Jurnal Dinamika Global Vol. 11 No. 1, Juni 2026
P-ISSN 2548-9216 | E-ISSN 2684-9399

COLLABORATIVE SECURITY GOVERNANCE AGAINST TRANSNATIONAL EXTREMISM: POLICY LESSONS FROM ISIS REGIONAL AFFILIATES

Suhirwan[1], Siswo Hadi Sumantri[2], Lukman Yudho Prakoso[3]
[1]Faculty of Defence Strategy, Indonesia Defence University
[2]Faculty of Public Administration, Hang Tuah University
[3]Faculty of Maritime Security, Indonesia Defence University
[1]suhirwan@idu.ac.id

Abstract

Regional Affiliates and the Brokered Governance of IST's Successor. While existent studies have analysed ISIS in detail, less attention has been paid to how governance flaws in digital places and decentralized extremism are changing violence also like the changes accompanying state responses outside of classic state-centred security frameworks. This study employs a qualitative comparative case-study design using semi-structured interviews with fifteen academics, policymakers and practitioners in the fields of governance and security from diverse countries. These interviews were supplemented by secondary data sources and reflexive thematic analysis. The study concluded that rather than the ISIS holding territory it would instead convert to a more diffuse transnational movement centred on regional affiliates which have sprung up like ISIS-K, ISCAP and Boko Haram all optimising digital spaces, propaganda outlets clear comms systems and crypto space for coordination logistics and funding needs. The research also reflects the impacts of weakened institutional coordination, fragmented governance and lack of adequate cyber-governance capacities on responses to adaptive extremist threats. These findings indicate that contemporary transnational extremism is not only a military-security challenge but also a governance challenge, one that will require institutional adaptation, as well as multi-sector collaboration and coordinated digital governance in the future. The insight of this article to security governance literature is to show how the adaptive and collaborative perspectives of governance explain why decentralized extremist networks have evolved in digital age.

Keywords: Adaptive Governance, Collaborative Security, Digital Governance, ISIS affiliates, Transnational Extremism.

INTRODUCTION

Transnational extremism in the post-caliphate era has challenged the integrity of modern security governance and public policy frameworks. After the territorial defeat of ISIS in Syria and Iraq, extremist groups began instead to pursue decentralized organizational structures based on digital mobilization, networked coordination, and more geographically dispersed regional affiliates. Such transformations have greatly widened the operational

range of extremist actors in terms of conventional territorial limits and produced contemporary governance challenges in other jurisdictions (Adigwe et al., 2024; Topal, 2024; Yashlavskii, 2025). Thus, physical security threats are transformed into cyberwarfare to the regulation, and the safety along with risks are now not constrained in corporeal space but rather through adjacent electronic environments. Such an evolution puts into relief approaches to governance which can effectively address transnational and mutating forms of extremism.

Similar recent research has recorded the transformation of ISIS from a territorial-based organization into a digitally networked extremist sub-culture dependent on online propaganda, encrypted communications, and transnational ideological diffusion (Adigwe et al., 2024; Borelli, 2023; Hutchinson et al., 2023). Previous scholarship has also explored the down to earth works of ISIS territorial branches and how recent computerized correspondence frameworks helped routine enrolment and radicalization forms (Jadoon et al., 2023).

Yet, a substantial part of this literature is still concentrating around security operations, military responses and counter-terrorism policies instead of the governance arrangements necessary to deal with adaptive extremist ecosystems. Consequently, less effort has focused on how governance institutions coordinate through different sectors, jurisdictions and policy domains when responding to decentralized extremist threats. This gap is significant for analysing the evolving adaptive (re)use of governance systems to an ever-dividing lexicon of transnational extremism.

A number of ISIS-associated regional affiliates have entered the mix as notable players in modern extremist ecosystems, most notably ISIS-Khorasan Province (ISIS-K), Islamic State Central Africa Province (ISCAP), Boko Haram factions and Abu Sayyaf-linked groups. Despite working in different political and socio-economic contexts, these organizations are linked through a present-day ideological narrative and transnational communications networks. The ability of those lavishing on them to exploit governance

weaknesses locally, prey upon black markets and tech-savvy rebels adds layers of complexity in the post-caliphate extremist environment (Jadoon et al., 2023; Makosso & Political, 2021; Tasev, 2025).

The above developments imply that modern extremism is not only a security concern, but also a governance issue associated an institutional adjustment process, policy alignment and multi-actor engagement. To appreciate these dynamics we need analytical frameworks that can explain how governance systems adapt to respond to adaptive and networked threats.

How major ISIS regional affiliates have operated, however, shows how decentralized extremist actors remain adapted to local conditions while linked to transnational ideas. Such features point show governance vulnerabilities can go beyond typical military and intelligence responses. Table 1 Adaptive Features of Key ISIS Regional Affiliates and Governance Implications.

Table 1. Characteristics of ISIS Regional Affiliates in the Post-Caliphate Era

ISIS Affiliate	Operational Region	Adaptive Characteristics	Governance Challenges
ISIS-K	Afghanistan and Central Asia	Online recruitment and decentralized cells	Border governance and intelligence coordination
ISCAP	Central Africa	Local insurgency integration	Weak regional institutional capacity
Boko Haram factions	West Africa	Hybrid extremist-criminal networks	Cross-border governance fragmentation
Abu Sayyaf-linked groups	Southeast Asia	Maritime mobility and digital networking	Regional coordination and cyber monitoring

Source: Adapted from Jadoon et al. (2023), Makosso & Political (2021), and Tasev (2025)

These shared trends among regional affiliates suggest transnational extremism now acts through a fusion of governance spaces rather than within local enclaves. Thus, counter-extremism responses need governance mechanisms that effectively coordinate across multiple actors dispersed

across varying institutional and territorial contexts. However, in the context of these shifting extremist trends, 21st century governance is tasked with devising systemic and enduring strategies to mitigate the crisis. The below discussion identifies important governance restrictions which are affecting collaborative counter-extremism efforts.

Counter-terrorism policies are still overwhelmingly state-centric, in which military interventions, border security and intelligence operations provide the blueprint for response to terrorist incidents. Although these measures are still important tools in countering threats, they often lack the capacity to contain decentralised networks of extremists working across digital and transnational terrains (Baldaro & D'Amato, 2024; Bonsoms, 2025; D'Amato, 2021). Ineffective responses are thus frequently seen as a result of fragmented political and social systems, and some scholars increasingly argue that effective responses only become possible through collaborative governance arrangements of state institutions, regional organizations from beyond borders, civil society actors from inside the population affected by crises (or seeking refuge), as well as technology providers. From this point of view, collaborative governance is defined as formalized processes in which public and non-public actors jointly participate in decision making; setting the agenda; sharing resources; or implementing policies to deal with complex public problems. These arrangements become especially important as the threat of extremism goes beyond the scope a single institution.

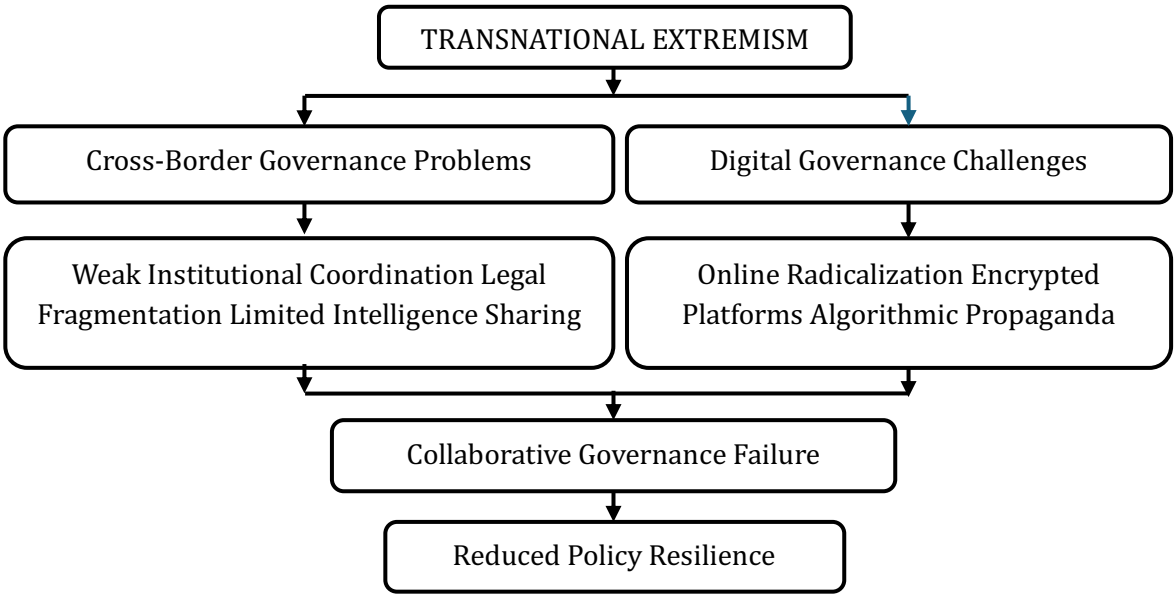
Yet, while there is growing recognition for a collaborative approach, counter-extremism efforts are still hindered by governance fragmentation at the local and regional levels. Many actors working across jurisdictions are impeded from achieving effective coordination at least in part because of differences in legal frameworks, intelligence-sharing mechanisms, institutional mandates and policy priorities (Bala & Tar, 2021; Calléja, 2021; Wanderi et al., 2022). The limitations of cyber-governance also make it difficult to oversee encrypted communication methods and virtual extremist groups (Anil & Babatope, 2024; Huang et al., 2022; Savaş & Karataş, 2022). This suggests that coordination failures emerge not only from resource

scarcity, but also from institutional complexity and governance fragmentation. Drawing on coordination processes, actor relations, and institutional interactions, collaborative governance serves as a framework for analysis regarding counter-extremism efforts. Unlike collaborative governance, adaptive governance highlights the ability of institutions to learn, adapt and respond to highly dynamic environments.

Adaptive governance evolves from network governance by highlighting institutional flexibility over network structures and from resilience governance by focusing on continuous policy adjustment, rather than the capacity to recover. In the transnational extremism theme context, adaptive governance involves changing policy instruments, coordination mechanisms between co-operative partners, intelligence practices and cyber-governance strategies to respond quickly to fast-moving extremist tactics. Adaptive governance indicators include institutional learning, policy flexibility, responsive technology and ability to coordinate across sectors (Barker Scott & Manning, 2024; Martini, 2024; Rajola et al., 2025). These features offer a more operational lens through which we can analyse the governance responses to evolving extremist threats.

In certain contexts — such as digitally mediated extremist environments — the interplay between collaborative governance and adaptive governance is especially salient. Collaborative governance provides the answer to how actors coordinate through institutional boundaries, while adaptive governance addresses how the governing system and elements of governing systems can adjust to changing threat conditions. Collectively these positions provide a broad framework for understanding contemporary frames of counter-extremism governance. The governance challenges at play for collaborative counter-extremism in the digital age.

Figure 1. Governance Challenges in Collaborative Counter-Extremism



Source: Author devised from Bonsoms (2025), Huang et al. (2022), and Melaku (2023)

In fact, Figure 1. demonstrates that governance failures are often caused by the interactions among institutional fragmentation, cyber-governance limitations and the less adaptive capacity. The way these weaknesses are interrelated makes clear why governance models must incorporate co-evolutionary dynamics that can adapt in transnational security contexts.

While cyber extremism, online radicalization and cybersecurity governance have recently been studied, little comparative research has examined how collaborative and adaptive governance functions across diverse ISIS regional affiliate contexts. In the literature, research on governance focusing on nonstate actors is ageconised to particular areas or certain dimensions of security (Bonsoms, 2025; Melaku, 2023; Sullivan, 2025). To add, contemporary counter-extremism scholarship is still limited in terms of collaborative governance and adaptive governance. This gap restricts theoretical investigations into the conditions under which governance arrangements can enhance institutional reprieve from decentralized radical extremist networks.

This paper explores state and non-state actor involvement in collaborative governance around countering violent extremism and its role in threat mitigation of the extremist variety. It further examines governance challenges resulting from the application of collaborative approaches between these actors. The study draws on adaptive governance to examine policy interventions that can improve institutional coordination, thus reinforcing resilience to external shocks of extremist actions. This research advances our understanding of multi-actor governance dynamics and provides insights into how policy may be improved by informing policymakers advocates, practitioners through the analysis of emerging complexities impacting contemporary challenges associated with extremism.

This paper contributes to the literature in three ways by answering these questions: It brings the concepts of collaborative governance and adaptive governance to inform counter-extremism analysis; It develops an explanation of transnational extremist adaptation based on governance; and It draws comparative policy lessons on how best to strengthen the governance of security in digitally interconnected environments.

These objectives form the analytical foundation underpinning this study. In this section, we present the qualitative comparative research design, data collection procedures and thematic analytical framework used to explore governance responses to transnational extremism.

Research Methods

Using a qualitative methodology, and building on the collaborative & adaptive governance framework introduced above, this study explores responses to transnational extremism in a post-caliphate context. The methodological design was established in order to examine modes of coordination, adaptation and response by both state and non-state actors in the context of changing forms of extremist threat in different regional contexts.

The study adopts a qualitative comparative case-study design to address collaboration in security governance in response to transnational

extremism linked to ISIS affiliates in the region. We took a qualitative approach, which is most appropriate to undertake a detailed analysis of governing processes and inter-institutional relations in the adaptation of policies for complex security environments. Qualitative inquiry is well-suited for understanding how actors make sense of and react to contextual change in meaningful ways (Patton, 2015; Tracy, 2013). The comparative design enables the analysis of commonalities and differences among governance responses between Central Asia, Africa, and Southeast Asia where extremist threats differ in their operational characteristics but exist within a transnational framework ((Rashid et al., 2019; Viera, 2023). The focus of the study is therefore on generating analytical insights about governance and institutional responses to different contexts instead of statistical generalisation. This methodology aligns with governance-focused qualitative research emphasizing exploratory depth and context-sensitive interpretation (Annamalah, 2024; Bonsoms, 2025).

The paper explores collaborative governance and adaptive governance as main ideational frameworks for analysis. I focus on aspects such as actor involvement, inter-organisational coordination/assembly, and monitoring and sharing information to enact joint policy responses-instrumental variables based on the analytical tradition of collaborative governance. In analysing institutional learning, policy flexibility, technological responsiveness and adaptation of governance to changing extremist threats, adaptive governance is used. These analytical perspectives guided our data collection, coding, and thematic interpretation — throughout the study. Thus governance concepts serve as analytical tools and not as normative policy options.

Because of the especially comparative and governance-focused orientation of the design, we required evidence from actors involved in counter-extremism governance. For that purpose, selection of participants and collection of data was designed carefully to include a variety in perspectives while still being relevant analytically to answer the research questions.

The study provides a framework that articulates in which research design and analytical procedures hypothesis relate to governance concepts with empirical data, before it presents participant profiles. The framework shows how the collaborative governance and adaptive governance guided the study from obtaining data to interpretation.

Table 2. Research Design Framework

Component	Description
Research Approach	Qualitative Research
Research Strategy	Comparative Case Study
Analytical Orientation	Governance-Oriented Analysis
Main Focus	Collaborative Security Governance
Unit of Analysis	ISIS Regional Affiliates and Governance Responses
Governance Frameworks	Collaborative Governance, Adaptive Governance, Network Governance, Resilience Governance
Data Sources	Interviews and Secondary Literature
Comparative Regions	Central Asia, Southeast Asia, Africa

Source: Developed by the author based on Annamalah (2024), and Viera (2023).

The framework suggests comprehensive existence of the link between governance theory and empirical testing through transnational security studies. It also explains how to relate research questions and governance concepts to procedures of comparative case-study.

Data Collection

Using a mix of semi-structured interviews and secondary literature review, data collection sought multiple perspectives on the collaborative security governance. This includes selection of 15 participant by purposive sampling based on defined inclusion criteria rather than representativeness of a wider population. Purposive sampling is very well advocated in qualitative research as it enables the researchers to select participants who have huge experience and knowledge related to the phenomenon (Patton, 2015).

Informants had to have a minimum of five years working or academic experience in relevant fields such as counter-extremism policy, governance, cybersecurity, or regional security cooperation. Moreover, whether the

individuals are involved directly with policy making and implementation, research or regional coordination regarding issues related to transnational insecurity was another selection criterion. This approach ensured that respondents were able to give reflective and knowledgeable insights into governance practice and institutional challenges relevant to the objectives of this study (Baxter & Jack, 2008; Dusdal & Powell, 2021).

The sampling of participants was purposively done to enhance variation in perspectives on governance across their different professions. Academics informed theory and analyses; policymakers brought institutional perspective; security practitioners contributed on the operational level; governance experts wrote about coordination; local or community-level responses came from regional voices. It was a diversity designed to furnish analytic triangulation rather than numerical representation. In contrast to quantitative governance research, sample size alone is not attributable for quantifying adequacy in participants; therefore, thematic sufficiency and information richness were instead used (Patton, 2015; Tracy, 2013). This was to evaluate the complexity of governance across various institutional settings.

Table 3. Profile of Research Participants

Participant Category	Number	Main Expertise
Academics	4	Terrorism Studies, Governance
Policymakers	3	Public Policy and Security Governance
Security Practitioners	4	Counterterrorism and Cybersecurity
Governance Experts	2	Collaborative Governance
Regional Stakeholders	2	Community and Policy Coordination

Source**:** Developed by the author based on field data (2026)

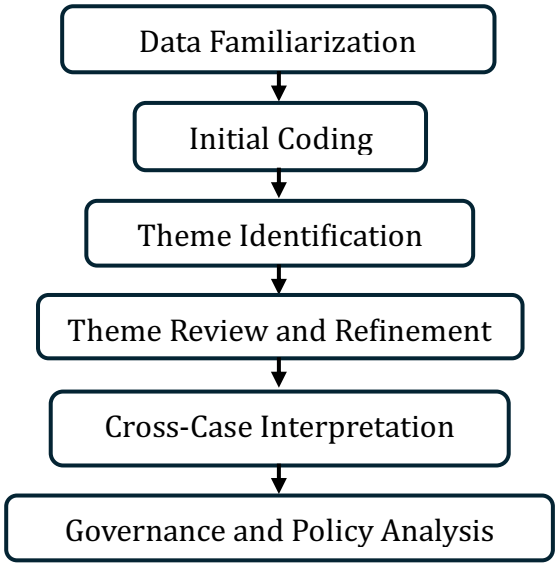
Participant profile showing the multisectoral expertise represented in this study. This diversity bolsters the capability of both analyses to find governance challenges both across and within sectors, institutions and regions.

Data Analysis

Data were analysed using reflexive thematic analysis to identify meaning making patterns in interview transcripts and documentary sources. For analysis, (Braun & Clarke, 2022, 2023) reflexive thematic process was adopted but also included governance-focused coding categories that pertained to the study objectives (Campbell et al., 2021). Reflexive thematic analysis was chosen for its flexible but systematic framework for identifying, analysing, and interpreting patterns within qualitative data while recognising the active role of researchers in knowledge generation (Braun & Clarke, 2022).

Coding was implemented across different iterative stages including familiarisation, open coding, refinement of codes, theme development and cross-case interpretation. Inductively generated initial codes from the data were then categorised into governance-related categories. This allowed for the systematic analysis of collaborative governance mechanisms and corresponding adaptive governance responses.

Figure 2. Reflexive Thematic Analysis Process



Source: Adapted from Braun & Clarke (2021, 2022, 2023)

Prior to final theme construction, a coding framework was created to support increased transparency and auditability. Some of the preliminary codes included intelligence sharing, institutional fragmentation, cyber monitoring, policy adaptation, regional cooperation, digital radicalisation and plurality of actors. These codes were then further grouped into larger

categories like governance coordination, adaptive capacity, digital governance and institutional resilience. Guided by an exploratory thematic analysis (Braun & Clarke, 2024; Naeem et al., 2023), these categories then informed higher order themes presented within the results section. They maintained an audit trail summarising their coding decisions, changes made to categories and themes that emerged/evolved.

This figure indicates that thematic development was a structured yet reflexive analytical process. It also explains how it has been transparent in releasing specified governance themes derived from empirical data.

Research Validity and Trustworthiness

Triangulation, reflexivity, member checking, and systematic documentation lent credibility to this research. A series of comparisons between the interview findings and relevant elements in policy documents, governance reports, and academic literature was performed to corroborate emerging interpretations (Janis, 2022; Schlunegger et al., 2024).

These processes ensured a sufficient level of credibility, transferability, dependability and confirmability (as per the framework for trustworthiness in qualitative research proposed by Lincoln & Guba (1985)). Triangulation and member checking enhanced credibility, rich contextual description supported transferability, systematic documentation of analytical procedures provided dependability, and reflexive engagement with data interpretation helped confirmability (Lincoln & Guba, 1985).

To keep track of interpretive assumptions and analytic decisions, researchers kept reflexive notes during coding and development of themes. Preliminary interpretations were compared for consistency and credibility with the source materials. In addition, the trustworthiness processes follow recommendations by Nowell et al. An established methodology is followed, for example using transparent coding practices and ensuring that the audit trail is retrievable and systematic in how logical themes are developed (2017). These processes increased both methodological transparency and credibility.

Ethical Approval: The study complied with established ethical standards for qualitative research. Pseudonymisation, secure data storage and informed consent were used to protect participant identities before the interviews (Campbell et al., 2021; Strunel & Cordoba, 2025). The ethical procedures taken included confidentiality and voluntary participation during the research. For this reason, the study incorporates ethical considerations across every phase of data collection and analysis. These protections are especially necessary in areas of research involving security governance and counter-extremism issues.

The study, before wrapping up this section, outlines both the validity and ethical precautions taken throughout the research process.

Table 4. Research Validity and Ethical Framework

Aspect	Implementation
Triangulation	Interviews, literature, policy documents
Reflexivity	Iterative interpretation and researcher awareness
Confidentiality	Anonymization of participants
Ethical Procedure	Informed consent
Credibility	Cross-case comparison and thematic validation

Source: Developed by the author based on Janis (2022), Lincoln & Guba (1985), Nowell et al. (2017), and Schlunegger et al. (2024).

Table 4. depicts systematic integration of validity and ethics during the study. These safeguards instil assurance in the analytical findings and aid compliance to the current qualitative research principles.

DISCUSSION

The results and discussion section offers the key findings from 15 qualitative interviews with experts from a variety of countries (scholars, politicians, governance experts and security specialists). This last section integrates the empirical data with literatures in governance theory and current policy debates to distil how ISIS's regional affiliates have unfolded through ongoing transformations in transnational extremism.

The analysis shows that contemporary extremism can no longer be completely understood through traditional military-security lenses alone. In fact, the evidence identifies increasingly de-centralised extremist networks and the clarion call for coordinated public policy approaches, multi-agency cooperation and most importantly, responsive digital governance.

The Post-Caliphate Period and The Evolution of ISIS Regional Branches

The data suggest that following the fall of ISIS in Iraq and Syria, the organization underwent a significant transformation. Most interviewees argued that ISIS legitimacy is no longer derived primarily from territorial control, but from decentralized networks composed of small groups, clandestine cells, and regional affiliates operating in environments characterized by weak governance. This shift reflects the emergence of adaptive extremist ecosystems marked by operational flexibility, opaque infrastructures, and network-based coordination. Similar trends have been identified by Jadoon et al. (2023), Morris (2024), and Yashlavskii (2025), who describe post-caliphate extremism as increasingly fluid and decentralized rather than organized through centralized command structures.

Respondents also emphasized that ISIS-Khorasan Province (ISIS-K) has become one of the most adaptable and militant regional affiliates in the post-caliphate era. Participants noted that ISIS-K exploits weak governance, porous borders, and ideological polarization to expand recruitment and operational capabilities. By leveraging local grievances, ethnic tensions, and political instability, the group has maintained influence despite sustained counterterrorism pressure. These observations support the findings of Kidwai (2022), and Tasev (2025), who characterize ISIS-K as a hybrid insurgent-extremist actor linking local conflicts with broader transnational extremist narratives.

Interviewees in Africa described the Islamic State Central Africa Province (ISCAP) and Boko Haram factions as adaptable extremist models that depend on local conflicts and governance crises. Informants reported that these groups employ decentralized tactics, territorial mobility, local recruitment, illicit economic activities, and ideological dissemination. Such

patterns indicate how state weakness and institutional voids create opportunities for extremist expansion. These findings align with Bala & Tar (2021), Makosso & Political (2021), and Okunade et al. (2021), who argue that regional affiliates flourish in governance gaps and under conditions of limited security cooperation.

Another important finding concerns the growing prevalence of lone-actor ecosystems and self-radicalized individuals driven by decentralized ideological narratives. Multiple respondents suggested that ISIS no longer requires formal membership structures to inspire violence because digital propaganda and symbolic messaging can motivate attacks without direct organizational involvement. This trend illustrates the transferability of extremist ideology beyond formal organizational boundaries, making extremist threats more difficult to identify and counter. The findings are consistent with Bou Nassif (2021), Metodieva (2023), and Morris (2024), who emphasize the increasing importance of self-radicalization and decentralized mobilization in contemporary terrorism.

In conclusion, the evolution of ISIS affiliates demonstrates that contemporary extremism is increasingly adaptive, interconnected, and multidimensional. Traditional top-down approaches to understanding terrorism are therefore insufficient for explaining the fluid and dynamic character of extremist movements operating across both physical and digital domains.

The accompanying Table 5 summarizes the major transformation patterns identified through cross-case analysis of interview data and secondary literature, illustrating how regional affiliates have adapted organizationally, ideologically, and operationally within different governance environments.

Table 5. Transformation Characteristics of ISIS Regional Affiliates

Regional Affiliate	Main Characteristics	Governance Vulnerability Exploited	Operational Adaptation
ISIS-K	Hybrid insurgent-extremist model	Border fragility and political instability	Cross-border recruitment and covert operations
ISCAP	Decentralized militant network	Weak regional governance	Localized insurgency and resource mobility
Boko Haram factions	Fragmented extremist alliances	Institutional weakness and social marginalization	Flexible territorial and ideological adaptation
Abu Sayyaf-linked actors	Maritime and regional mobility	Weak maritime governance	Kidnapping, digital propaganda, and local alliances
Lone actor ecosystems	Self-radicalized networks	Digital governance gaps	Independent attacks inspired online

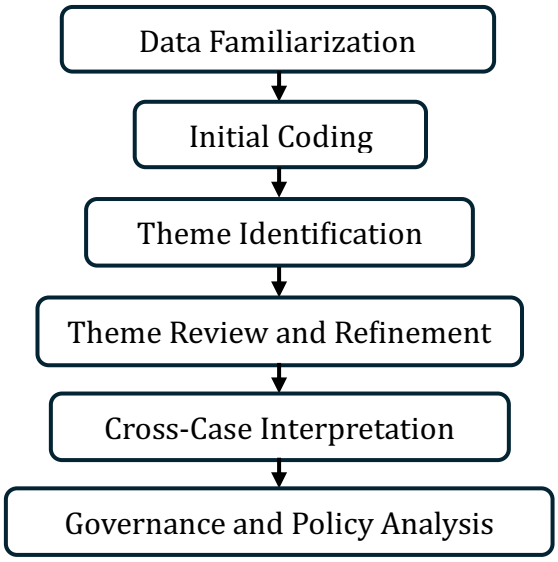
Source: Author's thematic analysis based on interviews with 15 informants and literature synthesis (2026)

Table 5 confirms that extremist organizations strategically adapt to governance vulnerabilities across different geographical contexts. This finding strengthens arguments for shifting counterterrorism policies beyond conventional military frameworks toward adaptive governance approaches capable of addressing complex and evolving threats.

The broader implications of these findings suggest that contemporary violent extremism requires more flexible institutional responses. Effective governance strategies must integrate international collaboration, stronger institutional coordination, and transparent national accountability in security management. The transformation of ISIS into an increasingly decentralized transnational movement illustrates how extremist networks exploit governance weaknesses, limited institutional capacity, and digital communication systems that transcend territorial boundaries.

The conceptual Figure 3 outlines the transformation of ISIS from a territorially based organization into a decentralized transnational extremist network. The figure indicates that the loss of territorial control does not necessarily reduce the operational effectiveness of extremist groups. Instead, the evidence suggests that decentralized, network-based, and governance-evasive structures may enhance resilience and make extremist organizations more difficult to defeat.

Figure 3. Transformation of Post-Caliphate Extremism



Source: Developed by the author based on thematic findings (2026)

The development of ISIS affiliates provides an important example of how digital technologies strengthen the resilience and survival of extremist ecosystems. The findings indicate that digitalization and cyber-enabled extremism have become central mechanisms of contemporary transnational extremism. At the same time, the reviewer's observation highlights the need for deeper theoretical engagement by moving beyond descriptive confirmation of previous studies toward broader conceptual contributions. Future discussion should further explore how these findings reshape understandings of governance and terrorism, what new theoretical implications emerge from adaptive governance perspectives, and how such approaches contribute to the advancement of security governance scholarship.

Digitalisation and the Emergence of Networked Extremism

These results confirm how digitalisation has reshaped the organisational logic and current modus operandi of extremist ecosystems. Among other notable trends, all interviewees reported that the loss of territorial control has pushed ISIS and its affiliates toward an increasing use of digital infrastructures (including social media platforms, encrypted applications, online forums and cryptocurrency systems) to ensure organizational continuity (Centre for Global Policy 2020). Older studies have shown how digital technologies are replacing the role of the dark web in extremism (Borelli, 2023; Lee et al., 2021; Sullivan, 2025), yet the interview data illustrate a wider transformation from territorial organizations toward digitally mediated governance ecosystems that reach beyond borders.

Many respondents concluded that extremist groups are no longer reliant on high-level coordination. Rather, they rely on decentralized communication networks through digital technologies. The way that they exert their power is becoming less about true read-only territory, but more interconnectivity. The researchers found that social media platforms were major pieces of infrastructure for the transmission and consumption of ideology, recruitment, and network maintenance. By supporting longer-term ideological contacts and the management of decentralized extremist communities, informants said that algorithmic systems raise governance issues as well as communicative concerns (Hodge, 2022; Hutchinson et al., 2023; Said et al., 2026).

Interviewees additionally elaborated that when extremist actors lose leaders or territory, their digital platforms often permit them to remain powerful. Digital ecosystems have emerged as the social spaces of our time, places where legitimacy, identity and collective action are being (re)produced continuously. Participants also noticed the growing melding of encrypted messaging apps and cryptocurrency systems. These technologies could be started for recruitment process and, communication within the organisation, resource mobilization, support financial transfer in the world of dynamics (where speedy delivery is major aspect of organisational development),

irrigation sectors [implementing weather forecasting model] or resilience framework(measuring climate change risk). Finally, participants highlighted that the true utility of cryptocurrency is not only within anonymity, but as part of a larger digital ecosystem (Anil & Babatope, 2024; Gbadebo, 2025; Rajola et al., 2025).

This is a significant empirical finding as it shows that extremist adaptation is increasingly governed by interdependencies across integrated digital technologies. Instead of being separate digital tools, governance challenges arise from interconnected systems.

Another key finding relates to the evolving nature of ideology in the digital extremist ecosystems. Respondents noted that ISIS affiliates appear to favour preserving ideological continuity in cyberspace as opposed to territorial conquest. These virtual spaces providing for self-radicalisation and engraining collective identities, maintaining transnational narratives of extremism without any need for direct organisational engagement. This further develops previous research on cyber-propaganda in demonstrating that the federated digital community operates as a governing space, continuously reactivating extremist norms, values and identities (Borelli, 2023; Sullivan, 2025; Viana & da Silva, 2021).

Consequently, such findings are cumulatively important to governance scholarship as they reveal how digital extremism functions under adaptive and networked environments that defy state-centric patterns of security response. Respondents highlighted this point from perspectives of collaborative governance and adaptive governance, describing that not a single institution has the comprehensive authority nor capacity to govern evangelical extremist ecosystems dispersed digitally. Because governance is continuous, it requires adjustments to regulatory systems, technological capacities and coordination mechanisms. Digital extremism should therefore be viewed not merely as a security response but rather governance challenge that demands dynamic institutional change.

Several digital tools were identified through the thematic analysis that both support extremist activity and create governance challenges. They are in turn summarized in Table 6 which draws out the main tools and their effects.

Table 6. Digital Instruments Used within Contemporary Extremist Ecosystems

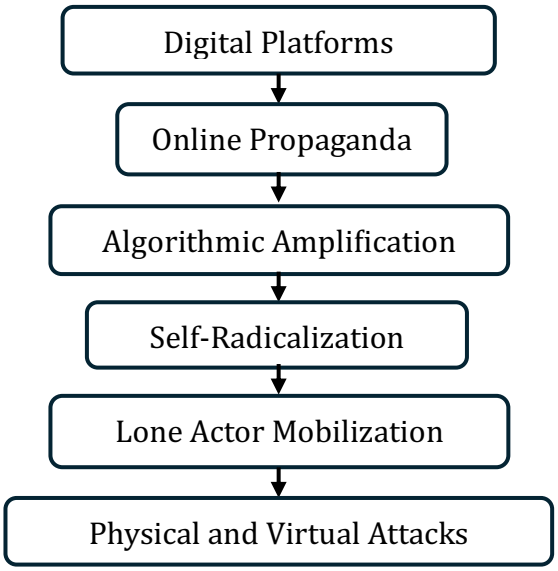
Digital Instrument	Extremist Function	Governance Challenge
Social media platforms	Recruitment and propaganda	Weak platform regulation
Encrypted applications	Covert communication	Surveillance limitations
Cryptocurrency systems	Financial transfers	Regulatory and monitoring gaps
Online forums	Ideological dissemination	Cross-border jurisdiction problems
Algorithmic recommendation systems	Radicalization amplification	Digital governance complexity

Source: Author's thematic coding from interview findings (2026).

As Table 6 indicates, extremist adaptation is more reliant on the merging of several digital technologies than on a single platform, thus necessitating transnational cyber-governance architectures. The results also show that digital extremism operates as an integrated ecosystem where recruitment, communications, funding and ideology reinforce each other in a continuous cycle.

Displaying the trans-national nature of digital extremism, Figure 4 conceptualizes inter-territorial governance spaces. This is consistent with what we have learned about the need for adaptive governance, collaborative institutional coordination, cross-sector cooperation and continuous policy learning to address decentralized extremist threats. As a result, digital extremism should be reformulated as a governance challenge with institutionalized improvement requiring long-term institutional improvisation, joint responses, integrated decision-making, and simultaneous policy learning.

Figure 4. Digital Extremism Ecosystem



Source: Developed by the author based on thematic findings (2026).

Collaborative Security Governance and Multi-Actor Responses

The results reveal that state-centric security solutions can by no means deal with current-day transnational extremism. The increasing importance of governments, regional organizations, telecommunications companies, civil society organizations, academic institutions and local communities in counter-extremism efforts was highlighted consistently by respondents. But the challenges only grow because actors need to cooperate but have different mandates, priorities and accountability structures. This contribution to governance literature demonstrates that collaborative security governance does not automatically follow from shared values, but rather arises through a dialectic process of bargaining among actors with counterposed interests (Barker Scott & Manning, 2024; Bonsoms, 2025; Subagyo, 2021). In keeping with the theory of collaborative governance (Ansell & Gash, 2008; Emerson et al., 2012).

One major theme that came out in the interviews relates to difficulties connected with sharing intelligence between jurisdictions. Participants did recognize intelligence exchange as critical to countering transnational extremist networks, but also noted sovereignty concerns, political mistrust, legal discrepancies/political considerations and institutional competition.

Due in large part to the legacy practice of verticalize where agencies prioritize their own organizational interests over collective security goals, information sharing is fragmented and slowness is a cyclical common response. Thus, the following wonders express that governance failures originate not just from the lack of cooperative mechanisms but also tensions between institutions and poor inter-organizational relationships (Bala & Tar, 2021; D'Amato, 2021; Wanderi et al., 2022). As such, effective governance is a function of trust and institutional capacity to handle conflict and uncertainty.

They also shed light on public-private tensions of cooperation in digital governance. Representatives from all groupings concurred that growing reliance on technology firms to identify extremist content and assist security agencies with cybersecurity was also having an effect on human rights. At the same time, governance dilemmas periodically arise from disagreements about data privacy, liability, platform regulation, and information disclosure. The need for technology companies to respond to attractive security demands may be in conflict with the business interests they must satisfy and this results in substantial hurdles to operational cooperation. These results reinforce studies that found governance of digital security is more about bargaining and contestation than it is about cooperation (Huang et al., 2022; Melaku, 2023; Savaş & Karataş, 2022). As a result, it is imperative to build adaptive governance mechanisms that align governance and market priorities.

An ensured correlation between community resilience and institutional governance is an equally significant finding. Respondents found that regional prevention efforts yielded considerable support but warned that local actors are typically on the backbenches of political decision-making, which is occupied mostly by national governments and security agencies. Consequently, a top–down approach of making decisions could interfere with trust and interventions since local actions may not be reached or targeted to the thought audience. These findings imply that where power is concentrated in formal institutions, collaborative governance remains underdeveloped. Thus, true stakeholder inclusion must entail a meaningful process that recognizes the need for true engagement and swap of power instead of just

symbolic involvement (Ansell & Gash, 2008; Emerson et al., 2012; Kolade, 2024; Shepherd, 2022; Subagyo, 2021).

The study also highlighted a governance paradox regarding penta-helix cooperation among government, academia, industry, community and media actors. In fact, forcing broad participation to tackle complex extremist threats comes with the potential for procurement costs in terms of coordination and/or competing mandates that may create policy mismatches. Diversity can pose challenges to joint action, but at the same time, also drives innovation and policy learning. Implications This finding contributes to the theory of collaborative governance by revealing that participation is insufficient and effectiveness, even in collaboration, also relies on managing institutional complexity. It is also why adapting governance has to be done, because the mechanisms for coordination must be remade and adapted continuously to meet evolving threats and constraints.

The findings are in line with perspectives of adaptive governance; demonstrating that, as security environments change faster than institutions do, a degree of institutional resilience relies on the capacity through which institutions learn and adapt. Flexibility in policy, responsiveness in technology, and iterative learning were imperative takeaways—as relayed by participants—in addressing such threats posed by digitally mediated extremism. These results fit with the adaptive governance literature highlighting flexible institutions and adaptive management principles such as continuous learning and multi-scaled collaboration in uncertain settings (Chaffin et al., 2014; Folke et al., 2005).

The results contribute to security governance literature theoretically by showing the compliments of collaborative action and adaptive governance. Collaborative governance explains the organization and mobilization of diverse actors, while adaptive governance helps explain how these kinds of actors change institutional arrangements, policies, and coordination mechanisms as threats are blown off course. Interviews make us sense that resilience arises from the capacity of group members to adapt and thrive with

each other, not just because of cooperation. Thematic analysis revealed a range of governance actors and their contributions to collaborative counter-extremism frameworks (Table 7).

Table 7. Collaborative Governance Actors in Counter-Extremism Responses

Governance Actor	Main Role	Strategic Contribution
Government institutions	Policy formulation and law enforcement	National coordination
Regional organizations	Intelligence and border coordination	Regional integration
Technology companies	Platform regulation and monitoring	Digital governance
Civil society organizations	Community resilience and prevention	Social trust building
Academic institutions	Research and policy recommendations	Evidence-based governance
Local communities	Early detection and social prevention	Grassroots resilience

Source: Author's synthesis based on interview findings and governance literature (2026)

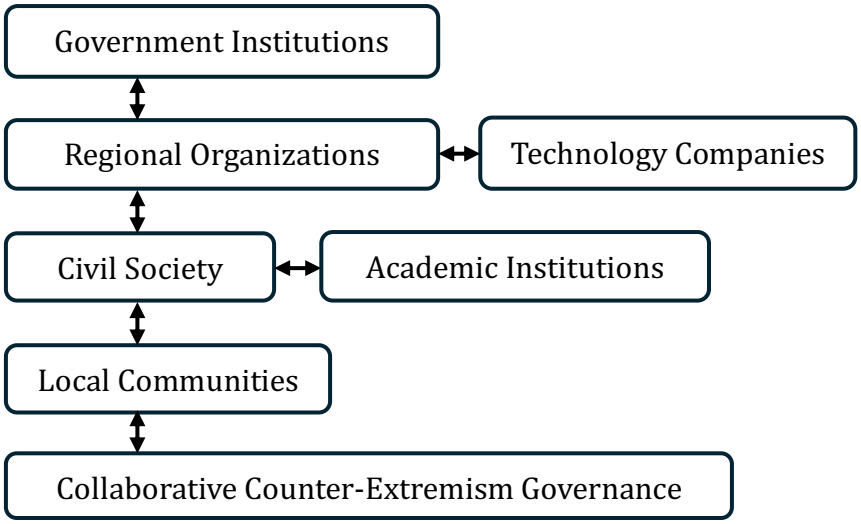
Governance Actor Main role Strategic Contribution Government institutions Policy formulation and law enforcement National coordination Regional organizations Intelligence and border coordination Regional integration Technology companies Platform regulation and monitoring Digital governance Civil society organizations Community resilience and prevention Social trust building Academic institutions Research and policy recommendations Evidence-based governance Local communities Early detection and social prevention Grassroots resilience

It reflects the fact that counter-extremism governance is increasingly dependent on interdependence across sectors and jurisdictions, underscoring the necessity for adaptive coordination mechanisms that can manage competing priorities and shifting security contexts.

Figure 5 sheds light on collaborative security governance as a dynamic process of multiple actors engaged throughout the different layers of authority. Because uncertainty, institutional fragmentation, and competing interests require capacity for adaptive governance (Patterson et al., 2004).

Instead of certainty derived from top-down control, good governance emerges as a slow but steady process whereby interdependent actors coordinate, negotiate and recalibrate. Thus, successful responses to transnational extremism will not only demand more cooperation: it will require substantial institutional capacity for managing conflict, bargaining and adapting continually to a rapidly changing security environment.

Figure 5. Collaborative Security Governance Framework



Source: Developed by the author based on thematic analysis (2026)

Policy Fragmentation and Governance Constraints

The analysis shows that it is not merely a case of administrative inadequacy but also a structural state of affliction that undermines global counter-extremism policy governance. Staying within formal silos whereby agencies operate with separate mandates, procedures and information systems even in counter-terrorism initiatives were legitimately flagged by almost every participant. These arrangements do not result in joint but layered responses, with competing authorities able to delay and fail to implement effective measures. Fragmentation manifests itself as weak institutional integration and limited stakeholder participation, which in turn leads to decreased efficacy by governments in responding to the particular nature of evolving extremist threats (D'Amato, 2021; Magnusson et al., 2025).

Interview data also suggests that extremist networks have been taking advantage of the space between states—which operate in a territorial basis—and transnational threats ever more so. Extremist actors operate in near real time exchanging information, resources and operational strategies across borders; government burdened by bureaucratic processes and jurisdictional boundaries. Such an incoherence between governance systems and the operational imperatives of transnational extremism are contributory to failures in counter-extremism. These findings support the scholarship on adaptive governance that emphasize continuous institutional adaptation under uncertainty (Chaffin et al., 2014; Folke et al., 2005; Huang et al., 2022; Savaş & Karataş, 2022).

The other significant takeaway relates to regional differences with respect to capacity of institutions. Participants from conflict-affected and developing countries also cited the lack of skilled personnel, ineffective legal systems, pervasive corruption and administrative instability as impediments. These limitations combine with institutional fragmentation, resulting in cumulative governance gaps. Such conditions make it difficult for fragmented institutions to coordinate preventive action, leaving behind vacuums that extremist actors can fill with recruitment, financing and local activity. These results further emphasize that institutional resilience relies on organizational capacity and intersectoral coordination as well (Baldaro & D'Amato, 2024; Chaffin et al., 2014; Folke et al., 2005; Makosso & Political, 2021).

Finally, a related but different problem is the existence of fragmented legal and regulatory regimes across jurisdictions. According to some participants, differences in intelligence-sharing standards, surveillance regulations and financial-monitoring systems often prevent rapid collective responses to transnational threats. Interviews indicate that failures of governance arise less from lack of political will and more from institutional disjuncture. As Bonsoms (2025), Rajola et al. (2025), and Uzougbo et al. (2024). to integrate information flows and ad-hoc cooperation between governments is hampered by fragmented regulations and indirectly contributes to boosting the adaptability of extremists (Emerson et al., 2012).

Survey respondents went on to confirm that excessive reliance on hard-security measures has a backlash, etc. Military interventions can quell immediate threats to civilians from terrorism but do not address the social exclusion, identity-based grievances and local conditions connected with radicalization. Reactive security policies then address symptoms, not root causes. This interplay erodes community confidence, dissuades civic engagement, and hampers proactive resiliency. The results bolster resilience-governance perspectives idealizing collaborative and co-creative engagement that can tackle structural root causes of extremisms (Ansell & Gash, 2008; Kolade, 2024; Melaku, 2023; Shepherd, 2022).

Theoretically, the study argues that fragmentation needs to be seen as a governance process rather than an institutional condition. As extremist networks Speed, Flexibility and Transnationalism surpass their coordination mechanisms, it refers basically to the inability of institutions to adapt to these changes (Governance failure). Between these two approaches, collaborative governance predominantly focuses on participation and consensus-building among actors while adaptive governance specifies how institutions transform governance arrangements to meet challenges when existing collaborative structures are no longer sufficient. Thus, the resilience of governance is rooted not merely in collaboration but also on the ability to iteratively adapt collaborative arrangements to changing threat environments (Ansell & Gash, 2008; Chaffin et al., 2014; Emerson et al., 2012; Folke et al., 2005).

Table 8. Major Governance Limitations Identified in the Study

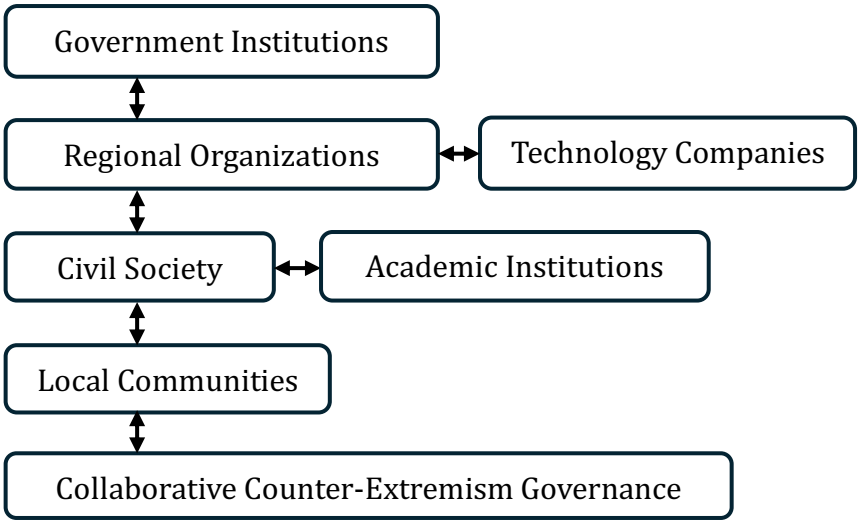
Governance Limitation	Main Impact
Institutional silo governance	Weak coordination and duplication
Cross-border legal fragmentation	Delayed collaborative responses
Weak cybersecurity governance	Digital exploitation by extremists
Limited state capacity	Governance vulnerability
Reactive policy orientation	Low policy adaptability
Weak community engagement	Reduced preventive resilience

Source: Author's thematic interpretation based on interview findings (2026).

The table shows that governance constraints are interlinked, not separate. Links among vulnerabilities in discrete governance domains suggest

that an integrated and flexible system necessary to respond effectively to complex, cross-sectoral challenges (Chaffin et al., 2014; Folke et al., 2005); thereby supporting adaptive governance arguments.

Figure 6. Governance Fragmentation in Counter-Extremism Policy



Source: Developed by the author based on thematic findings (2026)

Fragmentation leads to a series of inter-organizational consequences, characterized by weak linkages between organizations, poor flow of information, unevenness in policy implementation and diminishing administrative flexibility (see figure 6). Fragmentation then can block many pathways of successful counter-extremism results. The results suggest that just increasing collaboration environment is not enough. Governance that works Calls for reduced fragmentation and synergies through harmonizing regulatory regimes strengthens institutional learning, continuing adaptive evolution of collaborative structures to respond in real-time to the changing idioms through which extremist threats emerge. These results lay the groundwork for the subsequent explorations of policy implications and recommendations for adaptive security governance.

Policy Insights for Adaptive Security Governance

The results suggest that contemporary transnational extremism poses challenges to many assumptions which have been built into more traditional

security governance. Respondents highlighted how extremist networks function through porous assemblages of media technologies, far-flung ties and distributed organizational modalities. These networks are not traditional security threats that operate in isolation, but rather continuously evolve along with technology and geopolitical climates. Therefore, effective governance does not only come down to capacity to coordinate but also the ability of the institutions to adapt governance frameworks, policy tools and decision-making processes in uncertain conditions. This result strengthens resilience-based governance approaches focusing on both institutional adaptability and learning in dynamic contexts (Folke et al., 2005; Melaku, 2023; Rajola et al., 2025).

The distinction between collaborative governance and adaptive governance in an important theoretical implication of our analysis of the interviews. They acknowledged that without a responsive governance system, rapid evolution of peril is beyond the scope of collaboration. Collaborative mechanisms address the need to engage stakeholders and promote coordination, but they will prove less useful as extremist actors dynamically change their current tactics, technologies and communication patterns. Adaptive governance thus goes beyond collaboration, but rather highlights institutional learning, flexibility, experimentation and the ongoing restructuring of governance arrangements (Pahl-Wostl, 2009). From this perspective, adaptive governance is an important complement to collaborative governance in that it strengthens institutional response-ability for when there are less clear circumstances (Ansell & Gash, 2008; Emerson et al., 2012; Folke et al., 2005).

The interviews also evidenced the context-specific nature of governance adaptation. Governance responses cut across variations in state capacity, technological infrastructure, legal systems, social resilience and geopolitical conditions. As a consequence, practical governance models are not universally applicable. Support for Findings-These findings challenge universal policy prescriptions and are consistent with a contextual approach to understanding the effectiveness of governance approaches. Hence, adaptive

governance should be regarded as a relational process whereby institutions continuously adjust their arrangements to the evolving state of environmental changes (Adesokan-Imran, 2025; Anil & Babatope, 2024; Chaffin et al., 2014).

One significant area relates to digitisation governance and security governance. For the most part, respondents stressed that we must no longer view digital infrastructures as spaces where extremism happens but instead as core constituents of the extremist ecosystem. They enable the transmission of ideas across borders, provide channels for communication, recruitment and logistical coordination. As a result, the effectiveness of governance increasingly depends on enlarging the scope of security-governance frameworks to include cybersecurity governance, information governance, and technological regulation. This finding pushes the agenda of technological adaptation as a leading governance question, rather than a marginal policy topic (Folke et al., 2005; Rajola et al., 2025; Savaş & Karataş, 2022; Zhong et al., 2024).

The results also show that community resilience acts as a governing resource and not only a social outcome. According to respondents, trust, civic engagement, and local-level involvement all directly bolster the ability of governance systems to prevent, absorb, and respond to extreme threats. Strengthening legitimacy, improving information flows and bolstering preventive capabilities make community resilience a vital component of effective governance. This contributes to resilience-governance frameworks, illustrating support from social resilience for institutional adaptability and policy responsiveness (Ansell & Gash, 2008; Emerson et al., 2012; Kolade, 2024; Subagyo, 2021; Sullivan, 2025).

In terms of broader governance, adaptive security governance needs to be understood as a kind of dynamic system: it is iterative; institutional experimentation (institutional arrangements adapted in the particular context) occur within it and coordination across multiple levels occurs flexibly. Adaptive governance contrasts with classical security models that relied mainly on top-down control and centralization of authority, focusing

instead on continual adaptation to new challenges delivered through problem-solving partnerships. Such interpretation is consistent with some scholarship on adaptive governance that regards adaptability as a property of resilient governance systems (Chaffin et al., 2014; Folke et al., 2005).

Importantly, the diagnostics identified seven dimensions of governance that illustrate how institutions respond and adapt in the face of extremist threats. They cover one or more of six dimensions: digital governance, institutional coordination, regional cooperation, cybersecurity governance, community resilience and adaptive policy systems.

Table 9. Policy Recommendations for Adaptive Security Governance

Policy Area	Recommended Strategy
Digital governance	Strengthen cyber monitoring and platform regulation
Regional cooperation	Enhance intelligence-sharing mechanisms
Community resilience	Expand preventive deradicalization programs
Institutional coordination	Develop integrated governance platforms
Cybersecurity governance	Improve public-private digital collaboration
Adaptive policy systems	Apply risk-based and flexible governance models

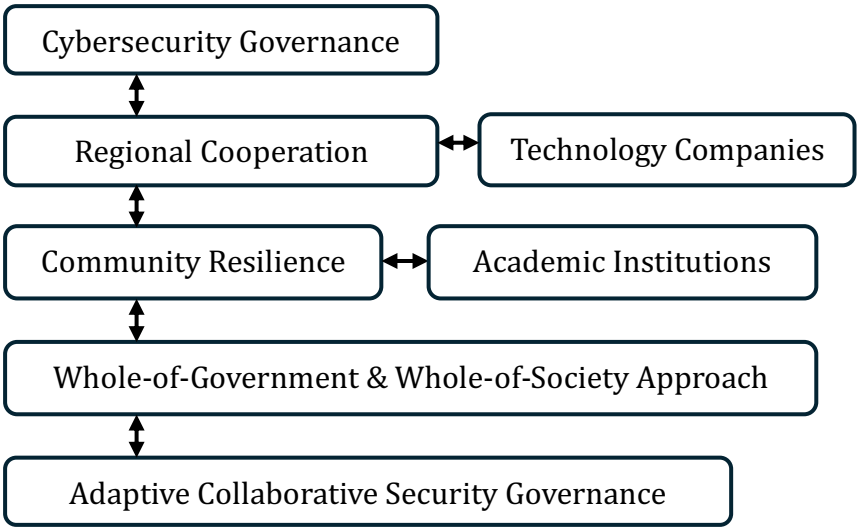
Source: Author's policy synthesis based on thematic findings (2026).

In sum, as conveyed by Table 9, actions include to bolster cyber monitoring and platform regulation; enhance intelligence-sharing mechanisms; strengthen preventive deradicalization programs; develop integrated whole-of-society governance platforms; improve public-private digital cooperation in the new hybrid threat landscape; and embrace risk-based flexible governance models. Note: Policy synthesis based on thematic findings (2026).

Results also show that adaptive governance functions through interactions of institutional, technology, terrain and social factor. Collaborative governance, as in the case of participatory budgeting (Figure 7: Adaptive Collaborative Security Governance Model), enables actor engagement and coordination, while adaptive governance ensures continuous

adjustment of institutions in response to emerging threats through iterative processes.

Figure 7. Adaptive Collaborative Security Governance Model



Source: Developed by the author based on thematic synthesis (2026).

Overall, the governance of ISIS regional affiliates and other transnational extremist networks must be shifted away from Individual trajectories. What it offers is a framework of adaptive security governance based in institutional learning, contextual responsiveness around technological adaptation resulting in dynamic coordination. Resilient governance for countering extremism thus requires communication between sectors, but also a pliable system of governance that identifies and re-aligns itself to engage with this evolving behaviour of extremists within the changing cyberspace and security environment.

CONCLUSION

The results of this study highlight a significant transition within ISIS in the post-caliphate era from an organization with a large territorial footprint to an increasingly decentralized, agile and digitally networked global terrorist network. Based on interviews with fifteen foreign fighters, the findings suggest that while ISIS's loss of territorial control in Iraq and Syria did not eradicate its ability to conduct operations, it instead prompted a proliferation of regional

subsidiaries, clandestine organizational networks, and digitally enabled radical activities. The instances of ISIS-K, ISCAP, factions of Boko Haram, and other affiliated actors illustrate the ways tech-savvy extremist networks fit the governance gaps, political uncertainties, and advancements in technology from region to region. Digital platforms, encrypted communication, online propaganda and alternative finance mechanisms have not only reinforced the resilience of extremist ecosystems but also made governance decisions more complex compared to pre-2010. Taken together, these findings suggest that the nature of contemporary extremism is more networked and cross-border --and flexible in operations-- than earlier generations of state-centric counter-terrorism approaches were able to deal with.

The results also suggest that collaborative security governance serves as an important analytical framework through which governments, regional organizations, technology companies and civil society actors, academics and local communities navigate shifting extremism threats. Instead of framing extremism purely as a defence or law-enforcement issue, the report emphasises that addressing modern security threats requires coordination across institutions (and between public and private actors), digital governance, sharing of information and building community resilience. The interviews have nevertheless disclosed how often the effectiveness of counter-extremism responses are constrained by fragmented governance, legal inconsistencies, weak cybersecurity arrangements and uneven institutional capacities. In this sense, the paper does not formulate a theory of adaptive security governance but rather provides evidence to support the notion that co-management approaches, involving collaborative (working with links) as well as strategic (fostering interdependence) interactional processes, may be proximate ways of framing complex transnational security problems. As such, the main contribution of the study therefore lies in showing how theory evolved concepts could help explain changes in manifestations of digital and transnational extremism in various geographic areas.

These findings should be interpreted with several limitations working. We use a qualitative synthesis based on fifteen informants and selected regional cases, meaning one should avoid overgeneralising to all forms of

transnational extremism or all geopolitical environments. Additionally, although the reflexive thematic analysis provides detailed descriptions of governance dynamics and institutional responses, it does not establish causal relationships between governance arrangements and counter-extremism outcomes. Future studies may make these findings more robust via mixed-methods approaches, larger comparative datasets, and longitudinal research into the long-term interplay among digital technologies, governance adaptation perspectives, and the evolution of extremist movements. These sorts of pulls in between qualitative and quantitative approaches will add to our understanding of how collaborative and adaptive governance mechanics function in a progressively confusing security situation where technology plays a main role.

ACKNOWLEDGMENT

The authors wish to thank Universitas Pertahanan Republik Indonesia (UNHAN RI) for its institutional support of this research. They also gratefully acknowledge the valuable contributions and insights from partners in collaborating countries and all international informants who participated. Their support, viewpoints, and willingness to share information greatly enhanced the quality and depth of the study.

REFERENCES

Adesokan-Imran, T. O. (2025). The Impact of Cybersecurity Governance on National Security by Strengthening Critical Infrastructure through IT Auditing and Risk Management. *Asian Journal of Research in Computer Science*, *18*(4), 301–322. https://doi.org/10.9734/ajrcos/2025/v18i4621

Adigwe, C. S., Mayeke, N. R., Olabanji, S. O., Okunleye, O. J., Joeaneke, P. C., & Olaniyi, O. O. (2024). The Evolution of Terrorism in the Digital Age: Investigating the Adaptation of Terrorist Groups to Cyber Technologies for Recruitment, Propaganda, and Cyberattacks. *Asian Journal of Economics, Business and Accounting*, *24*(3), 289–306. https://doi.org/10.9734/ajeba/2024/v24i31287

Anil, V. K. S., & Babatope, A. B. (2024). The role of data governance in enhancing cybersecurity resilience for global enterprises. *World Journal of Advanced Research and Reviews*, *24*(1), 1420–1432. https://doi.org/10.30574/wjarr.2024.24.1.3171

Annamalah, S. (2024). The Value of Case Study Research in Practice: A Methodological Review with Practical Insights from Organisational Studies. *Journal of Applied Economic Sciences (JAES)*, *19*(4 (86)), 485–498. https://doi.org/10.57017/jaes.v19.4(86).11

Ansell, C., & Gash, A. (2008). Collaborative Governance in Theory and Practice. *Journal of Public Administration Research and Theory*, *18*(4), 543–571. https://doi.org/10.1093/JOPART/MUM032

Bala, B., & Tar, U. A. (2021). Regional Cooperation in West Africa: Counter-Terrorism and Counter-Insurgency. *African Security*, *14*(2), 186–207. https://doi.org/10.1080/19392206.2021.1929747

Baldaro, E., & D'Amato, S. (2024). Transnational counterterrorism assemblages: the case of preventing and countering violent extremism in Mali. *Territory, Politics, Governance*, *12*(4), 519–536. https://doi.org/10.1080/21622671.2023.2268651

Barker Scott, B. A., & Manning, M. R. (2024). Designing the Collaborative Organization: A Framework for how Collaborative Work, Relationships, and Behaviors Generate Collaborative Capacity. *The Journal of Applied Behavioral Science*, *60*(1), 149–193. https://doi.org/10.1177/00218863221106245

Baxter, P., & Jack, S. (2008). Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers. In *The Qualitative Report* (Vol. 13). http://www.nova.edu/ssss/QR/QR13-4/baxter.pdf

Bonsoms, A. (2025). Power, governance, and coordination in the prevention of violent extremism and terrorism: towards multi-agency counterterrorism? *European Security*, *34*(3), 456–474. https://doi.org/10.1080/09662839.2025.2449866

Borelli, M. (2023). Social media corporations as actors of counter-terrorism. *New Media & Society*, *25*(11), 2877–2897. https://doi.org/10.1177/14614448211035121

Bou Nassif, H. (2021). Rethinking Pathways of Transnational Jihad: Evidence from Lebanese ISIS Recruits. *Security Studies*, *30*(5), 797–822. https://doi.org/10.1080/09636412.2021.2010888

Braun, V., & Clarke, V. (2022). Conceptual and design thinking for thematic analysis. *Qualitative Psychology*, *9*(1), 3–26. https://doi.org/10.1037/qup0000196

Braun, V., & Clarke, V. (2023). Is thematic analysis used well in health psychology? A critical review of published research, with recommendations for quality practice and reporting. *Health Psychology Review*, *17*(4), 695–718. https://doi.org/10.1080/17437199.2022.2161594

Braun, V., & Clarke, V. (2024). Supporting best practice in reflexive thematic analysis reporting in Palliative Medicine: A review of published research and introduction to the Reflexive Thematic Analysis Reporting

Guidelines (RTARG). *Palliative Medicine*, *38*(6), 608–616. https://doi.org/10.1177/02692163241234800

Calléja, L. (2021). Transnational terrorism: a threat to global security. *JANUS NET E-Journal of International Relation*, *1*(12), 1–12. https://doi.org/10.26619/1647-7251.12.1.1

Campbell, K. A., Orr, E., Durepos, P., Nguyen, L., Li, L., Whitmore, C., Gehrke, P., Graham, L., & Jack, S. M. (2021). Reflexive thematic analysis for applied qualitative health research. *Qualitative Report*, *26*(6), 2011–2028. https://doi.org/10.46743/2160-3715/2021.5010

Chaffin, B. C., Gosnell, H., & Cosens, B. A. (2014). A decade of adaptive governance scholarship: synthesis and future directions. *Ecology and Society*, *19*(3). https://doi.org/10.5751/ES-06824-190356

D'Amato, S. (2021). Patchwork of Counterterrorism: Analyzing European Types of Cooperation in Sahel. *International Studies Review*, *23*(4), 1518–1540. https://doi.org/10.1093/isr/viab024

Dusdal, J., & Powell, J. J. W. (2021). Benefits, Motivations, and Challenges of International Collaborative Research: A Sociology of Science Case Study. *Science and Public Policy*, *48*(2), 235–245. https://doi.org/10.1093/scipol/scab010

Emerson, K., Nabatchi, T., & Balogh, S. (2012). An Integrative Framework for Collaborative Governance. *Journal of Public Administration Research and Theory*, *22*(1), 1–29. https://doi.org/10.1093/JOPART/MUR011

Folke, C., Hahn, T., Olsson, P., & Norberg, J. (2005). Adaptive governance of social-ecological systems. *Annual Review of Environment and Resources*, *30*(Volume 30, 2005), 441–473. https://doi.org/10.1146/ANNUREV.ENERGY.30.050504.144511/CITE/REFWORKS

Gbadebo, M. O. (2025). Terrorism and global security: Cyber threats, governance, and counterterrorism strategies. *International Journal of Applied Research in Social Sciences*, *7*(3), 227–251. https://doi.org/10.51594/ijarss.v7i3.1863

Hodge, E. (2022). Online Networks of Hate: Cultural Borders in Aterritorial Spaces. *Borders in Globalization Review*, *4*(1), 79–82. https://doi.org/10.18357/bigr41202221162

Huang, K., Madnick, S., Zhang, F., & Siegel, M. (2022). Varieties of public–private co-governance on cybersecurity within the digital trade: implications from Huawei's 5G. *Journal of Chinese Governance*, *7*(1), 81–110. https://doi.org/10.1080/23812346.2021.1923230

Hutchinson, J., Amarasingam, A., Scrivens, R., & Ballsun-Stanton, B. (2023). Mobilizing extremism online: comparing Australian and Canadian right-wing extremist groups on Facebook. *Behavioral Sciences of Terrorism and Political Aggression*, *15*(2), 215–245. https://doi.org/10.1080/19434472.2021.1903064

Jadoon, A., Jahanbani, N., & Fruchtman, E. (2023). The uninvited guest: understanding Islamic State's alliances and rivalries in the Afghanistan-Pakistan region. *Asian Security*, *19*(1), 59–81. https://doi.org/10.1080/14799855.2023.2173581

Janis, I. (2022). Strategies for Establishing Dependability between Two Qualitative Intrinsic Case Studies: A Reflexive Thematic Analysis. *Field Methods*, *34*(3), 240–255. https://doi.org/10.1177/1525822X211069636

Kidwai, S. A. (2022). Rivalry Between the Taliban and ISKP: The Collision of Terror. *India Quarterly*, *78*(4), 544–557. https://doi.org/10.1177/09749284221127791

Kolade, T. M. (2024). Promoting Peace, Justice, and Strong Institutions: A Comprehensive Approach to Counterterrorism for Global Security. *Asian Journal of Education and Social Studies*, *50*(12), 490–509. https://doi.org/10.9734/ajess/2024/v50i121717

Lee, C. S., Choi, K. S., Shandler, R., & Kayser, C. (2021). Mapping Global Cyberterror Networks: An Empirical Study of Al-Qaeda and ISIS Cyberterrorism Events. *Journal of Contemporary Criminal Justice*, *37*(3), 333–355. https://doi.org/10.1177/10439862211001606

Lincoln, Y., & Guba, E. G. (1985). The Disturbing and Disturbed Observer. *Naturalistic Inquiry*, 92–109, 357–367. https://books.google.com/books/about/Naturalistic_Inquiry.html?hl=id&id=2oA9aWlNeooC

Magnusson, L., Iqbal, S., Elm, P., & Dalipi, F. (2025). Information security governance in the public sector: investigations, approaches, measures, and trends. *International Journal of Information Security*, *24*(4), 177. https://doi.org/10.1007/s10207-025-01097-x

Makosso, A. M., & Political, M. A. (2021). ISLAMIC STATE CENTRAL AFRICA PROVINCE (ISCAP): A THREAT TO REGIONAL STABILITY AND SECURITY. *The Journal of Intelligence, Conflict, and Warfare*, *4*(1), 101–117. https://doi.org/https://doi.org/10.21810/jicw.v4i1.2825

Martini, A. (2024). Governing through the prevention of extremism. The Security Council's P/CVE as a *dispositif* of liberal government. *Cambridge Review of International Affairs*, *37*(6), 815–839. https://doi.org/10.1080/09557571.2024.2378385

Melaku, H. M. (2023). A Dynamic and Adaptive Cybersecurity Governance Framework. *Journal of Cybersecurity and Privacy*, *3*(3), 327–350. https://doi.org/10.3390/jcp3030017

Metodieva, A. (2023). The Radical Milieu and Radical Influencers of Bosnian Foreign Fighters. *Studies in Conflict & Terrorism*, *46*(9), 1725–1744. https://doi.org/10.1080/1057610X.2020.1868097

Morris, A. M. (2024). Who Becomes a Foreign Fighter? Characteristics of the Islamic State's Soldiers. *Terrorism and Political Violence*, *36*(2), 246–264. https://doi.org/10.1080/09546553.2022.2144730

Naeem, M., Ozuem, W., Howell, K., & Ranfagni, S. (2023). A Step-by-Step Process of Thematic Analysis to Develop a Conceptual Model in Qualitative Research. *International Journal of Qualitative Methods*, *22*. https://doi.org/10.1177/16094069231205789

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic Analysis. *International Journal of Qualitative Methods*, *16*, 1–13. https://doi.org/10.1177/1609406917733847

Okunade, S. K., Faluyi, O. T., & Matambo, E. (2021). Evolving patterns of insurgency in Southern and West Africa: Refocusing the Boko Haram lens on Mozambique. *African Security Review*, *30*(4), 434–450. https://doi.org/10.1080/10246029.2021.1959360

Pahl-Wostl, C. (2009). A conceptual framework for analysing adaptive capacity and multi-level learning processes in resource governance regimes. *Global Environmental Change*, *19*(3), 354–365. https://doi.org/10.1016/j.gloenvcha.2009.06.001

Patterson, M. G., West, M. A., & Wall, T. D. (2004). Integrated manufacturing, empowerment, and company performance. *Journal of Organizational Behavior*, *25*(5), 641–665. https://doi.org/10.1002/JOB.261

Patton, M. Q. (2015). *Qualitative Research & Evaluation Methods: Integrating Theory and Practice* (4th Edition). SAGE Publication, Inc. https://www.amazon.com/Qualitative-Research-Evaluation-Methods-Integrating/dp/1412972124

Rajola, F., Gatelli, P., & Iacopino, V. (2025). Governance Processes and Technologies for Cyber Resilience in the Financial Sector: The Italian Scenario. *Information Systems Journal*. https://doi.org/10.1111/ISJ.70023

Rashid, Y., Rashid, A., Warraich, M. A., Sabir, S. S., & Waseem, A. (2019). Case Study Method: A Step-by-Step Guide for Business Researchers. *International Journal of Qualitative Methods*, *18*, 1–13. https://doi.org/10.1177/1609406919862424

Said, F. M., Agola, F. O., & Oluteyo, G. A. (2026). Social media ecosystems and transnational radicalization outcomes in Kenya: A mixed-methods analysis of content, platforms, networks, and algorithms. *African Journal of Empirical Research*, *7*(1), 349–362. https://doi.org/10.51867/ajernet.7.1.30

Savaş, S., & Karataş, S. (2022). Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance. *International Cybersecurity Law Review*, *3*(1), 7–34. https://doi.org/10.1365/s43439-021-00045-4

Schlunegger, M. C., Zumstein-Shaha, M., & Palm, R. (2024). Methodologic and Data-Analysis Triangulation in Case Studies: A Scoping Review. In *Western Journal of Nursing Research* (Vol. 46, Number 8, pp. 611–622). SAGE Publications Inc. https://doi.org/10.1177/01939459241263011

Shepherd, L. J. (2022). White feminism and the governance of violent extremism. *Critical Studies on Terrorism*, *15*(3), 727–749. https://doi.org/10.1080/17539153.2022.2089401

Strunel, A. M., & Cordoba, S. (2025). Insider/outsider dynamics: a reflexive thematic analysis of reflexivity/positionality in the 'qualitative research in psychology' journal. *Qualitative Research in Psychology*, *22*(4), 887–917. https://doi.org/10.1080/14780887.2025.2505460

Subagyo, A. (2021). The implementation of the pentahelix model for the terrorism deradicalization program in Indonesia. *Cogent Social Sciences*, *7*(1). https://doi.org/10.1080/23311886.2021.1964720

Sullivan, G. (2025). Algorithmic governance of 'terrorism' and 'violent extremism' online. *London Review of International Law*, *13*(1), 47–75. https://doi.org/10.1093/lril/lraf005

Tasev, I. (2025). Islamic State Khorasan Province (ISK): An Imminent Threat for Central Asia and Beyond. *Bulgarian Journal of International Economics and Politics*, *5*(1), 53–72. https://doi.org/10.37075/BJIEP.2025.1.04

Topal, S. A. (2024). A Relational Theory of Jihadist Affiliate Behaviour: The Case of Al Qaeda and the Islamic State. *Civil Wars*, *26*(2), 274–299. https://doi.org/10.1080/13698249.2024.2314899

Tracy, S. J. (2013). *Qualitative Research Methods* (First). Wiley-Blackwell Publishing. www.wiley.com/go/tracy.

Uzougbo, N. S., Ikegwu, C. G., & Adewusi, A. O. (2024). Cybersecurity compliance in financial institutions: A comparative analysis of global standards and regulations. *International Journal of Science and Research Archive*, *12*(1), 533–548. https://doi.org/10.30574/ijsra.2024.12.1.0802

Viana, M. T., & da Silva, P. P. dos S. (2021). Preventing extremisms, taming dissidence: Islamic radicalism and black extremism in the U.S. making of CVE. *Critical Studies on Terrorism*, *14*(1), 24–46. https://doi.org/10.1080/17539153.2020.1870259

Viera, C. A. (2023). CASE STUDY AS A QUALITATIVE RESEARCH METHODOLOGY. *Performance Improvement*, *62*(4), 125–129. https://doi.org/10.56811/PFI-23-0005

Wanderi, S. M., Mwangi, S., & Wasonga, J. (2022). MAJOR ISSUES AND DILEMMAS IN INTELLIGENCE GATHERING AND SHARING AS A COUNTERTERRORISM STRATEGY. *Strategic Journal of Business &*

Change Management, *9*(1), 370–387. https://doi.org/10.61426/sjbcm.v9i1.2191

Yashlavskii, A. (2025). Terrorist Networks of the “Global Jihad” in the 2020s: New Forms, Locations and Challenges. *World Economy and International Relations*, *69*(2), 44–54. https://doi.org/10.20542/0131-2227-2025-69-2-44-54

Zhong, J., Wang, X., & Zhang, T. (2024). Network Security Governance Policy and Risk Management: Research on Challenges and Coping Strategies. *Journal of Machine and Computing*, *4*(1), 153–169. https://doi.org/10.53759/7669/JMC202404015