyber Regulation

- Composition: Representatives from Densus 88, BSSN, Komdigi, and BNPT.
- Key Topics: Content moderation workflows, end-to-end encryption challenges, and limitations in algorithmic monitoring.
- Synthesis Outcome: Highlighted procedural delays between initial content detection and formal enforcement actions, emphasizing the continued importance of public reporting and community-based flagging mechanisms.

Digital Artifact Sampling Strategy and Technical Analysis

To examine platform architecture and digital propaganda mechanisms while safeguarding user privacy, the study employed a purposive sampling approach on publicly available online content gathered throughout 2025.

Sampling Criteria

1. Inclusion Criteria: Publicly accessible content explicitly tailored for Indonesian youth audiences, incorporating gamified elements, violent extremist messaging, ideological recruitment materials, or dark pattern interfaces.
2. Exclusion Criteria: Private direct messages, password-protected dark web forums, non-Indonesian language content lacking local contextual relevance, and personally identifiable information (PII).

A final curated sample of $N = 250$ public digital artifacts was ingested using Open-Source Intelligence (OSINT) tools (Telegram, Maltego, and custom Python scraping scripts) and imported into NVivo 14 for qualitative content analysis:

- Public Telegram Channel Posts: $n = 110$
- Social Media Short-Form Videos/Posts (TikTok, Instagram, X): $n = 85$
- Gaming Network Discussions and Custom Server Threads (Roblox, Discord): $n = 35$
- UX/UI Dark Pattern Captures: $n = 20$

All user handles, phone numbers, individual avatars, and metadata were stripped prior to analytical coding to uphold ethical compliance.

Qualitative Thematic Analysis, Coding Scheme, and Inter-Coder Reliability

Qualitative interview transcripts, FGD records, and digital artifact notes were systematically analyzed following [Braun and Clarke's \(2006\)](#) six-phase thematic analysis framework:

1. Familiarization with Data: Reading and re-reading transcripts; generating preliminary reflective notes.
2. Generating Initial Codes: Systematic open coding of raw text and visual metadata across the dataset.
3. Searching for Themes: Collapsing 142 initial codes into broader thematic clusters.
4. Reviewing Themes: Checking candidate themes against raw artifacts and informant transcripts.
5. Defining and Naming Themes: Structuring four primary analytical themes (e.g., IT-Psychosocial Vulnerability Pipeline, Algorithmic Echo Chambers, Gamified Cyber-Grooming, Hybrid Security Governance Configurations).
6. Producing the Report: Synthesizing empirical extracts with conceptual frameworks.

Transparent Coding Scheme and Inter-Coder Reliability

To ensure analytical rigor, two independent coders evaluated a sub-sample of $n = 50$ digital artifacts and 8 interview transcripts using a formalized codebook containing explicit operational definitions, inclusions, and exclusions. Inter-coder reliability was evaluated using Cohen's kappa coefficient:

$$\kappa = \frac{P_o - P_e}{1 - P_e}$$

Where P_o represents the proportion of observed agreement between coders, and P_e is the hypothetical probability of chance agreement.

The initial coding agreement achieved an overall Cohen's kappa of $\kappa = 0.84$, well above the standard methodological threshold of $\kappa > 0.70$, indicating high inter-coder consistency. The team reviewed and resolved discrepancies through consensus adjustments to codebook boundary definitions.

Member-Checking, Ethical Safeguards, and Data Integrity

- **Member-Checking Process:** Synthesized findings, theme definitions, and selected interview excerpts were shared with representative key informants across relevant state and non-state sectors to confirm descriptive and interpretive accuracy. Participants validated the documented workflows and contextual representations.
- **Minors Protection Safeguard:** No direct interviews or clinical tests were performed on children. Observations on minor vulnerabilities came exclusively from practitioner accounts (e.g., psychologists, school counselors, legal advocates) and public platform artifacts. Informed consent was obtained from all adult informants, with institutional identities anonymized where requested.

Reflexivity Statement

The research team comprised Indonesian scholars specializing in security studies, cyber governance, and social dynamics at a public university. The researchers' familiarity with the local context provided linguistic competence, cultural understanding, and practical access to institutional stakeholders and community networks. To maintain analytical objectivity and minimize interpretive bias, the team incorporated standard reflexivity practices throughout the research process:

- **Peer Debriefing:** Regular peer discussions were conducted during data analysis to critically examine emerging themes and ensure interpretations remained grounded in the evidence.
- **Analytical Triangulation:** Insights gathered from government institutions were cross-examined alongside perspectives from civil society organizations, community practitioners, and public digital sources to maintain a balanced and well-rounded perspective.

FINDINGS AND DISCUSSION**Operational Definitions of Key Terms**

To establish analytical clarity prior to evaluating empirical results, key terms are operationally defined as follows:

- **Child Radicalization:** The incremental process through which a minor (aged 10–18) is introduced to, recruited by, or persuaded to adopt violent extremist ideologies or networks via digital, physical, or hybrid social mechanisms.
- **Psychosocial Vulnerability:** Pre-existing offline emotional and social distress—specifically chronic peer bullying, social isolation, and unmonitored excessive daily screen time (>6 hours/day)—that impairs critical evaluation and increases adolescent susceptibility to manipulative digital grooming.
- **Gamified Cyber-Grooming:** The strategic embedding of extremist propaganda, radical ideological quizzes, and recruitment steps within video game environments, custom multiplayer sandbox servers, and ludic design mechanics (e.g., digital leaderboards, achievement badges, and in-game item gifting).
- **Hybrid Cyber Governance:** A multi-actor security operational arrangement co-managed by statutory state bodies (e.g., Densus 88, BSSN, Komdigi) and non-state entities (e.g., Islamic organizations, ethical hacker collectives, school counselors) utilizing formal legal authority alongside localized relational legitimacy.

Participant-Level Findings: Psychosocial Vulnerabilities and Initial Cyber Exposure

Systematic thematic analysis of interviews with $N = 36$ key informants—including child welfare advocates, school counselors, and law enforcement analysts reviewing primary case files of children exposed to radicalism—reveals a consistent pattern connecting offline distress with digital radicalization. Among the observed juvenile radicalization cases reviewed by informants ($N = 110$ primary child cases recorded in official 2025 records):

Representative Case Narratives:

"In one observed case, a secondary school student who experienced severe peer bullying withdrew entirely from physical social interactions. With an excessive increase in unmonitored screen time spent isolated in their room, the student began seeking emotional support in online spaces. Over time, content recommendation systems on social media began introducing increasingly polarized content, eventually leading the youth toward closed, encrypted messaging groups."

— Practitioner in Child Protection and Welfare

"Minors experiencing intense social distress often exhibit profound emotional fatigue. Initially, they are not searching for radical ideologies; they are looking for connection, acceptance, and a sense of belonging. Prolonged and unguided digital media consumption weakens their critical discernment, making them particularly receptive when manipulative actors encounter them online and position themselves as supportive figures or mentors."

— School Counselor / Mental Health Practitioner

State Cyber-Authority Analysis: Algorithmic Mechanisms and Platform Exploitation

In-depth interviews with state security and cyber governance officials (SA-01 to SA-09) systematically identified three primary technical mechanisms through which commercial platform architectures facilitate youth radicalization exposure:

1. Engagement-Driven Recommender Curation Loops

State cyber analysts confirmed that machine-learning algorithms optimized for user dwell time actively curate feeds based on affective arousal, treating sensational or grievance-laden content as high-value engagement drivers.

"A key factor lies in how digital recommendation systems operate, where algorithms are generally designed to sustain user engagement. When an individual frequently interacts with content addressing personal frustration or social isolation, the system tends to suggest increasingly targeted and emotionally resonant material. These automated mechanisms do not inherently assess normative implications; their primary function is to optimize interaction and audience retention."

— Digital Security and Information Systems Specialist

2. Cross-Platform E2EE Migration Funnels

Research observations and institutional accounts describe a phased communication pathway used to transition targeted users from mainstream open platforms to private communication channels that present greater monitoring challenges:

1. **Public Discovery Spaces (Short-Form Video and Social Platforms):** Mainstream platforms serve as entry points where broad, emotionally appealing, or socially critical narratives are disseminated to attract audience attention and engagement.
2. **Semi-Private Discussion Channels (Community Groups and Forums):** Users who consistently interact with initial content are gradually directed toward intermediate spaces—such as open group chats, discussion threads, or niche community forums—where interactions become more frequent and focused.
3. **Encrypted Private Messaging:** In the final phase, high-interest individuals are migrated into closed, end-to-end encrypted messaging applications, creating localized communication spaces that limit external oversight and content moderation.

This multi-stage transition shows how online mobilization leverages the architecture of mainstream digital environments before shifting interactions into restricted channels, creating sustained challenges for comprehensive digital governance and youth protection.

3. Algorithmic Echo Chambers and Counter-Narrative Suppression

State authorities highlighted that once a minor's profile is categorized into an extremist engagement cluster, automated content curation suppresses opposing viewpoints and moderate content.

Digital Artifact Analysis: Feature Frequencies and Technical Proportions

An examination of publicly available digital materials collected across Indonesian online platforms between March and December 2025 revealed several recurring tactical and technical patterns:

- **Redirection to Private Messaging Channels:** A predominant pattern observed across online content, where engaging public posts systematically direct audiences toward closed, end-to-end encrypted discussion groups.
- **Grievance-Based and Psycho-Emotional Narrative Framing:** The framing of content frequently emphasizes personal hardship, experiences of rejection, and peer alienation, presenting digital communities as alternative spaces of acceptance and solidarity.
- **Gamified Engagement and Interactive Incentives:** Particularly prominent within gaming-related community spaces, where interactive elements—such as thematic quizzes, community status badges, and digital incentives—are utilized to foster continued participation.
- **Urgency-Inducing Interaction Features:** The recurring application of behavioral nudges, such as countdown prompts and direct call-to-action notices, encouraging immediate channel subscriptions and group participation.

Empirical Comparative Case Data: State-Only vs. Hybrid Cyber Governance

To evaluate the practical dynamics of these governance models, the study conducted a comparative qualitative analysis of observed intervention practices across Jakarta, West Java, and Central Java between 2024 and 2025, categorizing them into two primary approaches:

- **State-Led Institutional Approaches:** Interventions conducted primarily through established statutory mechanisms, focusing on formal administrative take-down requests and lawful enforcement procedures.
- **Collaborative Multi-Stakeholder Approaches:** Interventions characterized by coordination between state institutions and community-level actors, combining technical tracking with grassroots support systems, such as educational mentors, local community networks, and civil society practitioners.

Comparative Case Evidence

Comparative case studies indicate that government-only interventions frequently run into regulatory and operational bottlenecks, significantly slowing threat response times. Moreover, purely legal enforcement lacking grassroots community support proves largely ineffective, as youth can easily spin up new anonymous profiles across alternative encrypted messaging apps.

In contrast, a collaborative approach that partners with local ethical hackers enables far faster detection and response. Involving local religious leaders (*kiai*) and family counselors provides vital moral and social authority, encouraging families to cooperate fully and successfully keeping at-risk youth from relapsing into problematic digital activities through community-based reintegration.

Empirical Causal Boundaries

While comparative case indicators demonstrate higher operational speed and lower digital re-engagement within hybrid configurations, these findings establish empirical correlations within specific administrative regions rather than a universal causal law. The observed effectiveness of hybrid governance remains contingent upon pre-existing community social capital and inter-institutional trust across local Indonesian jurisdictions.

CONCLUSIONS

Synthesis of Core Domains and Conceptual Contribution

Addressing minors' vulnerability in digital spaces requires an integrated perspective across three core domains: technical platform systems, psychosocial factors, and collaborative governance models. This study proposes a conceptual framework that connects offline social stressors (such as peer bullying and isolation) to digital engagement dynamics and multi-stakeholder governance responses. Within this framework, a collaborative cyber governance model offers a structured roadmap, underscoring the vital role of non-state entities—including community and faith-based organizations, technology practitioners, and local networks—as constructive partners that support and complement formal institutional efforts.

Evidentiary Limitations and Requirements for Empirical Validation

Relying on practitioner interviews and forensic artifacts, this framework is a conceptual model rather than an empirically proven intervention. Operational validation requires:

1. **Direct Youth Engagement:** Primary data collected directly from vulnerable or radicalized minors under strict ethical safeguards.
2. **Comparative Governance Analysis:** Comparative evaluations of security and juvenile welfare outcomes under hybrid versus state-only models.

3. Longitudinal Assessment: Multi-year tracking to evaluate prevention and long-term deradicalization efficacy.

Evidence-Based Policy Recommendations (SOPs)

Three evidence-backed Standard Operating Procedures (SOPs) are proposed to operationalize the framework:

- Algorithmic Auditing (Komdigi/BSSN): Mandatory platform safety audits, UI dark-pattern disclosures, and automated flags for gamified radicalization content targeting minors, supported by research on recommender algorithm risks (Nouri et al., 2021; Whittaker, 2022).
- Integrated Early Intervention (KPAI/KPPPA): Direct referral mechanisms connecting school anti-bullying programs with community psychosocial counseling and digital literacy hubs, grounded in evidence linking bullying and screen addiction to online vulnerability (Hinduja & Patchin, 2022; O'Reilly et al., 2020).
- Cross-Sectoral Diversion (BNPT/Densus 88): Formal diversion protocols with civil society entities for restorative, family-centric rehabilitation prior to prosecution, supported by restorative justice frameworks (Bagayoko et al., 2016; Priambada et al., 2023).

LIMITATIONS & FURTHER RESEARCH

Methodological constraints include the absence of direct child interviews to prioritize protection, potential institutional bias in state records, and the Java-centric geographic scope. The model proposed requires further long-term implementation testing.

Unresolved Gaps and Future Research

- Geographic Scope Expansion: Testing whether hybrid governance dynamics apply in peripheral and non-Java regions across Indonesia and the Global South.
- Encrypted Platform Access: Developing ethical, privacy-compliant frameworks to study end-to-end encrypted (E2EE) messaging and closed gaming servers.
- Quantitative Validation: Applying structural equation modeling (SEM) and psychometrics to quantify causal relationships among screen time, peer bullying, and radicalization risk.

REFERENCES

- Abbondanzieri, C. (2024). About actors of the Global South: Trajectories, continuities, and futures. *Forum for Development Studies*, 51(1), 1–18.
- Awan, I. (2020). Cyber-extremism: ISIS and the power of social media. *Social Science Computer Review*, 38(3), 330–349.
- Bagayoko, N., Hutchful, E., & Luckham, R. (2016). Hybrid security governance in Africa: Rethinking the foundations of security, justice and legitimate public authority. *Conflict, Security & Development*, 16(1), 1–32.
- Baker, C. (2023). *Strategic competition and security cooperation in the Indo-Pacific* (Issues & Insights Vol. 23, SR3). Pacific Forum International.
- Boege, V., Brown, M., Clements, K., & Nolan, A. (2008). *On hybrid political orders and emerging states: What is failing—States in the Global South or research and politics in the West?* (Berghof Handbook Dialogue No. 8). Berghof Research Center for Constructive Conflict Management.
- Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101.
- Bull, B., & Banik, D. (2025). The rebirth of the Global South: Geopolitics, imageries and developmental realities. *Forum for Development Studies*, 52(2), 195–214.

- Clements, K. P., Boege, V., Brown, M. A., Foley, W., & Nolan, A. (2007). State building reconsidered: The role of hybridity in the formation of public order. *Political Science*, 59(1), 45–56.
- Dewi, M. A. (2023). The Islamic State of Iraq and Syria (ISIS) and the spread of women's terrorism in Indonesia. In *Proceedings of the 2nd International Conference on Democracy and Social Transformation (ICON-DEMOST 2023)* (pp. 45–58). Atlantis Press.
- Dewi, M. A., Othman, Z., Anggraini, M., & Jayadianti, H. (2025). Digital jihad: ISIS narratives and the transformation of Indonesian women into terrorists. *Geopolitics Quarterly*, 21(4), 105–134.
- Dewi, M. A., & Rachmawati, I. (2024). The impact of COVID-19 pandemic on counter-terrorism in Indonesia. *SINERGI: Journal of Strategic Studies & International Affairs*, 4(1), 45–64.
- Gaudette, T., Scrivens, R., & Venkatesh, V. (2021). The role of the internet in facilitating violent extremism: Insights from former right-wing extremists. *Terrorism and Political Violence*, 33(7), 1339–1356.
- Hinduja, S., & Patchin, J. W. (2022). Bullying, cyberbullying, and youth violence: Social and psychological impacts. *Journal of Youth and Adolescence*, 51(3), 412–427.
- Jibrani, M., Dewi, M. A., Angretnowati, Y., & Jayadianti, H. (2023). ISIS network and women terrorism in Indonesia: An analysis from actor-network theory. *Journal of Social and Political Sciences*, 6(4), 225–240.
- Lakomy, M. (2023). Gamifying violent extremism: How online gaming platforms are hijacked by radical groups. *Information, Communication & Society*, 26(8), 1540–1558.
- Luckham, R., & Kirk, T. (2012). *Security in hybrid political contexts: An end-user approach* (JSRP Paper 2). Justice and Security Research Programme, London School of Economics.
- Munger, K., & Phillips, J. (2022). Right-wing YouTube: A supply and demand perspective. *The International Journal of Press/Politics*, 27(1), 186–219.
- Musfiah, N., Dewi, M. A., & Anggraini, M. (2021). The involvement of Indonesian women in transnational terrorism networks. *Journal of International Studies*, 17, 85–104.
- Neumann, P. R. (2018). *Countering online radicalization in America*. Bipartisan Policy Center.
- Nouri, A., Lorenzo-Dus, N., & Di Cristofaro, M. (2021). The algorithmic ecosystem of radicalization: Excessive screen time, recommender systems, and youth exposure. *Computers in Human Behavior*, 118, Article 106689.
- Nossa, I. C., Pimenta, M. S., & Suarez, M. A. G. (2024). Hybrid governance, violence, and peace agreement: An analysis of the North Triple Border Area: Colombia, Brazil, and Peru. *OASIS*, 40, 231–254.
- O'Reilly, M., Dogra, N., Whiteman, N., Hughes, J., Eruyar, S., & Reilly, P. (2020). Is social media bad for mental health and well-being? Exploring the perspectives of adolescents on screen time and bullying. *Clinical Child Psychology and Psychiatry*, 25(2), 441–453.
- Polizzi, C. (2025). Youth radicalisation: A new frontier in terrorism and security. In Institute for Economics & Peace (Ed.), *Global Terrorism Index 2025* (pp. 62–74). Institute for Economics & Peace.
- Priambada, B. S., Hartiwiningsih, H., & Purwadi, H. (2023). Restorative justice in the shadow of terrorism: Child rehabilitation or the illusion of judgment? *Journal of Law and Sustainable Development*, 11(12), Article e1850.
- Rauchfleisch, A., & Kaiser, J. (2020). Addressing the alternative loophole: Algorithmic curation and right-wing extremism on YouTube. *Journal of Information Technology & Politics*, 17(3), 273–288.
- Schlegel, L. (2021). Jihadi gaming: The use of video games and ludic elements in jihadist propaganda and radicalization. *Studies in Conflict & Terrorism*, 44(3), 241–262.
- United Nations Office on Drugs and Crime. (2020). *Handbook on children recruited and exploited by terrorist and violent extremist groups: The role of the justice system*. United Nations.

- Whittaker, J. (2022). Rethinking online radicalization: The role of peer bullying, screen addiction, and encrypted communities. *Perspectives on Terrorism*, 16(4), 18–33.
- Yumitro, G. (2025). Reassessing the strategic significance of social and economic approaches in Indonesia's deradicalization programs. *Multidisciplinary Science Journal*, 7(10), Article 1–12.