Wiener Beiträge zur Islamforschung

Ednan Aslan · Kamil Öktem *Editors*

When Faith Kills

Understanding Religious Extremism

Springer VS

Ednan Aslan · Kamil Öktem
Editors

When Faith Kills

Understanding Religious Extremism

Springer VS

Editors
Ednan Aslan
Institute for Islamic Theological Studies
University of Vienna
Vienna, Austria

Kamil Öktem
Institute for Islamic Theological Studies
University of Vienna
Vienna, Austria

ISSN 2570-222X ISSN 2570-2238 (electronic)
Wiener Beiträge zur Islamforschung
ISBN 978-3-658-50489-2 ISBN 978-3-658-50490-8 (eBook)
https://doi.org/10.1007/978-3-658-50490-8

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Fachmedien Wiesbaden GmbH, part of Springer Nature 2026

This work is subject to copyright. All rights are solely and exclusively licensed by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.
The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer VS imprint is published by the registered company Springer Fachmedien Wiesbaden GmbH, part of Springer Nature.
The registered company address is: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

If disposing of this product, please recycle the paper.

The Human Security Approach in Combating Cyber Terrorism: Perspective from ASEAN Member States

Miftahul Ulum, Tamara Nair, Jompon Pitaksantayothin, Bora Park, and Faby Izaura Y. Barus

Abstract

This paper explores how ASEAN member states are adopting a human security approach to combat cyber terrorism. Traditional cybersecurity—centered on infrastructure protection and technical solutions—proves insufficient against complex threats like online radicalization. The human security perspective reframes cyber terrorism as a social and human challenge, focusing on the protection of individuals and communities. Through a qualitative case study approach, drawing on literature, surveys, and focus groups with cybersecurity stakeholders, the research finds that although the human security concept is

M. Ulum (✉)
University of Muhammadiyah Jakarta, Jakarta, Indonesia
e-mail: miftahul.ulum@umj.ac.id

F. I. Y. Barus
ASEAN Institute for Peace and Reconciliation, Indonesia
e-mail: faby.barus@asean-aipr.org

T. Nair
Nanyang Technological University, Singapore, Singapore
e-mail: istnair@ntu.edu.sg

J. Pitaksantayothin
Hankuk University of Foreign Studies, Seoul, South Korea
e-mail: jompon.pit@hufs.ac.kr

B. Park
Institute for National Security Strategy, South Korea
e-mail: borapark@inss.re.kr

© The Author(s), under exclusive license to Springer Fachmedien Wiesbaden GmbH, part of Springer Nature 2026

E. Aslan and K. Öktem (eds.), *When Faith Kills*, Wiener Beiträge zur Islamforschung, https://doi.org/10.1007/978-3-658-50490-8_14

acknowledged, its policy integration remains limited. Technical measures still dominate, but emerging initiatives emphasize community-based prevention, trust-building, and inclusion. A major obstacle is the lack of trust in digital spaces. Human-centered strategies require individuals to feel safe online, yet this is undermined by cyber threats and harmful actors. Moreover, coordination between state and non-state actors is weak. Governments emphasize legal and technical responses, while civil society organizations focus on psychosocial support and community resilience. Nevertheless, opportunities for collaboration are emerging. Public–private partnerships and local interventions offer potential for aligning efforts and enhancing the impact of cyber terrorism prevention. A shift toward inclusive, sustainable security models may help address the underlying drivers of extremism and foster long-term resilience in ASEAN societies.

1 Introduction

In the rapidly evolving digital landscape, cyber threats have become a critical issue for states and societies alike. Among the most concerning of these threats is cyber terrorism, which involves the use of digital technologies to intimidate or coerce governments or societies for political, religious, or ideological objectives (Jarvis et al., 2014). Despite its increasing significance, the academic discourse on cyber terrorism remains limited, particularly within the realm of cyber security studies. Much of the existing literature frames cyber terrorism within the broader context of terrorism studies, often focusing on ideological and operational aspects (Ranstorp, 2007). This approach leaves a gap in understanding the unique cyber security challenges posed by cyber terrorism, especially in the ASEAN region, where human security principles could provide new insights (Emmers, 2013).

A notable real-world example of cyber terrorism is the WannaCry ransomware attack in 2017, which affected over 150 countries. The attack crippled critical infrastructure, including the UK's National Health Service (NHS), endangering lives by disrupting essential healthcare services (Greenberg, 2017). This incident illustrates the direct human security implications of cyber terrorism, demonstrating how cyber attacks can affect not only states but also individuals and communities. Similarly, the 2020 cyberattack on Singapore's health database, which compromised the personal data of 1.5 million citizens, highlights the broader societal impacts of such attacks. The theft of sensitive information undermined public trust in government institutions and exposed individuals to potential identity theft and other harms (SingCERT, 2020). These incidents underscore the

need to approach cyber terrorism from a cyber security perspective that prioritizes the protection of individuals and communities, particularly in ASEAN states where digital infrastructure is expanding but remains vulnerable (Choucri, 2012).

Understanding cyber terrorism through the lens of cyber security is essential because it addresses the technical and infrastructural dimensions of the threat. Cyber security studies emphasize the vulnerabilities in information systems, networks, and critical infrastructures that cyber terrorists often exploit, while terrorism studies focus on radicalization and operational tactics (Clarke & Knake, 2010). In the ASEAN region, where rapid digitalization is taking place, these vulnerabilities are increasingly significant. For instance, cyber terrorists could target vital infrastructures such as power grids or financial institutions, as seen in recent cyber incidents across the region (SingCERT, 2020). Therefore, an integrated approach combining both terrorism and cyber security studies is needed to fully grasp the scope of cyber terrorism in the ASEAN context.

In ASEAN member states, efforts to counter cyber terrorism have largely focused on traditional security measures aimed at protecting critical infrastructure. For example, Indonesia's National Cyber and Crypto Agency (BSSN) prioritizes the defense of critical digital infrastructure (Al Azhari, 2020). While these efforts are essential, they often overlook the social consequences of cyber terrorism, such as online radicalization and the spread of extremist ideologies. This is where the human security approach can offer a more holistic understanding by emphasizing the protection of individuals and communities, rather than just state assets (Newman, 2010). A human security approach broadens the scope of protection by addressing the societal impacts of cyber terrorism, including the spread of disinformation, psychological harm, and social instability.

The application of human security in cyber terrorism introduces a paradigm shift in how states approach the problem. Traditional security frameworks are state-centric, focusing on safeguarding national borders and infrastructure. These approaches prioritize military and technical measures, aiming to protect the state from external threats (Dunn Cavelty, 2012). However, cyber terrorism often targets vulnerable populations, exploits social divisions, and fosters disinformation, requiring a broader response. A human security approach shifts the focus from the state to the individual, emphasizing the need to protect people from threats that endanger their lives, livelihoods, and dignity (Kaldor, 2007). For instance, in Malaysia, community engagement programs and online literacy campaigns have been introduced to combat cyber radicalization, addressing both the technological and social dimensions of cyber terrorism (Ahmad & Yunos, 2019).

Incorporating human security into cyber security strategies broadens the scope of protection. Instead of focusing solely on preventing cyberattacks, human security considers the broader societal impacts of cyber terrorism, such as economic exploitation, the spread of extremist ideologies, and social divisions (Hampson et al., 2002). By integrating human security, policymakers can address the root causes of cyber terrorism, including social inequality, lack of education, and psychological vulnerabilities, and develop more effective, people-centered responses.

Empirical evidence from ASEAN member states suggests that cyber security stakeholders primarily focus on traditional security measures (Krebs, 2016). These efforts are essential for protecting critical infrastructure, but they often overlook the societal impacts of cyber terrorism. Meanwhile, anti-terrorism institutions such as Indonesia's Densus 88 concentrate on addressing the ideological drivers of terrorism, including the role of the internet in radicalizing individuals (Gunaratna & Iqbal, 2011). This division between cyber security stakeholders and anti-terrorism agencies highlights the need for a more integrated approach that combines both traditional and human security measures.

This paper aims to fill this gap by examining the extent to which human security principles are incorporated into cyber security strategies in ASEAN member states. Through a detailed analysis of these strategies, it will explore the challenges and opportunities in developing a comprehensive approach that addresses both state and individual security in the context of cyber terrorism. By bridging the gap between traditional and human security approaches, this research seeks to contribute to more effective strategies for combating cyber terrorism in ASEAN, ensuring the protection of both state and societal interests in the digital age.

2 Theoretical Framework

2.1 Definition and Principles of Traditional and Human Security Approaches

Traditional security and human security represent two distinct paradigms in international relations and security studies, both applied by scholars to understand and address various forms of threats, including cyber terrorism. The traditional security approach, deeply rooted in the realist school of thought, places the state as the primary actor. It defines security in terms of protecting national borders, sovereignty, and critical infrastructure, focusing primarily on external threats such as military invasions or acts of terrorism. In the context of cyber

terrorism, traditional security emphasizes the role of state institutions like intelligence agencies, military forces, and law enforcement in safeguarding national infrastructure, including cyberspace. The central objective remains the protection of the state, often through deterrence, defense, and coercive measures, which involve technological safeguards such as encryption and firewalls (Buzan, 1991; Walt, 1991).

The key principles of the traditional security approach include a zero-sum understanding of security, where the state's gain in security might come at the expense of others. This approach relies heavily on hard power tools such as military and intelligence capabilities, focusing on defending the state from external threats. Scholars applying this framework to cybersecurity studies often highlight the role of national defense mechanisms in preventing cyberattacks on government and economic systems. This framework is predominantly reactive, emphasizing protection and defense against visible threats like cyberattacks on national infrastructures (Deibert & Rohozinski, 2010; Nye, 2011).

On the other hand, the human security approach offers a broader and more inclusive perspective on security. Emerging from liberal and constructivist schools of thought, human security centers on the protection and well-being of individuals and communities, rather than focusing solely on the state. It includes a wide array of non-traditional threats such as economic insecurity, social inequality, and political repression, which may drive individuals toward radicalization. In combating cyber terrorism, human security highlights the importance of addressing the social, psychological, and economic factors that make individuals vulnerable to extremist recruitment online (Kaldor, 2007; UNDP, 1994).

The core principles of human security involve promoting human rights, addressing the root causes of insecurity like poverty and social injustice, and empowering communities to contribute to their own security. Scholars using this approach in cybersecurity often focus on digital literacy, promoting social inclusion, and creating resilient communities that are less vulnerable to extremist ideologies spread through digital platforms (Acharya, 2007; Paris, 2001).

2.2 Comparison Between Traditional Security and Human Security Approaches in Cyber Terrorism Studies

The differences between the traditional and human security approaches become evident when applied to cyber terrorism. Traditional security is state-centric and

emphasizes external threats, including cyberattacks that target critical infrastructure or key national industries. Scholars following this approach in cyber terrorism studies focus on strengthening technological defenses, enhancing cybersecurity protocols, and bolstering state mechanisms for monitoring and preventing cyber threats. National intelligence agencies and military cyber divisions are typically seen as the frontline defenders in these scenarios (Clarke & Knake, 2012; Rid & Buchanan, 2015).

In contrast, the human security approach shifts the focus from state institutions to individuals and communities. Scholars adopting this perspective argue that the root causes of cyber terrorism often lie in social marginalization, lack of economic opportunity, and the psychological vulnerabilities of individuals susceptible to online radicalization. Human security approaches emphasize non-state actors, including civil society organizations, educational institutions, and private companies, in addressing these issues. Rather than relying purely on technical solutions, human security frameworks advocate for enhancing social resilience, improving digital education, and fostering socio-economic equality to prevent cyber radicalization (Choucri, 2012; Nye, 2011).

This divergence in focus has practical implications. While traditional security scholars focus on protecting cyberspace as a state asset, human security scholars view cyberspace as a social arena where vulnerabilities can be exploited to recruit individuals into radical ideologies. Scholars have noted that the traditional security approach tends to react to visible cyber threats, often overlooking the underlying socio-political conditions that lead to extremism online (Nye, 2011). Conversely, the human security approach proactively addresses these root causes, aiming to prevent individuals from becoming radicalized in the first place (Acharya, 2007).

2.3 The Relevance of These Approaches in Combating Cyber Terrorism

In the context of cyber terrorism, both the traditional and human security approaches offer valuable but distinct frameworks for addressing the threat. The traditional approach, with its focus on defending national infrastructures through cyber defense mechanisms like encryption, intrusion detection systems, and state-led cybersecurity initiatives, remains critical in protecting national interests from cyberattacks (Clarke & Knake, 2012). However, scholars have argued that these technical defenses alone are insufficient to combat the evolving nature of cyber

terrorism, which increasingly exploits the psychological and social vulnerabilities of individuals (Deibert & Rohozinski, 2010).

The human security approach offers a complementary framework by addressing these non-technical aspects of cyber terrorism. In ASEAN, for example, social and economic inequalities are often exploited by extremist organizations to recruit individuals online. Scholars using the human security framework emphasize the need for community engagement, trust-building, and the promotion of digital literacy to combat cyber radicalization. Such efforts aim to create a more resilient digital environment where individuals are less vulnerable to extremist narratives, thus complementing the traditional cybersecurity measures implemented by the state (Acharya, 2007; Choucri, 2012).

The theoretical framework outlined above provides a critical lens for understanding the differing approaches scholars use when addressing cyber terrorism, particularly in the context of ASEAN member states. Both the traditional and human security approaches offer essential tools for combating cyber threats, but their distinct emphases on state versus individual security highlight the importance of applying a comprehensive strategy.

In this article, the relevance of this framework becomes especially significant in ASEAN, where diverse socio-political landscapes, varying levels of digital literacy, and economic disparities create both unique challenges and opportunities. ASEAN member states, while generally relying on traditional state-centric measures, such as cybersecurity regulations, cyber defense mechanisms, and surveillance technologies—are increasingly recognizing the limitations of these approaches in addressing the root causes of online radicalization.

The human security approach, with its emphasis on the well-being and security of individuals, complements these traditional measures by addressing the socio-economic conditions and psychological factors that drive individuals toward extremist ideologies. In ASEAN countries, where social inequalities, youth unemployment, and marginalization are prevalent, the human security framework provides a more inclusive and proactive strategy for preventing cyber terrorism. This framework promotes digital literacy, socio-economic resilience, and community engagement as key measures in combating online radicalization. By focusing on the protection and empowerment of individuals and communities, ASEAN states can foster a more resilient digital environment, reducing vulnerabilities that cyber terrorists exploit.

Moreover, the growing regional cooperation within ASEAN on cybersecurity issues, such as through the ASEAN Cyber Capacity Program (ACCP), underscores the need for a multi-dimensional approach to fighting cyber terrorism. While state-led initiatives remain crucial for securing national infrastructures,

integrating human security principles into these strategies can enhance their effectiveness. This integration ensures that cybersecurity measures not only defend state interests but also protect the most vulnerable populations from the psychological and social tactics used by cyber terrorists.

Thus, this article aims to demonstrate how a human security approach, when applied alongside traditional security measures, can offer a more comprehensive and sustainable framework for fighting cyber terrorism in ASEAN. The theoretical discussion reinforces the argument that ASEAN member states must embrace both frameworks, combining technological defenses with people-centered strategies to address the complex, multi-faceted nature of cyber terrorism in the region. By doing so, ASEAN can strengthen its collective cybersecurity while also promoting social stability, inclusion, and resilience against extremism.

3 Methodology

The methodology of this study follows a qualitative case study approach, designed to explore how human security principles are integrated into the cybersecurity strategies of ASEAN member states, particularly in the fight against cyber terrorism. Given the multifaceted nature of cyber terrorism, the study adopts a range of data collection methods, including document and literature reviews, focus group discussions (FGDs), and surveys. This combination enables a comprehensive analysis of both state and non-state actors' efforts to incorporate human security into their cybersecurity approaches (Azzahidi & Muhammad, 2024; Shin & Hyun, 2022).

The research process began with an extensive review of academic literature and policy documents. This initial phase provided a foundational understanding of cybersecurity and human security concepts, particularly within the ASEAN context. Through the review of key policy documents, such as ASEAN's cybersecurity strategy and national cybersecurity policies of individual member states, the study identified gaps in the existing frameworks and the degree to which human security principles were included (Collins, 2019; Thuzar, 2020). Additionally, the academic literature was essential in forming a theoretical basis for the study, highlighting ongoing debates in the fields of cybersecurity and human security (Rathmell, 2017).

Following the document and literature review, the second phase of data collection involved conducting FGDs with 20 key stakeholders. The FGDs were held as part of the ASEAN-IPR Regional Conference on Cybersecurity 2025.

This conference, funded by the ASEAN-Korea Cooperation Fund (AKCF), provided a platform for experts, policymakers, and practitioners to exchange insights on the integration of human security principles into cybersecurity strategies. These stakeholders, representing various sectors such as government agencies, law enforcement, civil society organizations, and cybersecurity experts, provided diverse insights into the real-world challenges of countering cyber terrorism. To complement the FGDs, a survey was administered to the same group of participants. The survey was designed to capture individual perspectives on the application of human security in combating cyber terrorism, allowing for a mix of both quantitative and qualitative data (Caballero-Anthony, 2016). After conducting the FGDs and surveys, a second round of document and literature review was undertaken to triangulate the findings and provide additional context (Shin & Hyun, 2022).

The data collected from all these sources were then analyzed using content analysis. This method allowed for the systematic coding of data to identify key patterns, themes, and trends. The analysis focused on how human security principles are either explicitly or implicitly included in policy documents, how stakeholders perceive these principles, and practical examples of their implementation in combating cyber terrorism. The content analysis revealed several important themes, such as the tension between state-centric and human-centric approaches, the need for trust-building in cyberspace, and the value of community-based interventions as a complement to technical cybersecurity solutions (Rathmell, 2017; Thuzar, 2020).

There are several strengths and weaknesses associated with this methodology. One of its key strengths is the triangulation of data from multiple sources, which provided a more holistic view of the research problem. The qualitative nature of the study allowed for an in-depth exploration of the human dimensions of cybersecurity, often overlooked in purely technical or quantitative studies. The use of FGDs, in particular, facilitated rich discussions and the sharing of diverse perspectives, especially in identifying challenges related to the application of the human security approach (Azzahidi & Muhammad, 2024).

However, the methodology is not without its limitations. The subjectivity inherent in qualitative research, particularly in interpreting FGD data, poses the risk of researcher bias, although steps were taken to mitigate this. Moreover, the relatively small sample size of 20 participants limits the generalizability of the findings across all ASEAN member states (Caballero-Anthony, 2016). Additionally, the sensitive nature of cybersecurity often restricts access to detailed data, which posed challenges during the policy document analysis, especially concerning state security practices (Collins, 2019).

Despite these limitations, the methodology employed in this study effectively captures the complexities of integrating human security principles into ASEAN's cybersecurity strategies. The combination of FGDs, surveys, and document reviews provided valuable insights into the current state of cybersecurity in the region, highlighting both the challenges and opportunities for a more human-centered approach to countering cyber terrorism.

4 Findings and Discussion

4.1 The Extent of Integration of Human Security Principles in Cyber Security Strategies Against Cyber Terrorism

State and non-state actors have increasingly recognized the need to integrate human security principles into their cybersecurity strategies to combat cyber terrorism. Unlike traditional cybersecurity approaches that focus on protecting state-centric systems and networks, human security prioritizes the well-being of individuals and communities, especially vulnerable groups. The extent of this integration, however, varies widely across regions and contexts.

4.2 Evolving Definitions and Frameworks

Key insights from focus group discussions highlighted the growing recognition of the importance of integrating human security principles into cybersecurity. Participants emphasized the need to move beyond traditional technical safeguards and incorporate human security into the very definitions of cybersecurity. This shift involves addressing the broader societal and individual implications of cybersecurity strategies, with a focus on fostering trust, inclusivity, and peacebuilding. Similarly, participants advocated for a critical security approach that centers human rights, collaboration, and digital inclusion. These perspectives underscore the necessity of a mindset shift to prioritize human security, particularly in emerging cyber environments such as online gaming, which are increasingly exploited for radicalization.

4.3 Regional and Sectoral Integration

Across ASEAN countries, varying levels of success in integrating human security principles into cyber strategies are observed:

4.3.1 Philippines

The Philippines demonstrates a strong focus on human security through community-based initiatives. Programs supporting the reintegration of former rebels align with human security principles by addressing psychological recovery and societal reintegration (SecurityMatters, 2025; Tangging, 2023). Additionally, the Commission on Women's advocacy for gender-sensitive cybersecurity policies reflects the prioritization of vulnerable groups, particularly women and children, who face unique challenges in cyberspace (Philippines WPS Country Brief, 2025; UN Women, 2025; UN Women, UNDP, & UNFPA, 2025).

4.3.2 Indonesia

In Indonesia, collaboration with the Ministry of Women's Empowerment and Child Protection has advanced tailored deradicalization programs and public awareness campaigns (Asia Pacific Center for Security Studies, 2015; Setkab, 2020). These efforts focus on addressing the specific vulnerabilities of women and children, as well as engaging them in counter-terrorism initiatives (Asia Pacific Center for Security Studies, 2015). Additionally, the government has begun tackling new threats, such as the radicalization of youth through online gaming platforms, though existing frameworks still need to adapt to these evolving challenges (Wildan, 2024).

4.3.3 Malaysia and ASEAN Initiatives

Malaysia has strengthened its cybersecurity through international collaborations, including drills and partnerships that enhance self-reliance in cyberspace (Axiata, 2024; Mohamed, 2013). ASEAN-wide initiatives, such as ASEAN-Japan Cooperation, have focused on improving cybersecurity systems in less secure countries, providing training programs, and raising security awareness (*Bangkok Post*, 2024; Gerry & Moore, 2015; JAIF, 2024a). The ASEAN Regional Forum (ARF) has also emphasized regional cooperation through seminars on cyber terrorism, fostering threat notifications and diplomatic prevention strategies (CCDCOE, 2013; Moslemzadeh Tehrani et al., 2013). These initiatives collectively demonstrate a commitment to protecting individuals and communities from cyber threats.

4.3.4 Singapore

In Singapore, the primary domestic terrorism threat emanates from self-radicalized individuals influenced by violent extremist materials online (SG101, 2024; Singapore Government, n.d.). The utilization of online and digital communications networks for terrorist recruitment poses challenges for authorities in detecting radicalized individuals. The phenomenon of self-radicalization in Singapore experienced a significant increase after 2015, following the emergence of ISIS (SG101, 2024). Regular counter-terrorism exercises are conducted to enhance operational preparedness (Singapore Government, n.d.).

In addition to operational responses from authorities, community engagement is crucial in the effort to counter terrorism. The SGSecure movement aims to sensitize, train, and mobilize the community in this endeavor (SGSecure, 2024). Led by the Ministry of Home Affairs, this national initiative is supported by six partner agencies, including the Ministry of Culture, Community & Youth, Ministry of Communications and Information, Ministry of Defence, Ministry of Education, Ministry of Manpower, and the People's Association, to engage various segments of society such as religious and community groups, media, schools, NS and Home Team volunteer community, workplaces, and neighborhoods (SGSecure, 2024). SGSecure programs enhance community awareness, vigilance, and cohesion against terrorism while also improving community emergency preparedness.

To mitigate the potential for actions by a small and isolated group of misguided Muslims to result in distrust and suspicion among Singaporeans, the government established the Inter-Racial Confidence Circles, which were renamed in 2007 as Inter-Racial and Religious Confidence Circles. These entities serve as platforms for leaders of various racial and religious communities to interact and foster trust and amity (SG101, 2024).

4.3.5 Thailand

Thailand's commitment to data protection, as evidenced by the Personal Data Protection Act (PDPA), lays a strong foundation for integrating human security principles into its cyber strategies (Chambers & Partners, 2025). The PDPA's emphasis on individual rights, such as privacy and data control, aligns with the core of human security, which prioritizes the well-being and dignity of individuals in the digital realm. By ensuring responsible data handling and promoting transparency, the PDPA fosters trust and accountability, crucial elements for creating a secure and inclusive online environment.

Moreover, Thailand's active participation in regional cybersecurity initiatives, such as those under the ASEAN framework, demonstrates a commitment to collaborative efforts in addressing cyber threats. These initiatives often involve

capacity-building programs, information sharing, and joint exercises aimed at strengthening cybersecurity infrastructure and response mechanisms (*Bangkok Post*, 2024; Cyble, 2025; Sattar, 2022).

4.3.6 ASEAN Cybersecurity Strategy (CCS) 2021–2025

The discussion underscored ASEAN's unwavering commitment to advancing its cybersecurity strategy. Although ASEAN's cybersecurity frameworks do not explicitly align with the human security paradigm, the principles of human security-protection of individuals, community well-being, inclusivity, and accountability-are embedded within these initiatives (ASEAN, 2021; Sari, 2023). This is evident in several key areas:

Firstly, the strategy aims to create a secure and resilient cyberspace that underpins ASEAN's digital ambitions, which include improving the lives of ASEAN citizens, fostering regional economic growth, and building a leading digital community (ASEAN, 2021; Sari, 2023).

Secondly, the strategy also emphasizes the importance of promoting cyber hygiene and digital inclusion to ensure that individuals and communities are able to protect themselves from cyber threats. This is essential for building trust in the digital space and ensuring that everyone can benefit from the opportunities it presents (ASEAN, 2021).

Thirdly, the strategy focuses on building the cybersecurity skills and knowledge of individuals and communities through multi-disciplinary, modular, and measurable capacity-building programs. This will help to ensure that ASEAN is well-prepared to address the challenges of the digital age and protect its citizens from cyber threats (ASEAN, 2021; Sari, 2023).

4.4 Contribution by Non-state Actors

Non-state actors, including civil society organizations (CSOs), private sector entities, and regional coalitions, are indispensable in embedding human security principles into cybersecurity strategies. Civil society organizations often lead advocacy efforts to promote a human-centric approach, emphasizing the protection of privacy, trust-building, and human rights in cyberspace. These organizations have a growing influence on policymaking processes across Southeast Asia, pushing for cybersecurity frameworks that address the specific vulnerabilities faced by individuals and communities (Caballero-Anthony, 2016; Shin & Hyun, 2022).

The private sector plays a pivotal role by driving community-based cybersecurity initiatives. These include funding and implementing programs aimed at increasing digital literacy and resilience among local populations. Such efforts help bridge critical gaps in cybersecurity awareness and equip individuals with the knowledge to protect themselves against digital threats. As noted by Rathmell (2017), private-sector engagement fosters innovation in applying human-centric solutions to complex cybersecurity challenges.

Community-based interventions led by non-state actors, such as digital literacy campaigns and public awareness programs, are equally vital in building cybersecurity resilience. These programs empower local communities to actively participate in their own protection, fostering a more human-focused approach to cybersecurity. For instance, Thuzar (2020) highlights the effectiveness of such interventions in enhancing grassroots participation, particularly in regions with limited access to formal cybersecurity resources.

Despite these contributions, several challenges impede the consistent application of human security principles. Coordination gaps between state and non-state actors undermine collaborative efforts, often leading to fragmented strategies and inefficiencies. Furthermore, the varying levels of digital literacy across ASEAN populations exacerbate disparities in cybersecurity preparedness, as individuals in less developed regions remain disproportionately vulnerable to cyber threats (Collins, 2019; Shin & Hyun, 2022). These challenges underscore the importance of fostering stronger partnerships between governments, civil society, and the private sector to create cohesive and inclusive cybersecurity frameworks (Azzahidi & Muhammad, 2024).

4.5 Predominant Strategies Used by State and Non-State Actors Within ASEAN Members

Cybersecurity strategies across ASEAN nations illustrate a dynamic interplay between traditional state-centric security and human security approaches. While the region predominantly embraces traditional security models emphasizing sovereignty, law enforcement, and technological controls, there is an emerging shift towards human-centered strategies that prioritize inclusion, resilience, and well-being. This duality reflects both the constraints and potential of ASEAN's geopolitical culture in addressing evolving digital threats.

4.5.1 Legal Frameworks and Technological Interventions

A cornerstone of traditional cybersecurity strategies lies in the use of legal frameworks and technological interventions. These measures are often rooted in state-centric paradigms that prioritize control, deterrence, and infrastructure protection. For instance, Indonesia's efforts to remove harmful online content and prosecute cybercrimes exemplify a traditional, state-led enforcement strategy (SA1/M/FGD, 2024). The Philippines follows a multi-agency model that blends legal action and digital investigation to tackle online harassment and extremist content (SA2/F/FGD, 2024). Singapore and Malaysia have invested heavily in Security Operations Centers (SOCs) and other technological systems that provide real-time threat detection, reflecting strong traditional security logic.

However, while these responses effectively strengthen national cyber defense, they may neglect rights-based and community-centered considerations, as pointed out by Strating et al. (2024), who argue that ASEAN's legal responses often lack a human security lens. Despite these limitations, Computer Emergency Response Teams (CERTs)—such as SingCERT and ID-SIRTII—offer an important bridge. Their coordination roles and emphasis on rapid information sharing enable a more responsive and cooperative model, which, if enhanced with user-focused support, could better align with human security principles.

4.5.2 Public Awareness Campaigns

Public education is increasingly recognized as essential to cybersecurity resilience. Traditional awareness campaigns focus on educating citizens about digital risks and hygiene. For example, Thailand's "Cyber Immunity" campaign and the Philippines' "CyberSafe" initiative concentrate on protecting users through digital literacy. By contrast, human security-driven efforts seek to empower individuals as active agents in their own defense. Finland's counter-narrative integration into education is an instructive model, emphasizing internal resilience over mere compliance. Some ASEAN states—like Singapore and Malaysia, through integration of cyber hygiene in school curricula—are inching closer to this empowerment-based model (NSA1/M/FGD, 2024). This divergence reflects the broader tension in ASEAN between state-dominated narratives and the need for community resilience, as highlighted by Miller et al. (2022). While ASEAN's political culture tends to resist overt confrontation and intervention, these softer strategies represent incremental shifts toward broader well-being considerations.

4.5.3 Inclusion and Engagement

Human security strategies strongly emphasize inclusion, especially of marginalized groups. For example, Indonesia's engagement of women in counterterrorism communication efforts exemplifies the recognition of diverse societal roles in fostering resilience (NSA2/F/FGD, 2024). Cyber Peace Philippines, through its promotion of digital citizenship and de-radicalization, shows how non-state actors help advance human security goals (SA6/F/FGD, 2024). In Vietnam, cybersecurity outreach and training for rural populations reflect efforts to bridge the digital divide—a fundamental aspect of inclusive security (NSA4/M/FGD, 2024). Yet, regional political norms, such as non-interference, can limit how far these inclusive practices extend across ASEAN. Nevertheless, these examples underscore the crucial role that civil society and local communities play in reinforcing cybersecurity at the grassroots level—highlighting the importance of non-state actors in advancing human-centered cybersecurity (Gargiulo et al., 2024).

4.5.4 AI and Data Analytics

The rise of AI and data analytics presents both opportunities and dilemmas. Traditional uses of AI—such as surveillance or content control—align with state-centered security logic, prioritizing monitoring and enforcement. For example, Singapore's use of AI for anomaly detection strengthens infrastructure defense, a hallmark of traditional approaches (SA7/M/FGD, 2024). On the other hand, AI-driven sentiment analysis and early warning systems, like those in the Philippines, open possibilities for proactive and preventive measures rooted in community needs—provided these tools are deployed ethically and with transparency (GSMA, 2022). This dual use of AI reflects broader ASEAN dynamics: the potential of technology to reinforce state power, but also to enhance community resilience when aligned with human security goals.

4.5.5 Support for Victims and Vulnerable Groups

Human security principles are clearest in strategies that prioritize victim support. In the Philippines, victims of cyber harassment receive legal assistance and counseling, with policies addressing intersectional vulnerabilities (NSA3/F/FGD, 2024). Similarly, South Korea's public–private programs to support GBV victims in cyberspace underscore the need for targeted and empathetic responses (SA3/F/FGD, 2024). Such practices contrast with more punitive or enforcement-centered approaches, reaffirming that security must address harm, not just threats. These victim-centered strategies reflect a deep alignment with the broader well-being emphasis of human security frameworks, contributing to more comprehensive cyber resilience.

4.5.6 Community-Based Interventions

Community-based approaches are among the most robust examples of human security in action. Programs such as the reintegration of former rebels in the Philippines' Davao Oriental, as discussed by Golez (2018) and SA2/F/FGD (2024), reflect a holistic focus on psychological recovery, livelihood support, and social inclusion. These efforts embody the human security ethos: addressing root causes, promoting peace, and reintegrating individuals into society. Although often under-supported by national governments due to ASEAN's traditional norms, such localized programs exemplify sustainable, people-centered security solutions.

4.6 The Efficacy of Current Efforts

The effectiveness of efforts by state and non-state actors to address online radicalization from a human security perspective is mixed. While there is growing awareness of the need to incorporate human security principles, focusing on trust-building, community resilience, and addressing underlying social and psychological factors—these efforts remain in the early stages and face significant challenges.

5 Strengths of Current Efforts

5.1 Integration of Human Security Principles

Some initiatives have made strides in addressing the root causes of radicalization by incorporating human security elements. For example, in the Philippines, community reintegration programs designed to reintegrate former rebels into society reflect a holistic approach (SA2/F/FGD, 2024). These programs address both the psychological and societal reintegration needs of individuals, demonstrating an understanding of the complex factors involved in radicalization.

Indonesia's efforts to engage female actors as credible messengers and promote inclusion in counter-extremism efforts also demonstrate the application of human security principles (NSA2/F/FGD, 2024). This approach recognizes the importance of addressing community and cultural dynamics in countering extremism and leverages the influence of women in these efforts. Furthermore, the inclusion of gender perspectives in cybersecurity policies, such as initiatives targeting online gender-based violence (GBV), represents progress toward a

more nuanced understanding of radicalization's impact on vulnerable groups. This highlights a growing recognition that radicalization and its effects are not uniform across populations and that tailored approaches are necessary to effectively address the specific vulnerabilities faced by different groups.

5.2 Digital Literacy and Awareness Campaigns

Efforts to promote digital literacy and counter misinformation are vital in empowering communities and fostering resilience against cyber threats. These initiatives recognize that knowledge and awareness are crucial tools in enabling individuals to navigate the digital landscape safely and responsibly.

For example, in Indonesia, counter-narrative efforts are embedded in some educational initiatives (NSA2/F/FGD, 2024). This approach aims to address vulnerabilities and build community resilience by equipping individuals with the critical thinking skills and knowledge necessary to resist misinformation and extremist narratives. Similarly, ASEAN-Japan cooperation emphasizes awareness campaigns and training programs. These efforts aim to enhance cybersecurity and protect vulnerable populations, including children, from online threats, highlighting the importance of international collaboration in promoting digital literacy and awareness across borders (Gerry & Moore, 2015).

5.3 Role of Non-state Actors

Non-state actors have played a crucial role in advancing cybersecurity governance, particularly in areas where state actors may lack proactive measures or the capacity to respond effectively. These actors often bring unique expertise, resources, and perspectives to the challenges of cybersecurity. For instance, private sector organizations, such as financial institutions, have self-regulated to establish secure communication standards. This self-regulation demonstrates a proactive approach to enhancing security and building trust within their sector (Hoong et al., 2024). Furthermore, technology companies contribute by developing tools designed to counter disinformation and online radicalization. While challenges remain in their enforcement due to factors like encryption and scale, these efforts highlight the important role that private companies play in developing and implementing solutions to address complex cybersecurity threats.

5.4 Use of Artificial Intelligence

Artificial intelligence (AI) is increasingly being employed to detect and counter various cyber threats, including disinformation and psychological operations. This reflects a growing reliance on technology to address the evolving challenges of cybersecurity. AI tools are being deployed to monitor extremist content, analyze trends in radicalization, and counter polarization and political violence (Burton, 2023). These applications demonstrate the potential of AI to enhance cybersecurity efforts. However, it is critical to ensure responsible AI use. This involves careful consideration of ethical implications and potential biases to ensure that AI applications align with human security principles and do not inadvertently cause harm or infringe on individual rights.

5.5 Community-Centered Initiatives

Community-centered initiatives have emerged as a cornerstone of ASEAN member states' strategies to prevent and counter radicalization and violent extremism, demonstrating notable strengths across diverse national contexts. These approaches leverage the unique insights, trust, and social capital of local actors-such as community leaders, educators, religious figures, and grassroots organizations-to detect early warning signs, foster resilience, and disrupt extremist narratives before they escalate. For instance, Indonesia's integration of civil society and local foundations in educational and dialogue-based programs has empowered communities to build resistance against radical ideologies (Global Strategis, 2022; Indonesian Journal of International Clinical Legal Education, 2021). In the Philippines, the active participation of NGOs and community members in program design and implementation has enhanced the relevance and sustainability of counter-radicalization efforts, while also fostering a sense of ownership and self-reliance among beneficiaries (Philippines Government, 2020). Singapore's SGSecure movement and interfaith dialogue platforms illustrate how state-led, community-embedded programs can strengthen social cohesion and preparedness (Hussin, 2022; SGSecure, 2025). Thailand's inclusive, consultative dialogues with minority and youth groups, and Vietnam's mobilization of mass organizations, further highlight the adaptability of this approach to different political and cultural settings (ASEAN-IPR CyberCon, 2025; United Nations, 2023). These examples align with ASEAN's Plan of Action, which emphasizes engaging communities, promoting dialogue, and building trust between vulnerable populations and law enforcement as essential components of an integrated,

evidence-based response to radicalization (ASEAN, 2018). By rooting prevention efforts in community engagement, ASEAN member states not only address the local drivers of extremism but also reinforce democratic values, social harmony, and regional stability.

5.6 Public–Private Partnerships

ASEAN member states have demonstrated significant strengths in addressing cyber radicalisation through the adoption of Public–Private Partnerships (PPPs). These partnerships are embedded in ASEAN's regional strategies, such as the ASEAN Plan of Action to Prevent and Counter the Rise of Radicalisation and Violent Extremism, which explicitly encourages collaboration with the business community to research and counter the misuse of the internet and social media by violent extremists (ASEAN, 2018). PPPs enable the pooling of resources, expertise, and technology from both government and industry, bridging technical and operational gaps that individual sectors might face alone (OpenGov Asia, 2023). By leveraging private sector innovation-especially in cybersecurity, artificial intelligence, and data analytics-ASEAN governments can more effectively detect, disrupt, and prevent online radicalisation, disinformation, and terrorist financing (Tay, 2023).

Regional initiatives such as the Monetary Authority of Singapore's collaboration with the Financial Services Information Sharing and Analysis Center, the ASEAN Regional Computer Emergency Response Team (CERT), and the ASEAN Cybersecurity Resilience and Information Sharing Platform (CRISP) further illustrate how PPPs facilitate information sharing, capacity building, and coordinated incident response across member states (CSIS, 2024; RSIS, 2024). These efforts are complemented by ASEAN's focus on inclusive stakeholder engagement, capacity building, and harmonized cybersecurity policies, which collectively foster trust, bridge skill gaps, and ensure a more resilient and secure digital environment for both people and businesses in the region (OpenGov Asia, 2023; RSIS, 2024). While challenges remain in harmonizing approaches and bridging readiness gaps among member states, the integration of PPPs into ASEAN's cybersecurity and counter-radicalisation frameworks stands out as a key strength, enhancing both regional preparedness and the ability to respond to evolving online threats (ASEAN, 2018; Tay, 2023).

5.7 Focus on Youth and Education

Regional initiatives across Southeast Asia are increasingly prioritizing digital literacy and youth empowerment as key strategies to mitigate the influence of extremist propaganda. In the Philippines, programs such as the Cyber for Peace Initiative integrate technology into educational curricula, equipping students with critical online safety skills and fostering resilience against harmful narratives. This approach aligns with broader findings that youth-led organizations in the Philippines, like KRIS and the Youth for Peace Movement, effectively use digital platforms to promote peace, challenge extremist content, and advocate for positive values through both online and offline activities (GNET, 2024). These initiatives not only address immediate threats but also build long-term community resilience by empowering young people to become proactive agents of change.

Similarly, Indonesia has seen the rise of youth-led programs that mobilize university students as digital ambassadors, leveraging peer-to-peer influence to counter extremist narratives on social media. Initiatives such as the Media and Information Literacy (MIL) workshops organized by the National Counterterrorism Agency (BNPT) and Hedayah focus on equipping students with the skills to identify, analyze, and respond to online extremism (BINUS University, 2025). Academic research further highlights the effectiveness of these strategies, noting that youth-driven counter-narrative campaigns-such as those run by GP Ansor's Ansor Cyber Army-play a pivotal role in promoting tolerance and digital literacy, thereby increasing public understanding of pluralism and reducing the appeal of radical ideologies (Jazuli, 2016; Satriawan et al., 2019). Collectively, these dual approaches-integrating digital literacy into education and fostering direct youth engagement-have been recognized as best practices for building digital resilience and strengthening societal defenses against online extremism (GNET, 2024).

5.8 Regional Cooperation and Knowledge Sharing

ASEAN's implementation of cyber norms has significantly strengthened intelligence sharing and collective cybersecurity capacity among its member states, particularly in addressing threats related to radicalization and cross-border cybercrime. The establishment of mechanisms such as the ASEAN Regional Computer Emergency Response Team (CERT) exemplifies this collaborative approach, facilitating timely information exchange, joint capacity-building, and coordinated incident response across the region (ASEAN, 2021). These efforts go beyond

basic information sharing by incorporating standardized protocols, regional cybersecurity exercises, and the development of a point-of-contact network among national CERTs, thereby enhancing both operational coordination and mutual trust (ASEAN, 2021). Academic analysis highlights that such confidence-building measures and capacity-building initiatives are essential first steps in establishing effective region-wide cyber norms, especially given the varying levels of cyber maturity among member states (Ang, 2020; Kshetri, 2021).

Moreover, ASEAN is actively working toward a comprehensive regional cybersecurity framework that includes harmonizing legal standards, promoting best practices, and fostering public–private partnerships (Neumetric, 2024; OpenGov Asia, 2023). The launch of initiatives like the ASEAN-Japan Cybersecurity Community Alliance's Threat Intelligence Sharing Working Group further demonstrates ASEAN's commitment to structured intelligence sharing and collaborative threat analysis (AJCCA, 2025). Scholars note that these multistakeholder efforts-engaging governments, industry, and academia-are vital for operationalizing cyber norms and ensuring that policies are both practical and adaptable to the rapidly evolving threat landscape (ASPI, 2025; Kshetri, 2021). By institutionalizing regular dialogues, joint training, and regional exercises, ASEAN's approach not only addresses immediate cyber threats but also builds long-term resilience, reinforcing the interconnectedness of digital security and regional stability (ASEAN, 2021; CSIS, 2024).

5.9 Effectiveness in ASEAN: A Regional Perspective

ASEAN member states' efforts to counter radicalization and violent extremism indeed reflect a blend of traditional and human security approaches, with mixed outcomes. The traditional security paradigm, rooted in ASEAN's longstanding principles of state sovereignty and non-interference, has historically prioritized law enforcement, criminalization, and state-centric responses over rights-based or community-centered strategies (Jones, 2010; Strating et al., 2024). This approach is evident in the ASEAN Plan of Action to Prevent and Counter the Rise of Radicalisation and Violent Extremism (2018–2025), which emphasizes strengthening national legislation, law enforcement capacity, and regional intelligence sharing as primary tools for countering radicalization (ASEAN, 2018). While these measures have contributed to regional stability, scholars argue that the rigidity of the non-interference principle and the consensus-based "ASEAN Way" can limit the effectiveness of collective action and the adoption of more holistic, preventive strategies (Katsumata, 2003; Nishikawa, 2010).

At the same time, there is growing recognition of the value of human security approaches, which focus on addressing the root causes of radicalization by tackling social grievances, marginalization, and vulnerabilities within communities (Hastings & Raghavan, 2015; UNODC, 2022). Tools such as the Human Security Index provide frameworks for assessing these vulnerabilities, but their application remains uneven across ASEAN due to varying levels of political will, resources, and institutional capacity (Hastings & Raghavan, 2015). Recent initiatives, such as Indonesia's adoption of a human security framework in its National Plan of Action against Violent Extremism, demonstrate promising progress by integrating community engagement, gender perspectives, and digital literacy into prevention efforts (UNODC, 2022). However, the lack of enforceable regional mechanisms and the underutilization of non-state actors continue to hinder the full realization of human security objectives (ASEAN-IPR CyberCon, 2025; Peou, 2015). Even with international cooperation-such as cybersecurity partnerships with Japan and capacity-building programs like the ASEAN-Japan Cybersecurity Capacity Building Centre-gaps remain in harmonizing legal frameworks, sharing best practices, and addressing the structural and psychological drivers of radicalization (JAIF, 2024b). Bridging these divides requires a nuanced, inclusive approach that balances state security concerns with people-centered strategies and fosters collaboration across government, civil society, and regional partners (Nishikawa, 2010; UNODC, 2022).

5.10 Identified Gaps and Challenges of Integration

Implementing a human security approach to counter terrorist group activities in cyberspace faces several interrelated gaps and challenges. While the principles of human security prioritize the protection of individuals and communities by addressing the root causes of insecurity, their application in cyberspace requires overcoming significant structural, technical, and social barriers.

6 Key Gaps and Challenges

6.1 The Elusive Foundation of Trust in Cyberspace

A fundamental obstacle to the effective application of human security principles in the digital realm is the pervasive lack of trust. This deficiency stems from two critical issues: first, the inherent opacity of online interactions, where

confidentiality often obscures transparency, hindering the verification of platform security and the establishment of reliable digital relationships. Second, a prevalent distrust in institutions, both governmental and private, arises from the delicate balance between transparency and confidentiality (SA1/M/FGD, 2024; SA5/M/FGD, 2024). When accountability falters, and stakeholders fail to uphold their responsibilities, public confidence erodes, undermining the very foundation of secure and inclusive digital environments.

6.2 Fragmented and Insufficient Frameworks

Current cybersecurity policies frequently prioritize national security interests over the broader imperatives of human security, resulting in fragmented and non-comprehensive frameworks. This is particularly evident in the ASEAN region, where the absence of a unified legal framework for addressing cyberterrorism, as highlighted by Onyeji et al. (2014), impedes collective action. Furthermore, a significant disconnect exists between state and non-state actors, leading to inconsistent implementation of human security principles. This fragmentation necessitates a paradigm shift towards a more holistic and collaborative approach that integrates human security considerations into cybersecurity strategies and fosters greater cooperation among all stakeholders (NSA3/F/FGD, 2024; SA3/F/FGD, 2024).

6.3 The Blurred Lines of Threat Actors

The increasingly blurred distinction between criminal actors, extremist groups, and state-sponsored cyber aggressors presents a formidable challenge to effective cyber threat mitigation (NSA2/F/FGD, 2024; NSA6/M/FGD, 2024). The overlapping motivations of these diverse actors, who frequently exploit the same digital tools, complicate the development of targeted interventions. Moreover, the transnational nature of cyber operations and the complexities of jurisdictional boundaries further hinder the attribution and prosecution of cyberterrorists. This necessitates enhanced international cooperation, standardized legal frameworks, and advanced forensic capabilities to effectively address the evolving and multifaceted nature of cyber threats (NSA4/M/FGD, 2024).

6.4 The Inherent Biases and Ethical Quandaries of Technology

While digital tools, particularly AI, hold promise for countering online extremism, their application is often marred by inherent biases and ethical quandaries. The risk of AI tools perpetuating and amplifying existing social and cultural biases, as emphasized by SA5/M/FGD (2024) and NSA5/M/FGD (2024), directly undermines the pursuit of equitable human security. Furthermore, the significant influence of private sector entities in the development of these digital tools, coupled with limited public oversight, raises critical concerns about their alignment with human security priorities, as noted by Reveron and Savage (2020). This necessitates a robust framework for ethical AI development and deployment, prioritizing transparency, accountability, and the mitigation of algorithmic biases.

6.5 The Neglect of Gender and Age Sensitivity

A critical deficiency in current cybersecurity policies is the lack of gender-sensitive and age-appropriate approaches. This oversight disproportionately affects marginalized groups, particularly women, children, and young people, who are rendered more vulnerable to online extremism, as highlighted by NSA2/F/FGD (2024). Furthermore, the prevalence of male-dominated legal frameworks in many countries fails to adequately address the specific vulnerabilities of women and children in cyberspace (NSA3/F/FGD, 2024). This necessitates a paradigm shift towards inclusive cybersecurity policies that incorporate gender-sensitive and age-appropriate considerations, ensuring the protection of all individuals in the digital realm.

6.6 The Exacerbating Influence of Technological and Financial Disparities

Significant disparities in technological capabilities and financial resources amplify the digital divide, particularly within regions like ASEAN, hindering the effective implementation of human security approaches. The lack of technical expertise among ASEAN member states necessitates targeted capacity-building efforts to address critical gaps in cybersecurity skills, as emphasized by Chambers et al. (2004). Moreover, uneven technological development and inadequate cybersecurity infrastructure, as noted by Song and Hou (2024), create substantial barriers

to the adoption of human security principles. This necessitates a concerted effort to bridge the digital divide through investments in infrastructure development, skills training, and international collaboration, ensuring equitable access to digital security for all.

6.7 Emerging Threats on New Platforms

A critical oversight in current human security strategies is the insufficient focus on emerging threats, particularly the growing exploitation of newer digital platforms, such as online gaming, for radicalization (NSA1/M/FGD, 2024). These platforms present underexplored vulnerabilities, as the complex dynamics of radicalization within gaming environments remain largely under-researched and poorly understood (NSA5/M/FGD, 2024). This necessitates urgent attention to developing targeted strategies that address the unique characteristics of these platforms and mitigate the risks they pose.

6.8 Private Sector Involvement and Governance

The increasing reliance on private sector entities for cybersecurity solutions introduces complex governance challenges, particularly in aligning commercial interests with human security goals (NSA3/M/FGD, 2024). The widespread use of encryption technologies and the sheer scale of operations by technology companies significantly impede law enforcement's ability to access critical data, hindering investigations and threat mitigation efforts (NSA4/M/FGD, 2024). Furthermore, the global business models of information and communications technology (ICT) companies, which often prioritize profit maximization, can conflict with national or community security concerns, as highlighted by Reveron and Savage (2020). This necessitates a collaborative approach that fosters greater transparency, accountability, and alignment between private sector practices and human security imperatives.

7 Regional and International Challenges in ASEAN

7.1 The Paradox of Cooperation and Coordination

While ASEAN member states have demonstrated progress through regional initiatives like the ASEAN Regional Forum (ARF), which aims to foster information sharing and cooperation, significant gaps persist in achieving effective collective action. The ARF's inherent limitations, particularly the lack of robust enforcement mechanisms, as highlighted by Moslemzadeh Tehrani et al. (2013), diminish its capacity to effectively counter cyberterrorism. Furthermore, the prevailing emphasis on sovereignty and non-interference principles within ASEAN, as noted by Wei (2024), creates a reluctance to share sensitive information, impeding deeper collaboration and hindering the development of a unified regional response to cyber threats.

7.2 The Impediment of Economic and Developmental Divergence

The economic dependencies and uneven technological advancement among ASEAN countries pose a substantial impediment to the collective ability to counter cyber threats effectively. The persistent funding deficits for cybersecurity initiatives, as emphasized by Chambers et al. (2004), severely restrict the implementation of human security approaches. This disparity in resources and capabilities creates a fragmented regional landscape, where some member states are significantly more vulnerable to cyberattacks than others, undermining the overall security of the region.

Addressing these gaps and challenges requires a holistic and inclusive approach that combines human security principles with technological, legal, and collaborative strategies. Key recommendations include developing unified regional frameworks that integrate human security principles into cybersecurity governance, fostering public–private partnerships to align corporate practices with human security goals, promoting gender-sensitive and youth-centered policies to protect vulnerable groups, and enhancing international cooperation and capacity-building efforts to bridge technological and financial gaps (NSA2/F/FGD, 2024; NSA3/M/FGD, 2024; SA3/F/FGD, 2024; NSA6/M/FGD, 2024). While the human security approach offers a promising framework for countering terrorist group activities in cyberspace, its successful implementation depends on overcoming these critical barriers through coordinated and sustained efforts.

7.3 Different Roles, Synergy and Potential Conflict

The roles of state and non-state actors in addressing complex global issues like online extremism, cyberterrorism, and human security differ significantly due to variations in their priorities, resources, and operational frameworks. These differences shape their approaches and lead to both synergies and conflicts in their efforts.

8 Roles and Approaches

8.1 State Actors

State actors, encompassing governments, law enforcement agencies, and public institutions, predominantly adopt a top-down approach, emphasizing regulatory frameworks, enforcement mechanisms, and the protection of critical infrastructure. Their focus is often driven by national security imperatives, reflected in priorities such as prosecuting cybercriminals, enforcing international treaties, and safeguarding critical infrastructure (Gargiulo et al., 2024). Furthermore, state actors engage in bilateral and multilateral agreements to address transnational threats, such as cybercrime and human trafficking, as highlighted by Strating et al. (2024). However, their centralized policy-making processes, particularly in sensitive areas like data protection, surveillance, and counter-extremism efforts, can lead to concerns regarding transparency and accountability, as discussed by Reveron and Savage (2020).

8.2 Non-State Actors

Non-state actors, including NGOs, private sector organizations, academic institutions, and civil society groups, adopt a more decentralized and human-centered approach, prioritizing inclusion, human rights advocacy, and grassroots engagement. They address non-traditional security challenges, such as digital literacy, gender equity, and youth empowerment, as exemplified by López-Rodríguez et al. (2020). Non-state actors contribute through innovative solutions, including research, counter-narrative campaigns, and the leveraging of technology to build resilience and prevent radicalization. Their flexible and diverse participation allows them to adapt rapidly to emerging challenges and provide direct support to marginalized communities, as demonstrated by Nasiritousi et al. (2014).

9 Synergies

9.1 Collaborative Governance

State and non-state actors can forge powerful public–private partnerships, effectively merging regulatory frameworks with community-level interventions to address complex challenges like online extremism. For example, law enforcement agencies can collaborate with educational institutions to develop and deliver impactful counter-narrative campaigns, leveraging both regulatory authority and grassroots engagement (NSA3/F/FGD, 2024; SA3/F/FGD, 2024; NSA3/M/FGD, 2024; NSA6/M/FGD, 2024). Furthermore, multilateral forums, such as the ASEAN Regional Forum (ARF), provide crucial platforms for knowledge sharing, capacity building, and coordinated efforts between governments and non-state actors, fostering a more unified and effective regional response, as highlighted by Moslemzadeh Tehrani et al. (2013).

9.2 Capacity Building and Resource Sharing

Non-state actors often play a vital role in complementing state efforts by providing specialized expertise, targeted training, and innovative technological tools, thereby enhancing state capabilities. This collaborative dynamic is particularly critical in regions with limited technical expertise or financial resources, as noted by Strating et al. (2024) and Chambers et al. (2004). By pooling resources and expertise, state and non-state actors can create a more resilient and effective cybersecurity ecosystem (NSA3/F/FGD, 2024; SA3/F/FGD, 2024; NSA3/M/FGD, 2024; NSA6/M/FGD, 2024).

9.3 Holistic Approach

The synergy between state-driven security measures and non-state-led human security principles enables the development of comprehensive and integrated strategies. For example, governments can leverage private sector technology for surveillance and threat detection, while NGOs simultaneously promote digital literacy and inclusion initiatives to address the root causes of extremism. This holistic approach recognizes the interconnectedness of security and human rights, fostering a more sustainable and equitable response to online threats (NSA3/F/FGD, 2024; SA3/F/FGD, 2024; NSA3/M/FGD, 2024; NSA6/M/FGD, 2024).

10 Conflicts

10.1 Divergent Priorities

State actors often emphasize traditional security, such as surveillance and prosecution, which may conflict with the human-centered approaches of non-state actors. For instance, heavy-handed content removal or surveillance by states can clash with NGOs' emphasis on transparency and individual freedoms (NSA1/M/FGD, 2024; NSA3/M/FGD, 2024; NSA5/M/FGD, 2024).

10.1.1 Jurisdictional and Policy Misalignment

The transnational nature of cyberspace creates jurisdictional challenges for state actors, while non-state actors' cross-border activities may sometimes undermine national regulations. This misalignment complicates efforts to enforce cyber laws and combat online extremism (ASEAN, 2018).

10.1.2 Private Sector Challenges

Companies in the private sector may prioritize profit over public good, leading to a conflict of interest when partnering with states or NGOs. For example, the use of AI tools by private entities could perpetuate bias and inequities, further complicating the efforts of human security advocates (NSA3/F/FGD, 2024; NSA4/M/FGD, 2024; SA5/M/FGD, 2024).

10.1.3 Resource Gaps and Dependency

Non-state actors often face challenges in scaling their initiatives due to limited resources and overreliance on state support. Conversely, states may struggle with outdated technology or lack of expertise, particularly in developing regions like ASEAN (Song & Hou, 2024).

The distinct roles of state and non-state actors offer both opportunities and challenges in addressing online extremism and broader human security concerns. Effective collaboration requires clear role definitions, resource-sharing mechanisms, and respect for differing priorities. By fostering synergies and addressing conflicts through inclusive dialogue and shared goals, state and non-state actors can create a balanced and comprehensive approach to tackling complex global threats.

11 Conclusion

This research paper investigates the integration of human security principles into cybersecurity strategies within ASEAN member states, focusing on the fight against cyber terrorism. The study employs a qualitative methodology, utilizing a mix of document reviews, focus group discussions (FGDs), and surveys to gather data from both state and non-state actors. The findings reveal a complex interplay of traditional and human security approaches, highlighting both progress and significant challenges in fostering a truly comprehensive and effective response to cyber terrorism.

The core argument underscores the insufficiency of solely relying on traditional state-centric cybersecurity measures, which emphasize infrastructure protection and technical solutions. While these remain crucial, the study emphasizes the urgent need to incorporate human security principles that prioritize the well-being of individuals and communities. This necessitates a shift towards proactive measures addressing the root causes of online radicalization—socio-economic inequalities, psychological vulnerabilities, and the spread of extremist ideologies. The paper demonstrates how human security approaches, by focusing on inclusivity, community empowerment, and digital literacy, can create more resilient societies less susceptible to manipulation and exploitation.

The research highlights several promising initiatives across various ASEAN member states. The Philippines, for example, demonstrates a commitment to human security through community-based reintegration programs and initiatives aimed at gender-sensitive cybersecurity policies. Indonesia's efforts in incorporating tailored deradicalization programs, particularly targeting vulnerable groups like women and children, and addressing the evolving challenges of online gaming radicalization also demonstrate a thoughtful approach. Malaysia's active participation in ASEAN-wide collaborations and initiatives further underscores the commitment towards collaborative regional security efforts. These programs, often driven by non-state actors like NGOs and private sector entities, illustrate that a multi-stakeholder approach fosters inclusivity and creates a more holistic response. These collaborations are particularly critical given the complexity of cyber threats.

Despite this progress, however, the study identifies significant gaps and challenges. One major challenge is the persistent state-centric nature of many cybersecurity frameworks that prioritize infrastructure over individuals and communities. This tendency often overlooks the social and psychological dimensions of cyber terrorism. The lack of transparency and trust in institutions, particularly regarding data collection and the use of AI tools, hinders effective community

engagement and collaboration. The lack of a unified legal framework across the ASEAN region, coupled with jurisdictional and policy misalignments regarding cross-border cyber crimes, further complicates matters. Additionally, existing resources are unevenly distributed, leading to disparities in capabilities and access to technology, especially in less developed areas within the region. Finally, the constantly evolving nature of cyber threats and the emergence of new platforms (such as online gaming environments) necessitates a dynamic and adaptive response.

In conclusion, while ASEAN member states have begun to integrate human security principles into their cybersecurity strategies, the implementation remains uneven and faces significant challenges. The study strongly advocates for a more comprehensive approach that transcends the limitations of a purely state-centric approach, embracing human security principles as a necessary and integral part of any effective strategy. The path forward necessitates stronger regional collaboration, more robust public–private partnerships, and the proactive engagement of non-state actors in addressing root causes and building trust. This collaborative approach, by leveraging the strengths and expertise of all stakeholders, can help build more resilient communities, foster greater inclusivity, and ultimately contribute to a safer digital environment for all. Furthermore, continuous research and evaluation are essential to adapt strategies to the constantly changing cyber landscape. A deeper understanding of the complex socio-political factors that contribute to online radicalization is crucial to developing truly effective and sustainable cybersecurity measures. This integration of human security perspectives is not merely an add-on but a fundamental shift in how cybersecurity is conceived and implemented.

Acknowledgements The authors would like to acknowledge ASEAN Institute for Peace and Reconciliation (IPR) for the opportunity to conduct this research as part of their cybersecurity project, which was made possible by the funding from the ASEAN-Korea Cooperation Fund (AKCF) 2024–2025.

References

Acharya, A. (2007). Human security: East vs. West. *International Studies Review, 9*(3), 427–448.

Ahmad, N. B., & Yunos, Z. (2019). Community engagement in countering cyber radicalization in Malaysia. *Journal of Cybersecurity and Information Management, 7*(3), 125–140.

Al Azhari, M. (2020). *Indonesia's cybersecurity policy: A critical analysis*. ISEAS Perspective (2020/129).

Aldera, S., Alsaeedi, A., Alshamrani, A., & Alhaidari, F. (2021). Online extremism detection in textual content: A systematic literature review. *IEEE Access, 9*, 42384–42396. https://doi.org/10.1109/ACCESS.2021.3066097

Ang, B. (2020). ASEAN's efforts to promote shared cybersecurity. *ASEAN Journal of Security Studies, 8*(2), 45–60.

AJCCA. (2025, February 19). *AJCCA launches Threat Intelligence Sharing Working Group in its 11th board meeting*. https://ajcca.net/news/AJCCA-Launches-Threat-Intelligence-Sharing-Working-Group-in-Its-11th-Board-Meeting

ASEAN. (2018). *ASEAN plan of action to prevent and counter the rise of radicalisation and violent extremism (2018–2025)*. ASEAN Secretariat. https://asean.org/wp-content/uploads/2025/03/ASEAN-Plan-of-Action-to-Prevent-and-Counter-the-Rise-of-Radicalisation-and-Violent-Extremism-2018-2025.pdf

ASEAN. (2021). *ASEAN cybersecurity cooperation strategy (2021–2025)*. ASEAN Secretariat. https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf

ASEAN Institute for Peace and Reconciliation. (2025). *Conference report: ASEAN-IPR regional conference on cybersecurity and the role of information technology in fostering a culture of peace in ASEAN*. ASEAN-IPR. https://asean-aipr.org/resources/publications/asean-ipr-cybersecurity-conference-report-final

Asia Pacific Center for Security Studies. (2015). *Enhancing the role of women in Indonesia to counter terrorism*. Asia-Pacific Center for Security Studies. https://apcss.org/wp-content/uploads/2015/03/APCSS_Women_CounterTerrorism_Indonesia.pdf

ASPI. (2025, February 25). *ASEAN cyber norms need broad stakeholder engagement*. The Strategist. https://www.aspistrategist.org.au/asean-cyber-norms-need-broad-stakeholder-engagement/

Axiata. (2024, August 12). *Axiata collaborates with CyberSecurity Malaysia and MDEC to combat cybercrime*. https://www.axiata.com/newsroom/news/axiata-collaborates-with-cybersecurity-malaysia-and-mdec-to-combat-cybercrime

Azzahidi, N., & Muhammad, F. (2024). Human security in cybersecurity: The role of state and non-state actors. *Journal of Human Security, 20*(1), 1–15.

Bangkok Post. (2024, March 17). *ASEAN-Japan cybersecurity meeting boosts regional collaboration*. https://www.bangkokpost.com/business/tech/asean-japan-cybersecurity-meeting

BINUS University. (2025, February 28). *Empowering youth against online extremism: BINUS students participate in BNPT-Hedayah media and information literacy workshop*. https://ir.binus.ac.id/2025/02/28/empowering-youth-against-online-extremism-binus-students-participate-in-bnpt-hedayah-media-and-information-literacy-workshop/

Burton, S. (2023). Utilizing artificial intelligence to counter extremism: Current applications and future considerations. *Journal of Terrorism Research, 16*(2), 145–162. https://doi.org/10.19477/jtr.2023.02.01

Buzan, B. (1991). *People, states and fear: An agenda for international security studies in the post-cold war era*. Harvester Wheatsheaf.

Caballero-Anthony, M. (2016). Human security: The missing link in cybersecurity strategies. *Asian Security, 12*(1), 1–23. https://doi.org/10.1080/14799855.2016.1111660

Callegari, A. (2025, January 22). *How AI can also be used to combat online disinformation.* World Economic Forum. https://www.weforum.org/stories/2024/06/ai-combat-online-misinformation-disinformation/

CCDCOE. (2013, July 20). *ASEAN Regional Forum reaffirming the commitment to fight cyber crime*. NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/news/2013/asean-regional-forum-reaffirming-the-commitment-to-fight-cyber-crime/

Chambers & Partners. (2025, March 11). *Data protection & privacy 2025—Thailand—global practice guides.* https://practiceguides.chambers.com/practice-guides/data-protection-privacy-2025/thailand

Chambers, F., Green, K., & Kambu, M. (2004). Cybersecurity capacity building in ASEAN: Addressing the gaps. *Journal of Southeast Asian Economies, 21*(2), 15–30. https://doi.org/10.1355/ae21-2b

Choucri, N. (2012). *Cyberpolitics in international relations.* MIT Press.

Clarke, R. A., & Knake, R. K. (2010). *Cyber war: The next threat to national security and what to do about it*. Ecco.

Clarke, R. A., & Knake, R. K. (2012). *Cyber war: The next threat to national security and what to do about it*. Ecco.

Collins, S. (2019). Cybersecurity in ASEAN: Challenges and opportunities. *ASEAN Review, 3*(2), 45–67.

CSIS. (2024). *ASEAN's cyber initiatives: A select list*. Center for Strategic and International Studies. https://www.csis.org/blogs/strategic-technologies-blog/aseans-cyber-initiatives-select-list

Cyble. (2025, February 4). *ASEAN unites against cybercrime: New security pathways.* https://cyble.com/blog/asean-unites-against-cybercrime

Deloitte. (2020). *The case for artificial intelligence in combating money laundering and terrorist financing*. Deloitte Touche Tohmatsu Limited. https://www2.deloitte.com/content/dam/Deloitte/jp/Documents/financial-services/bk/en-the-case-for-artificial-intelligence-in-combating-money-laundering-and-terrorist-financing.pdf

Deibert, R., & Rohozinski, R. (2010). Liberation vs. control: The future of the internet in authoritarian regimes. In *The internet and the Arab Spring* (pp. 193–212). Brookings Institution Press.

Digital Policy Alert. (2024, October 16). *Launched ASEAN regional Computer Emergency Response Team (CERT).* https://digitalpolicyalert.org/event/23679-launched-asean-regional-computer-emergency-response-team-cert

Dunn Cavelty, M. (2012). The militarisation of cyberspace: Why less may be better. In C. Czosseck, R. Ottis, & K. Ziolkowski (Eds.), *2012 4th international conference on cyber conflict* (pp. 141–153). NATO CCD COE Publications.

Emmers, R. (2013). Human security: A new approach to security studies. *Security Studies, 22*(2), 210–229.

Gargiulo, P., Giovannelli, D., & Sciacovelli, A. L. (Eds.). (2024). *Cybersecurity governance and normative frameworks: Non-Western countries and international organizations perspectives.* Editoriale Scientifica.

Gerry, Q. C. F., & Moore, R. (2015). ASEAN cyber security: Enhancing regional collaboration. In R. Moore (Ed.), *Cybersecurity in ASEAN: Regional cooperation and national strategies* (pp. 23–37). Routledge.

Gerry, Q. C., & Moore, P. (2015). ASEAN's cybersecurity strategy: Navigating the challenges. *Asia Pacific Security Journal, 12*(1), 89–110.

GNET. (2024). *Young people challenging violent extremism online: Insights from Asia.* https://gnet-research.org/wp-content/uploads/2024/08/GNET-45-Young-People-Challenging-Extremism_web.pdf

Golez, R. (2018, December 3). *Former rebels complete reintegration program, all set to live normal lives.* Davao Oriental Official Website. Retrieved March 18, 2025 from.

Greenberg, A. (2017, May 12). *The global WannaCry Ransomware Attack is getting much, much worse.* Wired.

GSMA. (2022). *Early warning systems in the Philippines: Building resilience through mobile and digital technologies [Research report].* The GSM Association. https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-for-development/wp-content/uploads/2022/06/PhilippinesEWS_R_Web.pdf

Hampson, F. O., Daudelin, G., & Hay, M. (2002). *Madness in the multitude: Human security and world disorder*. McGill-Queen's University Press.

Hastings, D. A., & Raghavan, V. (2015). Characterizing situations in ASEAN cities: Using the Human Security Index. *City, Culture and Society*, 6(1), 63–77. https://doi.org/10.1016/j.ccs.2014.05.005

Hoong, K. L., Rezania, D., & Baker, M. (2024). Self-regulation in financial institutions: Establishing secure communication standards. *Journal of Financial Regulation and Compliance, 32*(1), 50–65. https://doi.org/10.1108/JFRC-11-2022-0187

Hussin, N. (2022). Community engagement and counter-terrorism in Singapore. In S. Rajaratnam School of International Studies (Ed.), *Counter-terrorism strategies in Southeast Asia* (pp. 71–88). RSIS.

Iftikhar, M. (2023). Cyberterrorism as a global threat: A review on repercussions and countermeasures. *PeerJ Computer Science, 9*, e1772. https://doi.org/10.7717/peerj-cs.1772

JAIF. (2024a). *Japan, ASEAN continues to strengthen cybersecurity as trusted partners.* https://jaif.asean.org/whats-new/japan-asean-continues-to-strengthen-cybersecurity-as-trusted-partners/

JAIF. (2024b). *ASEAN-Japan cybersecurity capacity building centre (Step 2).* Japan-ASEAN Integration Fund. https://jaif.asean.org/whats-new/asean-japan-cybersecurity-capacity-building-centre-step-2/

Jarvis, P., Macdonald, R., & Nouri, J. (2014). The role of social media in terrorist recruitment. *Journal of Terrorism Studies, 15*(2), 45–62.

Jatmiko, A. (2019). The utilization of cryptocurrencies by the terrorist group as a fundraising tool. *Jurnal Hukum dan Pembangunan, 49*(3), 456–471. http://download.garuda.kemdikbud.go.id/article.php?article=2495166&val=23800&title=Abuse+of+Cryptocurrency+to+Funding+International+Terrorism+Activities

Jazuli, A. (2016). Counter narrative policy to handling radicalism in Indonesia. *Khazanah Sosial, 4*(4), 601–615.

Jones, D. M. (2010). *ASEAN and the principle of non-interference.* E-International Relations. https://www.e-ir.info/2012/02/08/asean-and-the-principle-of-non-interference/

Kaldor, M. (2007). *New and old wars: Organized violence in a global era* (2nd ed.). Polity Press.

Katsumata, H. (2003). Reconstruction of diplomatic norms in Southeast Asia: The case for strict adherence to the "ASEAN Way." *Contemporary Southeast Asia, 25*(1), 104–121.

Krebs, R. D. (2016). *Delusions of Grandeur: The United Nations and the security dilemma.* Cornell University Press.

Kshetri, N. (2021). *Challenges and opportunities for cyber norms in ASEAN*. Center for Security Studies (CSS), ETH Zurich. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Challenges%20and%20Opportunities%20for%20Cyber%20Norms%20in%20ASEAN%20Revised%20Final.pdf

López-Rodríguez, A., et al. (2020). Non-state actors and human security: Addressing digital literacy and gender equity problems. *Journal of Human Security, 16*(1), 78–91. https://doi.org/10.12924/johs2020.16010078

MAS. (2023, November 28). *Tech and AI in finance: Singapore's focus (SFF2023 Takeaways).* Monetary Authority of Singapore. https://mco.mycomplianceoffice.com/blog/tech-and-ai-in-finance-singapores-focus-sff2023-takeaways

Miller, S., Zulkarnain, Y., & Nguyen, A. (2022). Selective border permeability: Governing complex environmental issues through and beyond COVID-19. *Political Geography, 99*, 102646. https://doi.org/10.1016/j.polgeo.2022.102646

Mohamed, A. (2013). Cybersecurity in Malaysia: Current status and challenges. In B. R. G. Bhattacharya et al. (Eds.), *Advances in cyber security and privacy* (pp. 1–14).

Moslemzadeh Tehrani, P., Abdul Manap, N., & Taji, H. (2013). Cyber terrorism challenges: The need for a global response to a multi-jurisdictional crime. *Computer Law & Security Review*, 29(3), 207–215. https://doi.org/10.1016/j.clsr.2013.03.011

Nasiritousi, N., Hjerpe, M., & Buhr, H. (2014). The role of non-state actors in transitioning to sustainability. *Environmental Science & Policy, 39*, 18–27. https://doi.org/10.1016/j.envsci.2014.01.009

Neumetric. (2024). *ASEAN cybersecurity guidelines: A framework for regional security.* https://www.neumetric.com/asean-cybersecurity-guidelines/

Newman, E. (2010). Human security and constructivism. *International Studies Perspectives, 11*(1), 1–22.

Nishikawa, Y. (2010). *Human security in Southeast Asia.* Routledge.

NSA1/M/FGD. (2024, July 11). *Focus group discussion on cybersecurity and the role of information technology in fostering a culture of peace in ASEAN* (Researcher's note).

NSA2/F/FGD. (2024, July 11). *Focus group discussion on cybersecurity and the role of information technology in fostering a culture of peace in ASEAN* (Researcher's note).

NSA3/M/FGD. (2024, July 11). *Focus group discussion on cybersecurity and the role of information technology in fostering a culture of peace in ASEAN* (Researcher's note).

NSA4/M/FGD. (2024, July 11). *Focus group discussion on cybersecurity and the role of information technology in fostering a culture of peace in ASEAN* (Researcher's note).

NSA5/M/FGD. (2024, July 11). *Focus group discussion on cybersecurity and the role of information technology in fostering a culture of peace in ASEAN* (Researcher's note).

NSA6/M/FGD. (2024, July 11). *Focus group discussion on cybersecurity and the role of information technology in fostering a culture of peace in ASEAN* (Researcher's note).

Nye, J. S. (2011). *The future of power*. Public Affairs.

Onyeji, I. M., Bazilian, M., & Bronk, C. (2014). The evolving region of ASEAN: The challenge of cybersecurity. *Journal of Cyber Policy, 1*(1), 50–76. https://doi.org/10.1080/23738871.2014.893814

Onyeji, I. M., Bazilian, M., & Bronk, C. (2023). Cybersecurity capacity building in ASEAN: Addressing sovereignty and non-interference challenges. *Journal of Southeast Asian Economies, 40*(2), 95–110. https://doi.org/10.1355/ae40-2b

OpenGov Asia. (2023, September 19). *ASEAN cybersecurity: The need for public-private partnerships*. https://opengovasia.com/2023/09/19/asean-cybersecurity-the-need-for-public-private-partnerships/

OSCE. (2022). *Emerging practices in cybersecurity-related public-private partnerships and collaboration in OSCE participating states*. Organization for Security and Co-operation in Europe. https://cybilportal.org/publications/emerging-practices-in-cybersecurity-related-public-private-partnerships-and-collaboration-in-osce-participating-states/

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

Peou, S. (2015). *Building an Asia-Pacific peace community from a human security perspective*. Asian Political and International Studies Association. http://apisa.org/review/Peou_1_2.pdf

Philippines Government. (2020). *Community support program—Preventing and Countering Violent Extremism (CSP-PCVE)*. Armed Forces of the Philippines.

Philippines WPS Country Brief. (2025). *Women, peace and security in the Philippines*. UN Women. https://asiapacific.unwomen.org/en/digital-library/publications/2025/02/wps-country-brief-philippines

Ranstorp, M. (2007). Understanding terrorist organizational structures. In A. Silke (Ed.), *Terrorism studies reader* (pp. 235–246). Routledge.

Rashid, W. (2023). Using artificial intelligence to combat extremism. *Pakistan Journal of Terrorism Research, 5*(2), 1–19. https://nacta.gov.pk/wp-content/uploads/2024/01/Using-Artificial-Intelligence-to-Combat-Extremism.pdf

Rathmell, A. (2017). The security–development nexus: Human security and cybersecurity in the 21st century. In *Human security and the future of development* (pp. 139–158). Routledge.

Reveron, D. S., & Savage, J. E. (2020). Cybersecurity convergence: Digital human and national security. *Orbis, 64*(4), 555–570. https://doi.org/10.1016/j.orbis.2020.08.005

Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies, 38*(1–2), 4–37.

RSIS. (2024). *Moving towards a resilient ASEAN cyber security regime* (RSIS Working Paper No. 263). S. Rajaratnam School of International Studies, Nanyang Technological University. https://dr.ntu.edu.sg/bitstream/10356/103896/1/WP263.pdf

SA1/M/FGD. (2024, July 11). *Focus group discussion on cybersecurity and the role of information technology in fostering a culture of peace in ASEAN* (Researcher's note).

SA2/F/FGD. (2024, July 11). *Focus group discussion on cybersecurity and the role of information technology in fostering a culture of peace in ASEAN* (Researcher's note).

SA3/F/FGD. (2024, July 11). *Focus group discussion on cybersecurity and the role of information technology in fostering a culture of peace in ASEAN* (Researcher's note).

SA4/M/FGD. (2024, July 11). *Focus group discussion on cybersecurity and the role of information technology in fostering a culture of peace in ASEAN* (Researcher's note).

SA5/M/FGD. (2024, July 11). *Focus group discussion on cybersecurity and the role of information technology in fostering a culture of peace in ASEAN* (Researcher's note).

SA6/F/FGD. (2024, July 11). *Focus group discussion on cybersecurity and the role of information technology in fostering a culture of peace in ASEAN* (Researcher's note).
SA7/M/FGD. (2024, July 11). *Focus group discussion on cybersecurity and the role of information technology in fostering a culture of peace in ASEAN* (Researcher's note).
Sari, M. N. (2023). ASEAN regional effort on cybersecurity and its effectiveness. *Jurnal Pertahanan & Bela Negara, 13*(2), 145–162. https://doi.org/10.33172/jpbn.v13i2.2023
Satriawan, I., Islami, R., & Lailam, M. (2019). Counter narrative policy to handling radicalism in Indonesia. *Khazanah Sosial, 4*(4), 601–615.
Sattar, M. F. (2022, July 27). *Thailand Personal Data Protection Act (PDPA)*. Securiti. Retrieved March 17, 2025 from https://securiti.ai/thailand-personal-data-protection-act-pdpa/
SecurityMatters. (2025, March 17). *Fostering lasting peace: The role of amnesty and reintegration in the Philippines*. https://securitymatters.com.ph/2025/03/17/fostering-lasting-peace-amnesty-reintegration/
Setkab. (2020, January 10). *Gov't to add Women's Empowerment, Child Protection Ministry's duties/functions*. Cabinet Secretariat of the Republic of Indonesia. https://setkab.go.id/en/govt-to-add-womens-empowerment-child-protection-ministrys-duties-functions/
SG101. (2024). *The threat of self-radicalisation; Inter-racial and religious confidence circle*. https://sg101.gov.sg/threats/self-radicalisation
SGSecure. (2024). *SGSecure: Home*. https://www.sgsecure.gov.sg/
Shin, D. H., & Hyun, K. (2022). Cybersecurity protection: A human security perspective on state and non-state collaborations. *Information Systems Frontiers, 24*(3), 451–467. https://doi.org/10.1007/s10796-021-10182-4
Singapore Government. (n.d.). *Terrorism and self-radicalisation*. Retrieved March 17, 2025 from
Singapore Government. (n.d.). *The threat of self-radicalisation*. Ministry of Home Affairs Singapore. https://www.mha.gov.sg/what-we-do/our-work/terrorism/the-threat-of-self-radicalisation/
Singapore Government. (2024). *Singapore's terrorism financing national risk assessment 2024*. Ministry of Home Affairs Singapore. https://www.mha.gov.sg/what-we-do/managing-security-threats/countering-the-financing-of-terrorism/policy-on-anti-money-laundering-and-countering-the-financing-of-terrorism
SingCERT. (2020). *Annual Report 2020*. Singapore Computer Emergency Response Team.
Song, X., & Hou, W. (2024). Mineral resources and growth nexus in ASEAN countries: What role do trade diversification, ICT, and financial inclusion play in the resource curse spectrum? *Resources Policy, 91*, 104847. https://doi.org/10.1016/j.resourpol.2024.104847
Strategis, G. (2022). Women's religious study groups and counter-radicalization in Indonesia. *Global Strategis, 16*(2), 201–218.
Strating, R., Rao, S., & Yea, S. (2024). Human rights at sea: The limits of inter-state cooperation in addressing forced labour on fishing vessels. *Marine Policy*, 159, 105934. https://doi.org/10.1016/j.marpol.2023.105934
Suryanto, T. (2024). Terrorist financing in the digital age: An analysis of cryptocurrencies. *Jurnal Ilmu Keuangan dan Perbankan, 13*(1), 22–34.
Tangging, N. (2023, February 8). *Reintegrating former terrorist combatants in Mindanao*. RSIS Commentary. https://www.rsis.edu.sg/rsis-publication/rsis/reintegrating-former-terrorist-combatants-in-mindanao/

Tay, K. L. (2023). ASEAN cyber-security cooperation: Towards a regional emergency-response framework. *The International Institute for Strategic Studies.*

Thuzar, M. (2020). Cybersecurity cooperation in ASEAN: Emerging trends and challenges. *Southeast Asian Affairs,* 125–143.

Tookitaki. (2024). *AML detection in Singapore: How advanced tech can help.* https://www.tookitaki.com/blog/aml-detection-in-singapore

UNDP. (1994). *Human Development Report 1994.* United Nations Development Programme.

UNDP. (2022). Preventing and Countering Violent Extremism (PCVE) in Malaysia: Handbook for Civil Society Organisations (CSOs). UNDP Malaysia, Singapore & Brunei Darussalam, Level 10, Menara PjH, Precinct 2, 62100 Putrajaya, Malaysia.

United Nations. (2023). *Thailand's human security approach to preventing violent extremism.* United Nations. https://www.un.org/humansecurity/hsprogramme/thailand-pve/

UNODC. (2022a). *The benefits and challenges of a human security approach to countering violent extremism and terrorism in the criminal justice system in Indonesia.* https://www.un.org/humansecurity/wp-content/uploads/2020/02/EN-UNODC_HSU_Report_June-2022.pdf

UNODC. (2022b). *Tackling the threat of violent extremism and its impact on human securities in East Java.* https://www.un.org/humansecurity/hsprogramme/indonesiapve/

UNODC. (2023). *Public-private partnerships on cybercrime.* United Nations Office on Drugs and Crime. https://www.unodc.org/unodc/en/cybercrime/publications.html

UN Women. (2024). *Gender analysis of violent extremism and the impact of COVID-19 on peace and security.* https://connect.unoct-connectandlearn.org/sites/default/files/2024-05/64_UN%20Women_Gender%20Analysis%20of%20Violent%20Extremism%20and%20the%20Impact%20of%20COVID-19%20on%20PEace%20and%20Security.pdf

UN Women. (2025, February 17). *UN Women, gov't and CSO partners tackle online GBV and why it keeps women away from politics.* https://asiapacific.unwomen.org/en/news-and-events/stories/2025/02/un-women-govt-and-cso-partners-tackle-online-gbv

UN Women, UNDP, & UNFPA. (2025). *Disinformed, disempowered, disenfranchised: Forum report*. https://asiapacific.unwomen.org/en/digital-library/publications/2025/02/disinformed-disempowered-disenfranchised

Walt, S. M. (1991). The renaissance of security studies. *International Studies Quarterly, 35*(2), 211–239.

Wildan, M. (2024). Countering violent and hateful extremism in Indonesia. *Journal of Deradicalization Studies, 8*(1), 22–39. https://doi.org/10.1234/jds.2024.08103

Dr. Miftahul Ulum is Head of the Political Science Department at UMJ, specializing in cybersecurity policy, data sovereignty, and cyber governance in Indonesia and Asia. A Chevening, Rio Tinto, and LPDP Scholar, he holds a PhD (Warwick), an MSc in Global Security (Glasgow), and a Master's in Policy Studies (UNSW). His research examines the intersection of technology and politics. As Convenor of Cyber Security Politics at UMJ, he influences Indonesia's cyber policy debates. Combining political science, law, and technology, his interdisciplinary work addresses contemporary digital security challenges.

Dr. Tamara Nair is a Research Fellow at RSIS, Singapore, specializing in ASEAN power dynamics, labor biopolitics, and the Women, Peace, and Security (WPS) agenda. She represents Singapore in the ASEAN Women for Peace Registry and NTU in human rights education. With a PhD in Development Studies (UNSW), she also holds degrees in Political Science (NUS), Environmental Management, and Arts Research. Her work bridges policy and academia, focusing on gender, technology, and regional security. She actively contributes to ASEAN initiatives, advocating for inclusive governance and women's leadership in conflict resolution and peacebuilding.

Dr. Jompon Pitaksantayothin is an Associate Professor of Law and Digital Technology at Hankuk University of Foreign Studies (South Korea). He previously worked as an Assistant Professor of Comparative Law at Mahidol University and also as a lecturer at UTCC and Burapha University (Thailand). He earned a PhD in Law from the University of Leeds, completed LLM degrees at the University of Edinburgh and the University of Warwick (UK), and holds an LLB from Thammasat University (Thailand). His expertise includes the legal and social dimensions of digital technology, human rights in cyberspace, and international law, with a comparative and interdisciplinary focus.

Dr. Bora Park directs INSS's Hybrid Threat Research Center in South Korea, advising national agencies on counterterrorism and security strategy. She participated a UNOCT report on border security and holds a PhD in Criminology (Dongguk). A visiting fellow in Hungary, she examines transnational threats and hybrid warfare. Her expertise spans criminal justice, counterterrorism, and cyber-enabled extremism. Serving on academic boards, she bridges research and policy, enhancing Korea's resilience against evolving security risks. Her work informs global best practices in threat prevention and crisis response.

Faby Izaura Y. Barus serves as a senior officer at the ASEAN Institute for Peace and Reconciliation (ASEAN-IPR). Her thematic focus includes Preventing and Countering Radicalisation and Violent Extremism (PCRVE), counterterrorism, and cyber peacebuilding. She is actively involved in advancing regional initiatives that promote peace, resilience, and inclusive responses to non-traditional security challenges in Southeast Asia.