ASEAN-KOREA COOPERATION FUND
한 - 아세안 협력기금

CYBER CON 2025

Forging and Fostering Peace
ASEAN Institute for Peace and Reconciliation



FOCUS GROUP DISCUSSION (FGD) ON

"Cybersecurity and the Role of Information Technology in Fostering a Culture of Peace in ASEAN"

FGD REPORT 2024

Focus Group Discussion (FGD) Report on Cybersecurity and the Role of Information Technology in Fostering a Culture of Peace in ASEAN

ASEAN Institute for Peace and Reconciliation (ASEAN-IPR)
Jakarta

Focus Group Discussion (FGD) Report on Cybersecurity and the Role of Information Technology in Fostering a Culture of Peace in ASEAN

Publisher:
ASEAN Institute for Peace and Reconciliation

Authors:
Tamara Nair
Miftahul Ulum
Jompon Pitaksantayothim
Bora Park
Faby Izaura Y Barus

Book Designer:
Audreysha Zalfa (ODD2E1)
Bayu Wicaksono

First Published in 2025

Forging and Fostering Peace
ASEAN Institute for Peace and Reconciliation

WHAT IS

ASEAN-IPR?

The ASEAN Institute for Peace and Reconciliation (ASEAN-IPR) is an ASEAN think tank. The Institute's establishment started on 8 May 2011, at the 18th ASEAN Summit, where the ASEAN Leaders adopted a "Joint Statement on the Establishment of an ASEAN Institute for Peace and Reconciliation". The Statement was in pursuit of an action line under Provision B.2.2.i of the ASEAN Political-Security Community (APSC) Blueprint (2010-2015), which aims to "strengthen research activities on peace, conflict management and conflict resolution".

The following year, at the 45th ASEAN Foreign Ministers Meeting (AMM) in July 2012, the Institute's terms of reference (TOR) was adopted, making way for the Institute's official launch – and thus now known as the date of birth of the Institute – on 18 November 2012 during the 21st ASEAN Summit in Phnom Penh, Cambodia, with the Chairman's Statement paragraph 15 stating:

"We emphasised the importance of promoting conflict resolution and conflict management to enhance peace, security and stability in the region. We, therefore recalled our decision at the 10th ASEAN Summit in Bali, Indonesia, on 17 November 2011, to establish the ASEAN Institute for Peace and Reconciliation. We welcomed the endorsement of the Terms of Reference of the ASEAN Institute for Peace and Reconciliation by the ASEAN Foreign Ministers Meeting in July 2012 and agreed to officially launch the Institute on this 18th November 2012, in Phnom Penh, at the sidelines of our 21st ASEAN Summit. We looked forward to the full and effective operationalization of the Institute so as to contribute to the interest of ASEAN in this regard."

The Institute's legal personality is established under a Host Country Agreement with the Government of the Republic of Indonesia, granting the ASEAN-IPR's privileges and immunities, which was signed on 1 February 2018.

As stipulated in its Terms of Reference (TOR), available as ANNEX 1, ASEAN-IPR is mandated to be ASEAN's institution dedicated for research activities, and supporting ASEAN bodies, on peace, reconciliation, conflict management and conflict resolution. Additionally, the Institute is also called

to promote activities agreed in the APSC Blueprint, and additional activities as agreed by ASEAN Member States. Accordingly, ASEAN-IPR has been assigned to be one of the implementers of 10 Action Lines under the APSC Blueprint 2025.

Pursuant to its mandate, ASEAN-IPR functions to undertake the following activities:

1. RESEARCH

Compile ASEAN's experiences and best practices on peace processes, with the view of providing appropriate recommendations to ASEAN bodies and enhance regional mechanisms.

2. CAPACITY BUILDING

Knowledge building on peace processes for all stakeholders.

3. POOL OF EXPERTISE AND SUPPORT FOR ASEAN BODIES

Develop a pool of experts to assist ASEAN (governments and/or Bodies) in conflict management, provide policy recommendations, as well as facilitation for peace negotiations.

4. NETWORKING

Establish linkages with like-minded institutions and organisations in ASEAN Member States, as well as other region, and at the international level with similar objectives aimed at promoting culture of peace.

5. DISSEMINATION OF INFORMATION

Disseminate best practices, lessons learned, relevant information to ASEAN Member States, other relevant stakeholders, as well as the general public; including outreach and engagement and promote awareness on the work of the Institute.

Against such background, the ASEAN Institute for Peace and Reconciliation has been envisioned to be ASEAN's knowledge hub and centre of excellence in building capacity on conflict resolution and reconciliation and further strengthening peace-oriented values towards harmony, peace, security and stability in the region and beyond.



Acknowledgement

ASEAN-IPR extends its sincere gratitude to all stakeholders who generously contributed their time, insights, and expertise during the focus group discussions and virtual expert meetings that shaped this project.

The Editors

1. **Dr. Tamara Nair** – Research Fellow, Centre for Non-Traditional Security Studies (NTS Centre), S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University, Singapore.
2. **Dr. Miftahul Ulum** – Senior GTA, Department of Politics and International Studies, University of Warwick; Lecturer, Department of Politics, University of Muhammadiyah Jakarta, Indonesia.
3. **Dr. Jompon Pitaksantayothin** – Associate Professor, Information Technology Law, Division of International Studies, Hankuk University of Foreign Studies (HUFS), Thailand.
4. **Dr. Bora Park** – Research Fellow, Department of Emerging Security Studies, Institute for National Security Strategy (INSS), Republic of Korea.
5. **Ms. Faby Izaura Y. Barus** – ASEAN Institute for Peace and Reconciliation, Indonesia.

The Focus Group Discussion (FGD) on “Cybersecurity and the Role of Information Technology in Fostering a Culture of Peace in ASEAN” is supported by the ASEAN-Korea Cooperation Fund (AKCF) and implemented by the ASEAN-IPR Secretariat

The opinions expressed in this publication are solely those of the author and do not necessarily reflect the views or officials policies of the Government of the Republic of Korea.

All facts, viewpoints, and interpretations presented in this report are the exclusive responsibility of the authors and do not represent the institutional stance of ASEAN-IPR, its governing board, staff, or affiliated partners.



Published : January 2025
Copyright © 2025 by ASEAN Institute for Peace and Reconciliation (ASEAN-IPR)

All rights reserved. This book, or parts thereof, may not be reproduced in any form or by any means, electronic or mechanical, including photocopying, recording or any information storage and retrieval system now known or to be invented, without written permission from the publisher.

Printed in Indonesia

Foreword

As Ambassador of the Republic of Korea Mission to ASEAN, I am privileged to contribute to this report on the Focus Group Discussion (FGD) titled "Cybersecurity and the Role of Information Technology in Fostering a Culture of Peace in ASEAN." I would first like to express my appreciation to the ASEAN-IPR for initiating this program which will play a meaningful role in building a safer and more inclusive digital future of the region. The Republic of Korea is happy to work with the ASEAN-IPR on this important initiative by supporting through the ASEAN-Korea Cooperation Fund (AKCF).

The relationship between ASEAN and ROK has witnessed significant progress in every aspect since establishing the dialogue partnership in 1989. It was culminated by the introduction of the Korea-ASEAN Solidarity Initiative (KASI) in 2022 and establishment of the Comprehensive Strategic Partnership (CSP) in 2024 in celebration of the 35th anniversary of the partnership. The ROK Government proved its genuine commitment to strengthening the partnership by significantly increasing its yearly contribution to the ASEAN-Korea Cooperation Fund (AKCF) from 14 million USD in 2019 to 28 million USD in 2024.

Cybersecurity is one of the priority areas to which the ROK Government is working with ASEAN through the AKCF. In addition to the FGD project, Korea has been also funding the ASEAN Cyber Shield Hacking Contest and a project to enhance the Cybersecurity of the ASEAN Secretariat. Financing these cybersecurity projects through AKCF demonstrates ROK's commitment to enhancing the ASEAN centrality in navigating the evolving cybersecurity landscape in the region, empowering stakeholders to leverage technology for peacebuilding, and ensuring that the benefits of digital transformation are equitably shared among all.

The FGD represents an essential initial step in realising the goals of the ASEAN-IPR Regional Conference on Cybersecurity and the Role of Information Technology in Fostering a Culture of Peace, to be held in Bangkok, Thailand, in February 2025. The FGD also underscores the critical intersection of cybersecurity and peacebuilding—fundamental to fostering regional stability and prosperity. By addressing issues such as human security in cyberspace, the gender impacts of technology, and the threats posed by radicalisation and political polarisation, this project will lay the groundwork to advance ASEAN's regional security objectives.

These cybersecurity events resonate deeply with the goals set out in the KASI and the Joint Statement on the Establishment of the ASEAN-ROK Comprehensive Strategic Partnership, prioritising building a comprehensive and forward-looking partnership with ASEAN under the Republic of Korea's Indo-Pacific Strategy. These core documents of the ROK-ASEAN partnership have highlighted the importance of the non-traditional security cooperation, particularly in addressing emerging challenges in the use of technology. I believe that this FGD exemplifies the synergy between ASEAN and ROK's shared aspirations for a digitally connected, safe, peaceful, and resilient region.

I commend the ASEAN-IPR for its commitment to hosting this important dialogue and the ROK Institute for National Security Strategy for its engagement and cooperation. I also express my gratitude to all participants and contributors for their invaluable insights. Let this report inspire further collaboration and innovation as we work toward our shared vision of a secure, technologically advanced, inclusive and harmonious ASEAN.



Amb. Lee Jang-keun

Ambassador of the
Republic of Korea (ROK) to ASEAN

Foreword

I welcome this important and comprehensive report of the ASEAN-IPR Focus Group Discussion (FGD) on Cybersecurity and the Role of Information Technology in Fostering a Culture of Peace, which was organised on 11-12 July 2024 in Jakarta. This event gathered experts and stakeholders across the ASEAN region to deliberate on the intricacies of cybersecurity and its intersection with peacebuilding.

The primary goal of this FGD was to deepen our understanding of the current cybersecurity landscape within ASEAN. This understanding is crucial as we navigate the challenges posed by emerging threats to critical infrastructure and human security. By identifying specific cybersecurity challenges that impact peace, we aim to forge pathways that not only respond to these threats but also bolster our collective security.

To address these challenges, this FGD emphasized the need for a comprehensive strategy that begins with foundational elements: knowledge sharing, dialogue, and meaningful discussions. These elements are essential for building a cohesive and effective regional response. Over the course of our discussions, the experts explored innovative solutions and strategies that leverage cybersecurity and information technology to enhance our peace efforts. The insights gathered from these discussions are intended to inform and inspire actionable strategies that can be adopted across ASEAN member states and beyond.

The Focus Group Discussion (FGD) and its series of related activities represent an important initial step in supporting the implementation of the ASEAN-IPR Regional Conference on Cybersecurity and the Role of Information Technology in Fostering a Culture of Peace, to be organized in Bangkok, Thailand in February 2025. These activities not only provide a platform for sharing insights and experiences but also serve as part of ASEAN-IPR's effort to explore the concept of cyber peacebuilding. This concept underscores the importance of integrating peacebuilding efforts into the digital domain within the cybersecurity framework. As an institution dedicated to research and capacity building in peace, security, and reconciliation, ASEAN-IPR believes that a holistic approach involving diverse stakeholders is key to realising a peaceful and secure ASEAN region, both in the physical and digital realms.

This FGD was made possible through the generous support of the ASEAN-Korea Cooperation Fund (AKCF) and the Mission of the Republic of Korea to ASEAN in Jakarta. Their commitment to fostering regional security and peacebuilding has been instrumental in advancing our shared goals.

As we move forward, let this report serve not only as a record of our discussions but as a beacon guiding our collective efforts in cybersecurity and peacebuilding. I extend my gratitude to all participants and organizers who made this FGD a fruitful endeavour. Together, let us continue to work towards a secure, peaceful, and resilient ASEAN.

I Gusti Agung Wesaka Puja

Executive Director of
ASEAN Institute for Peace and Reconciliation
(ASEAN-IPR)



Contents

About ASEAN-IPR i

Acknowledgment iii

Foreword v

Abbreviation viii

Executive Summary 1

Introduction 3

Agenda and Sessions 6

Session 1 : Cybersecurity and Peacebuilding – Understanding the Landscape 7

Session 2 : IT's Dual Role in War and Peace 16

Session 3: Gender and Human Rights – Approaches to Cybersecurity 21

Session 4: Cybersecurity and Radicalization 26

Session 5: Social Media's Effect on Political Polarization 30

Summary of Finding and Moving Forward 34

Differing Viewpoints 41

Potential topics/themes for Cybersecurity Conference 2025 42

Recommendations 44

Annex I 47

Annex II 49

Abbreviation

AB	Advisory Board
AI	Artificial Intelligence
AMS	ASEAN Member States
APT	Advanced Persistent Threats
AR	Augmented Reality
ASEAN	Association of Southeast Asian Nation
ASEAN-IPR	ASEAN Institute for Peace and Reconciliation
CBM	Confidence Building Measures
CEDAW	Convention on the Elimination of All Forms of Discrimination Against Women
CIA	Confidentiality, Integrity, Availability
CSO	Civil Society Organization
EWS	Early Warning System
FGD	Focus Group Discussion
GBV	Gender-based Violence
GC	Governing Council
ISP	Internet Service Providers
IT	Information Technology
LGBTQ	Lesbian, Gay, Bisexual, Transgender and Queer
NAP	National Action Plan
NGO	Non-governmental Organization
OPAPRU	Office of the Presidential Adviser on Peace, Reconciliation and Unity
RAP	Regional Action Plan
STEM	Science, Technology, Engineering and Mathematics
UN	United Nations
VR	Virtual Reality
WPS	Women, Peace and Security



EXECUTIVE SUMMARY

The Focus Group Discussion (FGD) on "Cybersecurity and the Role of Information Technology in Fostering a Culture of Peace in ASEAN" was held on July 11-12, 2024, at Ascott Sudirman, Jakarta, Indonesia. The primary objectives were to gain a comprehensive understanding of how cybersecurity impacts peacebuilding efforts in ASEAN member states to identify key cybersecurity challenges and opportunities that affect peace and conflict in the region and develop actionable insights and policy recommendations to integrate cybersecurity into peacebuilding frameworks. The assertion that cybersecurity significantly impacts peacebuilding efforts in ASEAN member states is grounded in the complex interplay of challenges and opportunities arising from the region's unique geopolitical landscape. Integrating cybersecurity into peacebuilding frameworks is not only relevant but essential for fostering stability and security in the region. The cybersecurity landscape in ASEAN is characterized by various challenges, including the increasing frequency and sophistication of cyber threats.

Key discussions during the five FGD sessions highlighted various aspects of cybersecurity and peacebuilding in the region. A detailed agenda for the FGD sessions is provided in Annex 1. The first session *Cybersecurity and Peacebuilding* emphasized the importance of expanding the definition of cybersecurity to include human security, the role of cybersecurity in creating safe dialogue spaces and ensuring trust in peace processes, and the geopolitical implications of cybersecurity alongside the importance of international law. The session on *IT's Dual Role in War and Peace* explored the neutral nature of IT and its potential as both a tool for conflict as well as peace, strategies for leveraging IT for peacebuilding, including digital literacy and community engagement, and the importance of collaboration between peacemakers and IT developers. In the *Gender and Human Rights – Approaches to Cybersecurity* session, discussions centered on the gendered impact of cybersecurity policies and the need for gender-sensitive approaches, addressing online harassment and gender-based violence, and creating safe digital spaces while encouraging women's participation in cybersecurity and peacebuilding. In the session on *Cybersecurity and Radicalization*, the discussion highlighted the complex relationship between the internet, social media, gaming platforms, and radicalization. The final session on *Social Media's Effect on Political Polarization* highlighted the role of social media in exacerbating political polarization and spreading misinformation, and also included strategies to mitigate the negative effects of social media, including media literacy programs and regulatory oversight.

The FGD yielded several key outcomes and recommendations. Policy recommendations include the development of comprehensive cybersecurity policies that incorporate human security aspects, the promotion of gender-sensitive cybersecurity practices, and the implementation of media literacy programs while holding social media companies accountable for their algorithms. Specific recommendations from participants highlighted the need for a binding cybersecurity mechanism for ASEAN, addressing disparities in cybersecurity maturity among member states, and enhancing international cooperation to tackle cross-border cyber threats. There were also calls for strengthening legal frameworks, improving public-private collaboration, and fostering capacity-building programs to develop a skilled cybersecurity workforce.

Regarding collaboration and capacity building, the FGD emphasized fostering regional cooperation to enhance cybersecurity and peacebuilding efforts and encouraging collaboration between governments, the private sector, and civil society to address cybersecurity challenges. The importance of public-private partnerships and the role of civil society in raising awareness and advocating for stronger cybersecurity policies were underscored. Innovative solutions included leveraging digital tools and AI for peacebuilding and defensive purposes and exploring the potential of IT to create inclusive and resilient communities. Participants recommended investing in advanced technologies such as artificial intelligence, machine learning, and blockchain for proactive threat detection and secure transactions.

The FGD is a critical precursor to the ASEAN-IPR Regional Conference on Cybersecurity and the Role of Information Technology in Fostering a Culture of Peace in ASEAN. It provided a platform for multidisciplinary dialogue, informed the main conference discussions, and contributed to shaping the regional cybersecurity agenda. The insights and recommendations from the FGD are expected to guide future actions and enhance the integration of cybersecurity into peacebuilding initiatives across ASEAN member states.

INTRODUCTION

In 2020, the Governing Council of ASEAN-IPR endorsed a Concept Note on the "ASEAN Institute for Peace & Reconciliation (ASEAN-IPR) Focus Group Discussion (FGD)" during their 18th Meeting. The idea for an FGD first surfaced during an Interface Meeting between the Governing Council (GC) and the Advisory Board (AB) of the Institute, which recommended: (i) the AB to identify and draw up a list of Think Tanks and/or Track 2 institutions in each ASEAN Member State relevant to the work of ASEAN-IPR, which the Institute could potentially work with; and (ii) convene dialogue sessions with such institutions to share information about the ASEAN-IPR.

The Concept Note envisioned the FGD as a basis for a regular platform for the ASEAN-IPR to host and engage with Think Tanks in the region, sharing best practices and lessons learned on issues relevant to the work of the Institute and like-minded institutions. Topics may be drawn from ASEAN-IPR's list of "Priority Research Areas," as well as issues of regional relevance and concern. The Concept Note also suggested that the FGD could be considered a side-event of ASEAN-IPR's activities (e.g., training/capacity building, launch of ASEAN-IPR research/research outcomes, etc.).

The ASEAN-IPR has successfully convened three FGD sessions so far, all three adopting different themes relevant to the priority or interest of the Institute. The first in January 2021 on "The Role of ICT as a Tool in Mitigating Conflict and Fostering Peace"; the second in December 2021 on "Lessons Learned on Engaging Constituents for Peace Building in the Region"; and third in December 2022 on "The Role of "a regional mechanism" in Post-Conflict Peacebuilding". These FGDs became platforms for frank discussions and exploration of thematic issues, through gauging opinions from experts and practitioners, including members of the ASEAN-IPR Governing Council and Advisory Board, a pool of experts and the network of Think Tanks.

As a follow-up to the first FGD "The Role of ICT as a Tool in Mitigating Conflict and Fostering Peace" and in support of the ASEAN-IPR Regional Conference on Cybersecurity and the Role of Information Technology in Fostering a Culture of Peace in ASEAN, scheduled for early 2025, ASEAN-IPR organized a subsequent FGD to explore the intersection of cybersecurity and peacebuilding. This FGD, which is detailed in this report, aimed to understand how technological advancements and cyber challenges can both threaten and support peace efforts.

Objective

This FGD served as a precursor to the ASEAN-IPR Regional Conference scheduled for early 2025, exploring the critical intersection of cybersecurity and peacebuilding. The aim was to understand how technological advancements and cyber challenges impact peace efforts, providing a multi-dimensional view of cybersecurity's role in both conflict and peacebuilding. These insights will inform broader discussions at the main conference

Goals



Gain a comprehensive understanding of the current landscape of cybersecurity and its implications for peacebuilding.



Identify specific cybersecurity challenges that impact peace, including threats to critical infrastructure and human security.



Explore innovative solutions and strategies to leverage cybersecurity and IT for enhancing peacebuilding efforts.

Expected Outcomes



Develop actionable insights on integrating cybersecurity into peacebuilding initiatives, highlighting threats and opportunities.



Generate a set of policy recommendations for integrating cybersecurity strategies into national and regional peacebuilding and conflict prevention frameworks.



Foster enhanced collaboration among cybersecurity, IT, and peacebuilding experts to create a multidisciplinary approach to addressing cyber challenges in peace efforts.



Provide a well-rounded foundation of knowledge and perspectives that will inform and enrich the discussions and activities at the main conference.

Overview of Participants

Facilitators and Discussants

Dato' Ts. Dr. Haji Amirudin Abdul Wahab FASc
Chief Executive Officer of CyberSecurity Malaysia, Malaysia

Mr. Johannes Laaksonen
Security Manager, CMI – Martti Ahtisaari Peace Foundation, Finland

Mr. Felix Kufus
Consultant, Digital Peacemaking Team, CMI – Martti Ahtisaari Peace

Dr. Miftahul Ulum
Senior GTA, Department of Politics and International Studies, University of Warwick, Lecturer, Department of Politics, University of Muhammadiyah Jakarta, Indonesia

Dr. Tamara Nair
Research Fellow at the Centre for Non-Traditional Security Studies (NTS Centre) at the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University, Singapore

Dr. Jompon Pitaksantayothin
Associate Professor of Information Technology Law Division of International Studies Hankuk University of Foreign Studies (HUFS), Thailand

Dr. Bora Park
Research Fellow, Department of Emerging Security Studies, Institute for National Security Strategy (INSS), Republic of Korea

Dr. Whisnu Triwibowo
Assistant Professor (Communication) and the Head of Undergraduate Studies at the Universitas Indonesia, Indonesia

Mr. Beltsazar Krisetya
Researcher, Department of Politics and Social Change, CSIS Indonesia, Indonesia

Participants

Col. Francel Margareth Padilla
Commissioned Officer, Philippine Army's Signal Corps, Philippines

Dr. So Jeong Kim
Director of Emerging Security Studies and a Senior Research Fellow of the Institute for National Security Strategy (INSS), Republic of Korea

Dr. Nguyễn Việt Lâm
Visiting Lecturer, Diplomatic Academy of Viet Nam (DAV), Viet Nam

Mr. Sigit Kurniawan
Director of Strategy for Cybersecurity and Cryptography, National Cyber and Crypto Agency of Indonesia (BSSN), Indonesia

Ms. Isya Hanum Kresnadi
Public Policy Manager, Google Indonesia, Indonesia

Ms. Genalyn Macalinao
Section Head, Critical Information Infrastructure Protection, CIECSD - Cybersecurity Bureau,

Dr. Gulizar Haciyakupoglu
Research Fellow at the Centre of Excellence for National Security (CENS), S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University, Singapore

Ms. Johanna Poutanen
Head for Women in Peacemaking & Digital Peacemaking, CMI – Martti Ahtisaari Peace Foundation, Finland

Mr. Sean Tan Yi Jin
Senior Analyst for the Cyber and Homeland Defence Programme at the Centre of Excellence for National Security, S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University, Singapore

Mr. Rahnee Cheysser Estrada
Project Development Officer V, Division Head, Information and Communications Technology, Office of the Presidential Adviser on Peace, Reconciliation and Unity, Philippines

Ms. Arti Alifah Aviandari R
Member of Yayasan Forum Komunikasi Aktivis Akhlakulkarimah Indonesia (FKAAI), Indonesia

The participation of these experts from various backgrounds provided meaningful contributions and expanded the range of issues discussed. Their diverse perspectives enriched the dialogue, offering useful and enlightening insights that were instrumental in shaping the recommendations and outcomes of the FGD.

Agenda & Sessions

The FGD was structured into five sessions, each dedicated to examining different aspects of the cybersecurity landscape, its impacts on peace and security, and the potential for Information Technology to contribute to peacebuilding initiatives. Each session began with an overview to set the stage for discussions and was adjusted based on the participants' expertise and emerging topics during the FGD. The discussions were led by project experts and attended by participants with experience in both cybersecurity issues and peacebuilding efforts, ensuring a productive exchange of ideas and solutions.

Session 1

Cybersecurity and Peacebuilding - Understanding the Landscape

Facilitator : Dato' Ts. Dr. Haji Amirudin Abdul Wahab FASc

Discussant : Mr. Johannes Laaksonen

This session provided an overarching view of how cybersecurity intersects with peacebuilding efforts. It explored the definition of cybersecurity, extending it beyond technical aspects to include human security and community welfare. The session aimed to highlight the dual nature of cybersecurity as both a threat and a support mechanism for peace initiatives.

Topics covered

- Expanding the definition of cybersecurity
- Cybersecurity in peacebuilding efforts
- Cybersecurity and geopolitics
- Resilient community-building (cybersecurity from a community perspective)

Session 2

IT's Dual Role in War and Peace

Facilitator : Mr. Felix Kufusc

Discussant : Dr. Miftahul Ulum

This session delved into the dual nature of information technology (IT), examining its role as both a catalyst for conflict and a pivotal tool for peacebuilding. The discussions explored how IT can be leveraged to prevent conflict, promote peace, and enhance humanitarian efforts.

Topics covered

- The potential of digital technology in peace-making processes
- The neutrality of Technology
- The incentivizing of Information Technology as a tool for peace
- Early Warning Systems

Session 3

Gender and Human Rights - Approaches to Cybersecurity

Facilitator : Dr. Tamara Nair

Discussant : Dr. Jompon Pitaksantayothin

Focusing on the intersection of gender, human rights, and cybersecurity, this session explored the diverse ways in which cybersecurity policies and practices affect different gender groups. The discussions delved into the implications of online harassment, gender-based violence, and the need for creating safe digital spaces for dialogue and reconciliation. This introduction sets the stage for a detailed examination of various related topics including legal frameworks, policy inclusion, and the roles of social media and children's rights within the cybersecurity landscape.

Topics covered

- Impact of cybersecurity on gender groups
- Gender overlooked in digital technology development
- Prevalence of online harassment and violence
- Comparative legal readiness
- Women's role in cybersecurity and peacebuilding
- Social media's role in gender advocacy
- Children's rights in cyberspace.

Session 4

Cybersecurity and Radicalization

Facilitator : Dr. Bora Park

Discussant : Dr. Miftahul Ulum

This session focused on the role of cybersecurity in addressing and preventing radicalization. It discussed the responsibilities of social media platforms, the use of gaming for radical purposes, and the legislative frameworks in place to counter radicalization efforts.

Topics covered

- Expansion of radicalization space into cyberspace
- State involvement in cybersecurity and radicalization
- Role of private companies
- Social media's role in addressing radicalization
- Rehabilitation and reintegration strategies:
- Government and social media company collaboration
- Gaming platforms as a venue for radicalization

Session 5

Social Media's Effect on Political Polarization

Facilitator : Mr. Beltsazar Krisetya

Discussant : Dr. Whisnu Triwibowo

This session examined the role of social media in political polarization, particularly within ASEAN Member States. It identified the effects of cyber threats on political stability and explored ways to mitigate and depolarize political discourse through social media.

Topics covered

- Impact of cyber threats on political stabilization
- Amplification of political tensions by social media.
- Role of social media in political events
- Demographic shifts in political engagement on social media
- Mitigation strategies for social media-induced political polarization



Session 1

Cybersecurity and Peacebuilding - Understanding the Landscape

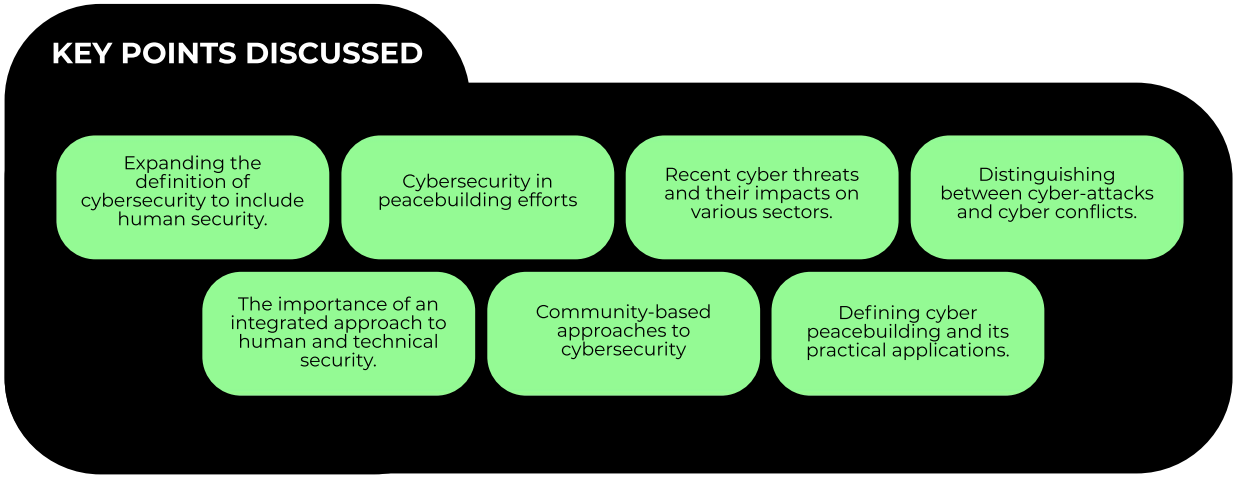
As the first of five Focus Group Discussion (FGD) sessions, this session zoomed in on understanding the current landscape of cybersecurity and peacebuilding to set a foundational base for the next four sessions. To comprehend the landscape of cybersecurity and peacebuilding in ASEAN member states, this session discussed several key points: how different actors defined cybersecurity, how they viewed cybersecurity in peacebuilding efforts, and how they practically contextualized it within recent cyberthreats and their impacts, differentiating between cyberattacks and cyber conflicts. Furthermore, the session explored the integration of cybersecurity from technical to human security issues, the community perspective of cybersecurity, and how different actors defined cyber peacebuilding.

Overview

The first session focused on broadening the understanding and definition of cybersecurity in the context of peacebuilding. It explored the multi-faceted nature of cybersecurity, extending beyond technical aspects to include human security and community welfare. The session aimed to highlight the dual role of cybersecurity as both a threat to, and a support mechanism for peace.

Introduction

The session commenced by emphasizing the interconnectedness of the cyber and physical realms and underscored the necessity of integrating human security into the concept of cybersecurity, spotlighting the repercussions of cyber risks on individuals, communities, and societies at large. The broadening of the conventional CIA triad (Confidentiality, Integrity, Availability) to include Authenticity as an additional value was elaborated upon, especially on how each component might correlate with human security. Subsequently, the discussion shifted towards exploring the function of cybersecurity within peacebuilding efforts underscoring the significance of establishing secure spaces for dialogue and fostering trust in multi-stakeholder processes. The session also addressed the challenges presented by threat actors, particularly the ambiguity between state and non-state actors and the complexities of attribution.



MAJOR INSIGHTS AND PERSPECTIVES

Expanding the definition of cybersecurityto include human security

The nexus between cybersecurity and human security has emerged as a critical area of concern. Traditional definitions of cybersecurity, primarily focused on protecting information within computer systems and networks, must be expanded to encompass the broader implications for individuals, communities, and societies.This includes integrating elements like confidentiality, integrity, and access to ensure they contribute to human security. Traditional definitions of cybersecurity do not take into account the human impact of risks and incidents related to cyber security. Traditional approaches mostly apply to safeguarding of data, organizational process and continuity of critical systems and infrastructure. This creates technical bias. Traditional definitions and concerns of human security can be used to bridge traditional and critical definitions of cybersecurity. Cybersecurity and its role in social issues is underexplored from a definition's perspective. This needs to be investigated further.

Cybersecurity is a complex and multifaceted concept, with researchers in various fields, including international relations and security studies, increasingly examining the impact of technology on national and international security. According to one participant: "cybersecurity is not just about protecting computer systems; it's about safeguarding individuals and communities. The human element is crucial in defining and implementing effective cybersecurity measures." The rapid expansion of the internet has reshaped traditional forms and norms of the international landscape, necessitating a new era of geopolitics. The UN 11 norms of responsible state behaviour in cyberspace provide a common basis for states to design strategic direction, develop capabilities, and execute actions responsibly.[1] These norms include interstate cooperation on security, protection of critical infrastructure, and respect for human rights and privacy, among others.

Understanding the landscape of cybersecurity and peacebuilding by ASEAN member states involve examining how various actors define and contextualize cybersecurity. Definitions of cybersecurity differ based on objectives, generally focusing on protecting sensitive information within computer systems and networks. Cybersecurity is not merely a technical challenge, it also involves regulatory, administrative, and organizational dimensions. Cybersecurity aims to ensure the availability, confidentiality, and integrity of information systems, while also enhancing the protection and privacy of personal data. However, an expanded definition of cybersecurity must consider the broader implications for human security, including economic and social aspects. This expanded view recognizes the importance of understanding the nexus between the cyber and physical domains, which is crucial for peace and conflict dynamics. Building trust in cybersecurity processes is fundamental to their success, as it ensures the security of sensitive information shared during negotiations and dialogues. There's an increasing call to incorporate human security into these definitions, reflecting its broader implications for individuals, communities, and societies. This expanded view includes economic and social aspects, emphasizing the importance of understanding the nexus between cyber and physical domains, which is crucial for peace and conflict dynamics.

The importance of cybersecurity in establishing trust within peacebuilding processes

The importance of cybersecurity in establishing trust within peacebuilding processes cannot be overstated. Without robust information and cybersecurity measures, trust in multi-stakeholder peacebuilding initiatives cannot be achieved. Trust is fundamental for the success of these processes, as it ensures the security of sensitive information shared during negotiations and dialogues. In the realm of peacebuilding, cybersecurity is seen as critical for creating safe spaces for dialogue in conflict resolution and for ensuring trust and process integrity.

During the FGD, several participants emphasized the vital role of cybersecurity in peacebuilding efforts. It was highlighted that cybersecurity is a critical component in creating safe dialogue spaces. When parties involved in a conflict want to convene, the confidentiality and security of the information shared are paramount. If the information is compromised, it not only endangers the physical security of the participants but also undermines the entire peace process. Therefore, relaying accurate information and designing strategies on cybersecurity at the core of peacebuilding interventions is essential to maintain trust and ensure the process's integrity.

The concept of "cyber peacebuilding" has gained prominence amid widespread cyber conflicts and rapid digital transformations. However, referring to these efforts solely as cybersecurity may be too narrow, as cybersecurity primarily focuses on securing digital systems and networks. One of the

[1] The 11 norms, established within the UN framework for responsible state behavior in cyberspace, aim to guide the development of rules governing online activities. The UK is committed to supporting global partners in implementing these norms and empowering them to engage in international discussions at the UN. These norms were first agreed upon by a UN group of governmental experts in 2015, with the group's report later endorsed by consensus through UN General Assembly resolution 70/237. In 2018, ASEAN leaders pledged to make these norms central to their efforts in fostering regional cyber stability. See https://documents.unoda.org/wp-content/uploads/2022/03/The-UN-norms-of-responsible-state-behaviour-in-cyberspace.pdf Accessed 23 September 2024.

participants highlighted that "cyber operations" is a more encompassing term, as it integrates not only security but also cyber support and other elements critical to peacebuilding efforts. When the conversation expands towards peacebuilding, it moves beyond technical security measures to include broader dimensions such as responsible state behavior and collaborative international actions.

One of the participants further emphasized the role of the United Nations' 11 norms of responsible state behavior in cyberspace, which were endorsed by the UN General Assembly. These norms lay the groundwork for defining acceptable and unacceptable actions in the cyber domain, including not attacking critical infrastructure or engaging in malicious cyber activities against other states. Understanding how states are adopting and operationalizing these norms is crucial, as it reflects their commitment to cooperation and sets a foundation for cyber peacebuilding efforts. The participant highlighted that examining the implementation stages of these norms in different countries provides insight into global cyber governance and peacebuilding dynamics.

Building trust in cyberspace was identified as a fundamental component for the success of multi-stakeholder peacebuilding and conflict resolution initiatives. One of the participants underscored that without embedding information and cybersecurity at the core of interventions, achieving trust among governments, NGOs, and local communities becomes challenging. The participant further noted the need to define the content of trust within cyberspace, particularly in the context of peacebuilding. Frameworks like the Paris Call for Trust and Security in Cyberspace were mentioned as vital references, emphasizing the multi-stakeholder approach to cyber trust.

Furthermore, mechanisms like Confidence Building Measures (CBMs) were cited as essential tools to foster trust, as they provide agreed-upon standards and guidelines under international law. The complexity of modern cyber threats—where data breaches and cyber-attacks blur the lines between criminal actors and state-sponsored entities—further necessitates a comprehensive approach. This approach should combine technical cybersecurity measures with human security elements, ensuring that peacebuilding efforts in cyberspace are both effective and sustainable.

Recent cyber threats and impacts

The session's discussion highlighted the increasing sophistication of cyber threats, including ransomware attacks, data breaches, and state-sponsored cyber operations. Participants noted the rise of AI-generated information campaigns, and the significant threats that can impact national security and individual safety.

Participants observed that cyber threats are becoming more sophisticated and varied. Ransomware attacks – encrypting a victim's data and demanding payment for its release – have seen a sharp increase. These attacks not only disrupt operations but also cause financial losses and harm an organization's reputation. Data breaches, where sensitive information is accessed and often leaked or sold, were also highlighted as a major concern. The implications of such breaches extend beyond immediate financial damage to include long-term issues such as identity theft and the erosion of trust in digital systems.

State-sponsored cyber operations were discussed as a growing threat, with nation-states increasingly using cyber means to achieve political, economic, and military objectives. These operations often involve advanced persistent threats (APTs) that target critical infrastructure, government institutions, and private sector entities. The complexity and resources behind state-sponsored attacks make them particularly challenging to attribute to any particular entity or to defend against them.

The rise of Artificial Intelligence (AI)-generated information campaigns was noted as a significant development in the landscape of cyber threats as well. These campaigns use sophisticated algorithms to create and disseminate false information, manipulate public opinion, and influence political processes. The ability of AI to generate realistic and persuasive content poses a new kind of threat that is difficult to counter with traditional security measures.

Contextualizing cybersecurity within the framework of recent threats reveals the significant impact of data breaches on physical security. The breach of sensitive information can lead to real-world consequences, such as threats to individual safety and compromising critical infrastructure. This blurring of lines between digital and physical security underscores the need for a comprehensive approach to cybersecurity.

Cybersecurity issues often transcend national borders, complicating efforts to regulate and respond to threats. The geopolitical implications of cyber-attacks are profound, as state-sponsored activities can lead to international tensions and conflicts. Participants discussed the difficulty in distinguishing between cyber-attacks and cyber conflicts, noting that the focus often shifts to the impact rather than the origin of the attacks. This raises important questions about the appropriate responses to state-supported cyber-attacks and whether they should be considered acts of cyber conflict.

The session emphasized the necessity of continuous vigilance and the adoption of advanced protective measures. Cyber threats evolve rapidly, and staying ahead requires a proactive approach to security. This includes not only technological defence but also policy measures, international cooperation, and the development of a robust cybersecurity culture. Participants stressed the importance of comprehensive strategies that incorporate both technical and human elements to effectively mitigate the risks posed by modern cyber threats.

Distinguishing between cyber attacks and cyber conflicts

Participants explored the distinctions between cyber-attacks, typically opportunistic and individual actions, and cyber conflicts, which involve sustained confrontations using cyber means to achieve strategic objectives. Understanding these distinctions helps in formulating appropriate responses and strategies to mitigate their impacts. Cyber attacks are generally seen as isolated incidents perpetrated by individuals or small groups, often motivated by financial gain, ideological beliefs, or the desire to cause disruption. These attacks can include activities such as hacking, phishing, ransomware, and data breaches. Although serious, they are usually less complex and less coordinated than cyber conflicts.

Cyber conflicts, on the other hand, involve prolonged and coordinated cyber activities, often orchestrated by states or state-sponsored groups. These activities are strategically planned to achieve significant political, economic, or military objectives. Cyber conflicts may target critical infrastructure, disrupt essential services, or undermine national security. The involvement of actors with resources and the use of advanced techniques distinguishes these conflicts from more opportunistic cyber-attacks.

Integrating cybersecurity from technical to human security issues highlights the need for human empowerment and procedural protections. This comprehensive approach includes protecting critical users, such as journalists, human rights activists, and election officials, who are often targeted due to the sensitive nature of their work. Comprehensive capacity building should extend beyond IT departments to include human resources and legal departments, ensuring a thorough and comprehensive understanding of cybersecurity. This approach recognizes that cybersecurity is not just a technical issue but also involves human and procedural elements. Training programs, awareness campaigns, and policy development are crucial for building a resilient cybersecurity framework.

From a community perspective, cross-border institutions and the human element are crucial components. Two examples are that of personalized interventions, especially for small business owners, and combating election misinformation. Small businesses, often lacking extensive cybersecurity resources, benefit significantly from tailored support and training. Election misinformation poses a unique challenge, requiring targeted efforts to educate and protect vulnerable populations. Extending cybersecurity awareness beyond IT roles to broader community engagement is essential. This involves fostering a culture of cybersecurity awareness that includes all stakeholders, from individual users to large organizations. Community-based approaches can enhance overall resilience by promoting shared responsibility and collective action in safeguarding digital environments.

Integrated approach to human and technical security

Technology is an all-compassing issue so the necessity of combining technical security measures with human intervention was a key point of discussions. Participants agreed that technology alone cannot solve all security issues. Risk assessment and management approaches need to put human security at the forefront of identifying the negative events in cyberspace and matters relating to cyberspace, in general. Human awareness, literacy, and timely intervention are crucial for a resilient cybersecurity framework. Examples from Google Indonesia and other organizations illustrated the benefits of empowering individuals to recognize and respond to cyber threats.

While advanced technologies such as firewalls, encryption, and intrusion detection systems are vital, they are not sufficient on their own. Human error, such as falling prey for phishing scams or failing to update software, often lead to security breaches. Thus, it is essential to integrate human intervention into cybersecurity strategies.

Training and awareness programs are critical for equipping individuals with the knowledge and skills to identify and respond to cyber threats. Participants highlighted the importance of ongoing education to ensure that all users, from employees to end-users, understand the risks and how to mitigate them. This includes recognizing phishing attempts, using strong passwords, and understanding the importance of regular software updates.

Organizations like Google have implemented initiatives to empower individuals to protect themselves and their data. These initiatives include providing security keys, offering cybersecurity training sessions, and collaborating with local organizations to raise awareness. For example, during elections, Google Indonesia worked with local CSOs to provide security training to election officials, ensuring they were equipped to handle potential cyber threats. Beyond individual awareness, procedural protections are necessary to create a security-conscious culture within organizations. This involves establishing and enforcing policies and procedures that promote cybersecurity best practices. For example, implementing regular security audits, conducting

simulated phishing attacks to test employee awareness, and developing incident response plans to handle breaches effectively. Comprehensive capacity building should extend beyond IT departments to include human resources, legal departments, and other relevant areas. Ensuring that all departments understand their role in cybersecurity helps create a unified approach to managing risks.

Community-based approaches enhance overall resilience by promoting a culture of shared responsibility and collective action in safeguarding digital environments. From a community perspective, integrating cybersecurity efforts involves engaging with various stakeholders, including small business owners, educators, and local government officials. Personalized interventions, such as tailored training sessions and resources, help address the specific needs and vulnerabilities of different groups.

A more resilient and comprehensive cybersecurity framework can be established by empowering individuals through education, involving all organizational departments, and engaging with the broader community. This holistic strategy ensures that both technical and human elements work together to mitigate cyber threats effectively.

Community-based approaches to cybersecurity

Community-based approaches were discussed as a means to enhance cybersecurity resilience. Emphasizing shared responsibility, participants highlighted the role of community resilience programs in building a secure digital environment. Tailored interventions based on specific community needs and collective action were considered essential for effective cybersecurity.

Participants emphasized that cybersecurity is not solely the responsibility of individual users or organizations but a collective effort that involves the entire community. Community resilience programs are crucial in fostering a culture of shared responsibility. These programs aim to educate and empower community members to recognize and respond to cyber threats, thereby enhancing the overall security posture of the community. Examples of such programs include local cybersecurity awareness campaigns, community workshops, and collaborative initiatives between local governments and community organizations.

One of the key points discussed was the importance of tailoring cybersecurity interventions to meet the specific needs of different communities. A 'one-size-fits-all' approach is often ineffective, as different communities face unique challenges and threats. For instance, small business owners may require targeted support to protect their businesses from cyber-attacks, while local schools might need resources to educate students about online safety. Tailored interventions ensure that resources are used efficiently and that the most vulnerable groups receive the support they need.

Collective action is essential for building a resilient cybersecurity framework. Participants highlighted the role of community engagement in promoting cybersecurity awareness and encouraging proactive behavior. One participant reiterated that: "cybersecurity from a community perspective shifts the emphasis from individual and organizational security to the overall digital health of the community. Shared responsibility is key." Community-led initiatives, such as neighborhood watch programs for cybersecurity, can help create a sense of ownership and responsibility among community members. These initiatives can also facilitate the sharing of information and best practices, further strengthening the community's defenses against cyber threats.

From a community perspective, the involvement of transnational institutions and the human element are crucial components. Cyber threats often transcend national boundaries, making international cooperation and coordination essential. Cross-border institutions can provide support and resources to local communities, helping them to address cybersecurity challenges that are beyond their capacity to handle alone. Additionally, focusing on the human element—such as fostering a culture of cybersecurity awareness and encouraging responsible online behavior—is vital for creating a resilient digital environment.

Defining cyber peacebuilding

The session concluded with discussions on defining cyber peacebuilding, which involves extending traditional peacebuilding practices into the digital realm. This involves using digital tools and platforms to facilitate dialogue, mediate conflicts, and build trust among conflicting parties. Participants discussed how online forums, social media, and other digital communication tools can serve as safe spaces for dialogue and reconciliation. These platforms can help bridge gaps between conflicting groups, allowing for open communication and mutual understanding.

Participants highlighted several examples of how cyber tools can be effectively used in peacebuilding efforts. For instance, conflict resolution platforms that use encrypted messaging and secure communication channels ensure that sensitive discussions remain confidential. Additionally, digital storytelling and multimedia projects can be used to share personal narratives and experiences, fostering empathy and understanding between opposing sides. Virtual reality (VR) and augmented reality (AR) technologies were also mentioned as innovative tools for simulating conflict scenarios and training peacekeepers.

The need for a comprehensive and inclusive approach to cyber peacebuilding was emphasized. This approach involves not only the use of advanced technologies but also the active participation of diverse stakeholders, including governments, NGOs, community leaders, and tech companies. Ensuring that all relevant parties are involved in the design and implementation of cyber peacebuilding initiatives helps address the multifaceted nature of conflicts and ensures that solutions are culturally and contextually appropriate.

Finally, cyber peacebuilding integrates digital tools and platforms into traditional peacebuilding practices, leveraging technology to foster dialogue, mediate conflicts, and build trust among conflicting parties. Online forums, social media, and other digital communication tools create safe spaces for dialogue and reconciliation, enabling open communication and mutual understanding. To maximize its impact, cyber peacebuilding must be embraced at the national level, with governments integrating strategies into national peace policies and frameworks. This includes investing in digital infrastructure to ensure access for all, providing training and resources to equip individuals and organizations with the necessary skills, and fostering collaboration between public and private sectors.

Key Findings and Recommendations

- The definition of cybersecurity should go beyond technical aspects to incorporate human security, reflecting broader implications for individuals, communities, and societies.
- Cybersecurity is critical for creating safe dialogue spaces in conflict resolution and ensuring trust and process integrity. Responsible state behaviour and the application of international law in cyberspace are essential.
- The impact of data breaches on physical security highlights the blurred lines between different threat actors. Cross-border issues and geopolitical implications make distinguishing between cyberattacks and conflicts challenging.
- A holistic approach to cybersecurity involves human empowerment, procedural protections, and extending capacity building beyond IT departments.
- Community-based approaches, personalized interventions, and collective action are crucial for building cybersecurity resilience.
- Extending traditional peacebuilding practices into the digital realm requires a comprehensive and inclusive approach, utilizing IT tools to foster peace among conflicting parties.



Session 2
Information Technology's Dual Role in War and Peace

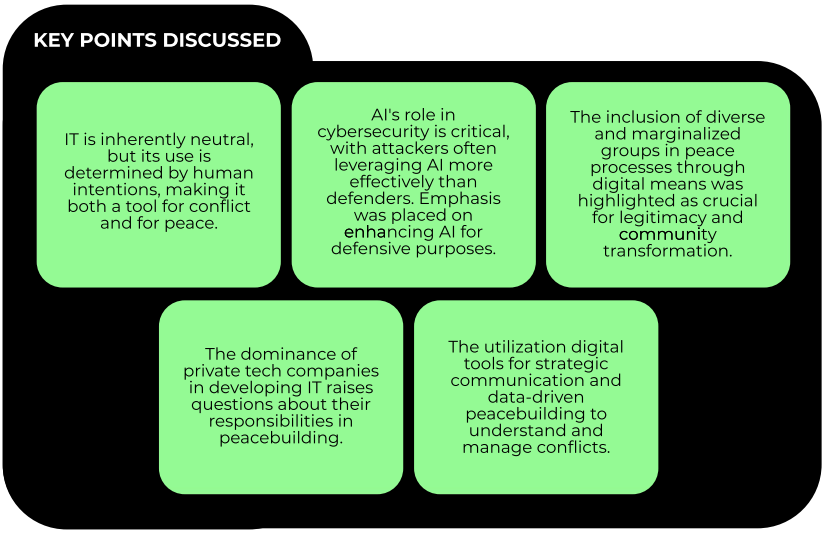
This session delved into the dual nature of Information Technology (IT), examining its use as both a tool for conflict and as an instrument for peace. The discussions explored the various ways IT can be leveraged to prevent conflict, promote peace, and enhance humanitarian efforts. It examined how information technology serves both as a weapon in cyberwarfare by state and non-state entities and as a tool for promoting peace and humanitarian efforts. Strategies for using information technology to build a culture of peace, prevent conflicts, and mitigate the impact of conflict were proposed and discussed. Furthermore, the session discussed how peacebuilding in cyberspace contributes to global security within a broader framework by fostering social cohesion and resilience through digital platforms that enable communication, spread awareness, and mobilize support during crises, particularly with the utilisation of Artificial Intelligence (AI).

Overview

Session two explored the multifaceted nature of information technology (IT) and its implications in both conflict and peacebuilding contexts. The session brought together experts to discuss how IT can serve as both a weapon in cyber warfare and a tool for promoting peace and humanitarian efforts. The discussions emphasized the importance of strategic approaches to leveraging IT for peace while mitigating its potential threats.

Introduction

The session commenced with an acknowledgment of the rapid spread of digital technologies globally. It highlighted the dual nature of IT, which can be used to both escalate conflicts and foster peace. The speakers underscored the neutrality of technology, emphasizing that its impact is determined by human motives and applications.



MAJOR INSIGHTS AND PERSPECTIVES

IT's dual nature

The rapid spread of Information Technology (IT) has brought about a landscape filled with both opportunities and threats. Despite its neutral stance, the impact of IT is significantly shaped by human use. As one participant stated: "technology is neutral, but its use depends on human motives. Humans and technology cannot be separated in contemporary times". Social media, for example, holds the power to counter misinformation, yet it can also propagate biases, illustrating the dual nature of technology. Artificial Intelligence (AI), another critical component of IT, mirrors this neutrality but is frequently manipulated by human motives, often benefiting attackers more than defenders. This imbalance calls for a strategic shift towards using AI defensively, where influencers and public figures can play a pivotal role in promoting the positive use of cyber tools.

The dominance of private companies in the development of technology further complicates this dynamic, raising pertinent questions about their responsibilities in contributing to peacebuilding efforts. These companies, while driving technological advancements, must also consider their public duty to support societal well-being. Moreover, digital inclusion is essential in amplifying the voices of conflict stakeholders, thereby enhancing the legitimacy and fostering community transformation. By ensuring that all groups, especially marginalized ones, are represented in digital dialogues, technology can support more inclusive and representative policy-making processes. This requires a fundamental shift in perspective on how technology is utilized, moving beyond its conventional applications to harness its potential for promoting peace and resolving conflicts.

Strategies for leveraging IT's positive use

Digital technology significantly enhances peacebuilding efforts through several key areas, including data analysis, engagement, inclusion, and strategic communication. Organizations like CMI have been at the forefront of promoting these strategies through tools like Remesh, Inclus, and Foresight. In recent years, CMI has pioneered a digitally enhanced foresight methodology, applied in future-oriented dialogue processes in countries such as Yemen, Libya, Palestine, and Armenia. Central to this approach is the use of an online platform for data collection, analysis, and visualization. CMI's tool of choice has been Inclus, a web application provided by a Finnish company of the same name.

During the FGD, Inclus was used to conduct a cyberpolicy survey, offering a hands-on example of the tool's implementation. A detailed example of this usage is provided in Annex 2. These platforms facilitate large-scale digital dialogues and data management, ensuring that diverse perspectives are incorporated into peace processes. However, the success of these initiatives hinges on digital literacy and connectivity, highlighting the need for widespread access and education.

Cyber initiatives must take into account the varying levels of community access to digital tools. It's essential to combine technological approaches with traditional methods of peacebuilding to ensure a comprehensive and inclusive process. Collaboration between peacebuilders and IT developers is crucial in this regard, as it fosters the development of innovative and effective solutions tailored to specific conflict contexts. Strengthening AI for defensive purposes is another critical strategy. This requires building and relying on robust regulatory knowledge to protect against cyber threats while leveraging AI's capabilities for good. IT can also enhance engagement and inclusion, providing a platform for all stakeholders to participate in policy-making processes. As one participant reiterated: "Digital inclusion in peacemaking means the voice of conflict stakeholders gets further into the peace process. By supporting policymaking, technology ensures that peacebuilding efforts are grounded in practical and actionable strategies.

Data-driven peacebuilding is a powerful approach to understanding conflicts and identifying hotspots. By analyzing vast amounts of data, peacemakers can gain insights into the underlying causes of conflicts and facilitate online dialogue that address these issues. This strategic use of IT not only aids in conflict resolution but also in the prevention of future conflicts, creating a more stable and peaceful environment.

The contribution of cyber peacebuilding to broader global security issues

Cyber peacebuilding plays a pivotal role in addressing broader global security issues by leveraging digital tools to increase diverse perspectives and support peace processes. The central question remains whether IT serves as a threat or as an opportunity, and identifying measures to accelerate its use for peace is paramount. Digital tools enable the inclusion of various viewpoints, which is crucial for comprehensive and effective peacebuilding.

Artificial Intelligence (AI) is a critical component of cybersecurity, underscoring the necessity for secure and unbiased data to protect global security. Ensuring that AI systems are used ethically and effectively requires ongoing efforts to safeguard data integrity and prevent misuse. Dialogue with technology companies is essential in this regard, as collaboration can help counteract the negative impacts of misinformation algorithms and promote the responsible use of digital platforms.

Adopting a critical mindset towards cybersecurity is vital, one that prioritizes human rights and well-being. This approach involves integrating traditional security measures with critical perspectives that emphasize inclusivity, transparency, and ethical considerations. Balancing confidentiality and transparency within peace processes is also crucial. Maintaining this balance helps build trust among stakeholders and manage their expectations, ensuring that peace initiatives are both credible and effective. Overall, the strategic use of cyber peacebuilding tools contributes significantly to global security by fostering an environment where diverse perspectives are heard, human rights are prioritized, and technological advancements are leveraged for the greater good.

Key Findings and Recommendations

- The dual nature of IT in the context of war and peace is multifaceted, offering both significant opportunities and serious threats.
- IT's rapid spread and its fundamentally neutral stance mean its impact is determined by human use.
- Similarly, AI, although neutral, often serves attackers more effectively than defenders due to human motives.
- Strengthening AI for defensive purposes necessitates building regulatory knowledge, enhancing engagement, and supporting policymaking.
- AI's role in cybersecurity is pivotal for global security, requiring secure, unbiased data. Dialogue with tech companies is essential to counter misinformation algorithms, and a critical mindset towards cybersecurity must prioritize human rights and well-being.
- The dominance of private tech companies in developing IT also raises questions about their responsibilities in peacebuilding.
- Digital inclusion is crucial as it empowers conflict stakeholders, promotes legitimacy, and fosters community transformation.
- Technology aids policymaking, demanding a shift in how it is utilized.
- To leverage IT positively, digital literacy and connectivity are key, alongside community access to cyber initiatives, which should be combined with traditional approaches.
- Collaboration between peacemakers and IT developers is vital for effective solutions.
- Data-driven peacebuilding is also crucial for understanding conflicts and facilitating online dialogue.
- Balancing confidentiality and transparency in peace processes is vital for maintaining trust and managing expectations.



Session 3
Gender and human rights-based approaches to cybersecurity

Overview

The third session on Gender and Human Rights – Approaches to Cybersecurity was along the intersection of gender, human rights, and cybersecurity, exploring how cybersecurity policies and practices impact different gender groups. It addressed online harassment, gender-based violence, and the creation of safe digital spaces for dialogue and reconciliation.

Introduction

The rapid changes and development of information and digital technologies often overlook the issue of gender, particularly how these technologies impact female users (as well as the LGBTQ+ individuals). This oversight may stem from a lack of awareness among developers regarding the unique online experiences and sensitivities of female users compared to their male counterparts. Female users frequently encounter online harassment and gender-based violence when engaging with these technologies. Therefore, it is crucial for developers to consider gender inclusiveness when designing, developing, and launching technologies. A starting point could be in addressing how users of different genders can be effectively protected from such online harms.

KEY POINTS DISCUSSED

- Legal frameworks and actions against online gender-based violence
- Policy inclusion and women's participation
- Roles of social media
- Vulnerabilities of children and their rights in cyberspace

MAJOR INSIGHTS AND PERSPECTIVES

Legal frameworks and actions against online gender-based violence

Many countries are facing significant problems related to online harassment and violence against women and children. Different countries have varying levels of policy and legal frameworks to tackle these issues. For example, the Philippine Commission on Women plays a major role in addressing these problems through a comprehensive government approach involving various agencies. The importance of law enforcement and handling cases from a gender-sensitive perspective, including proper case recording, was emphasized. In the Republic of Korea, the Ministry of Gender & Family, along with the Ministry of Public Safety, leads the response to online violence against women, with policies that include investigation, legal assistance, and protection for victims. Additionally, 14 private organizations provide counselling to victims of online harassment and gender-based violence. In Indonesia, there is a prevention of sexual violence framework that includes protections in cyberspace. An anti-sexual violence law exists to safeguard women online. Specific commissions, such as the Commission on Protection of Women and the Commission on Protection of Children, collaborate with law enforcement authorities to address harassment content.

However, despite these various measures in different countries, it was also noted that while some countries have legal regulations in place against online harassment, some lack a gender focus. The discussion then focused on legislative frameworks stressing the point that all legislative tools against online harm, must be enforced within a gendered framework. This is especially so for those frameworks that are not tailored to protect violence against women in the digital realm. This gendered approach would include training legal personnel to view cases from a gendered perspective and ensuring that those documenting cases and interacting with survivors consider gendered nuances. Reporting platforms should include gender-specific considerations as well, and mechanisms for handling cases should integrate a gender perspective beyond just court procedures.

Policy inclusion and women's participation

Women's involvement in the development of cybersecurity and peacebuilding is critical, yet it remains underemphasized. Only a small number of people truly consider gender perspectives in these fields, creating a significant blind spot. Women's active participation is essential in shaping peace policies, from upstream policymaking to downstream implementation. There is a need to address the current mindset when it comes to women's participation in online fora. Despite longstanding discussions and some positive discrimination mechanisms, challenges like election quotas persist, limiting women's political participation. Matters become more serious when women in politics are discriminated against online. As one participant shared: "Those women who are politically active are particularly targeted. It is just old threats in new places. But we do have to take this issue quite seriously, because if we want this problem to be addressed by women who are politically active, they already face structural challenges, and increased challenges by online mobilization." Women active in social movements are also prime targets of online gender-based violence. Female religious leaders, too, face scrutiny and negative comments, reflecting ongoing cultural challenges. It is essential to explore and gain insights into different aspects of gender-based violence facilitated by information and digital technologies.

Efforts to enhance women's roles include the establishment of consortiums focusing on gender mainstreaming like the ones in Indonesia, which grew from 19 to 88 NGOs. Additionally, partnerships with the UN and international organizations aim to incorporate gender-responsive approaches in digital transformation and personal data protection. Vietnam's commitment to global gender equality, evidenced by its early ratification of CEDAW, exemplifies such efforts. However, challenges remain, firstly, in the form of male-dominated industries such as the tech industry, and even patriarchal institutions, such as the legal institution, and also in inadequate support from NGOs and CSOs for women involved in social movements, especially in addressing online violence and cyber threats. And despite having gender-sensitive frameworks in place, legal institutions can also be highly patriarchal and even parochial because of historical antecedents.

The focus should be on supporting national reconciliation and unity through gender and human rights programs. An interesting example is the Office of the Presidential Adviser on Peace, Reconciliation and Unity's (OPAPRU) Gender and Development Programme, which aims to understand gender roles, empowering women, especially in peacebuilding. A notable instance of women taking action to protect others from online gender-based violence occurred in 2019. The Nth Room case is a criminal case involving blackmail, cybersex trafficking, and the spread of sexually exploitative videos via the Telegram app[2]. Two female students exposed a group chat on Telegram sharing videos of rape and harassment. Their bravery led to police protection, awards, and future careers in politics and journalism..

[2]The Nth Room case involved one of South Korea's largest blackmail rings, which victimized 16 minor girls and at least 58 women. The victims were coerced into sending violent and degrading sexual images and video clips, which were then shared with clients over the Telegram app. In 2020, the ring's leader, Cho Ju-bin, was arrested and charged with abuse, threats, and coercion in addition to breaking the Child Protection Act, the Privacy Act, and the Abuse Act by Korean authorities. See https://www.theguardian.com/world/2020/mar/25/outrage-in-south-korea-over-telegram-sexual-abuse-ring-blackmailing-women-and-girls. Accessed 23 September 2024

Equally important is the fact that digital innovation for women's advancement should be prioritized. Initiatives to increase women's participation in the Science, Technology, Engineering and Mathematics (STEM) fields should be promoted through advocacy and volunteer efforts. Encouraging more women and girls to enter technology-related areas is seen as a way to create a more inclusive environment.

Roles of social media

The role of youth in gender advocacy on social media is significant. Social media can be a powerful tool for promoting human rights and protecting women, making the emphasis on gender equality through social media essential. From ASEAN's regional perspective, particularly the WPS (Women, Peace, and Security) Agenda, there is a strong link between women's roles in social media and cybersecurity. Recent initiatives, such as the NAP Academy in Bangkok supported by UN Women, have targeted these issues. The Philippines' 4th NAP WPS addresses social media and misinformation, and the ASEAN RPA WPS launched in 2022 focuses on promoting WPS on social media. Future efforts should include monitoring and evaluation, with active participation from groups like the ASEAN Women for Peace Registry and Southeast Asia Women Peace Mediators. Despite privacy concerns, social media is a powerful tool for mobilization, campaigns, and community building, as demonstrated by the #MeToo movement. It can also serve as an educational platform for gender issues and advocate for policy changes such as closing gender pay gaps and addressing gender-based violence.

Vulnerabilities of children and their freedoms in cyberspace

The issue concerning vulnerabilities of children in cyberspace and their protection without compromising their rights and freedoms is very important. Technology development has made materials related to child exploitation more accessible, necessitating punitive measures as well as incentives for companies to include protective measures. However, incorporating children's rights presents a dilemma. It is not easy to balance their right to access digital technology with protection them from harm such as addiction and cyberbullying. This challenge is exemplified by legislative responses to incidents of cyberbullying and child suicides.

The issue of social media algorithms plays a significant role in this context. Governments currently lack regulations on algorithms, which can facilitate the radicalization and recruitment of new members through targeted narratives. It is essential to regulate these algorithms without impeding free speech and to clarify the responsibility of those who create these products. The main responsibility lies with social media operators, but parents and governments must also play a key role in protecting children while allowing them to express their rights. Governments should encourage and support social media operators, many of which are based outside Asia, to incorporate mechanisms that safeguard children's online experiences. In the Philippines, the Internet Service Providers (ISP) are responsible for blocking offensive content due to limited user control over installed applications. Communication channels that monitor and report anomalies, including text messages, are also utilized. The Philippines' collaborative approach in combating child exploitation, involving telecommunications companies and emerging technologies, is a pioneering effort in Southeast Asia. The concept of "digital nannies"[3] highlights the importance of educating parents about the impacts of digital addiction on children.

[3]To explain term Digital nannies refer to the excessive reliance on digital or smart devices by parents to occupy their children. In other words, these devices are used to keep children engaged with digital content. This allows parents to divert their attention to other tasks. Without proper limitations, there is a risk that children may develop smart device addiction. See https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10453252/ Accessed 23 September 2024

Addressing children's rights in cybersecurity involves government engagement with ISPs and social media operators like META to block harmful content. This should be supplemented by, awareness raising activities in schools through curricula that encourage parents to educate their children about online safety.

It is important to note that governments alone cannot deal with these problems. The private sector, civil society, governments, and families should have a share in the protection of children from harmful content and online exploitation while trying to maintain children's rights to digital access.

Key Findings and Recommendations

- The enforcement of laws against online sexual harassment and other forms of gender-based violence is a small but essential part of a broader framework aimed at ensuring safe internet use for women and children.
- Empowering women in the IT industry and developing technological solutions to protect young users from undesirable content—while balancing their right to freedom of expression—are constructive suggestions but a comprehensive approach combining legal, social, and technological measures is necessary to safeguard against online harm effectively.
- Women and young users should be equipped with digital literacy, knowledge, and practical know-how to protect themselves online.
- Educational programmes tailored to different user groups, such as women and children across various age brackets, should be developed. Such programmes should be supported and promoted primarily by governments, as well as NGOs and civil society, and made accessible in schools, workplaces, and homes.
- Beyond individual knowledge and self-protection, a collaborative network of public and private organisations is crucial.
- This network should function as a complaint receipt centre, assist law enforcement authorities when the harm in question is illegal, and provide counselling services.
- These services should offer advice on personal safety, physical and mental health, cybersecurity, and other areas to help victims recover from the harm they have experienced.



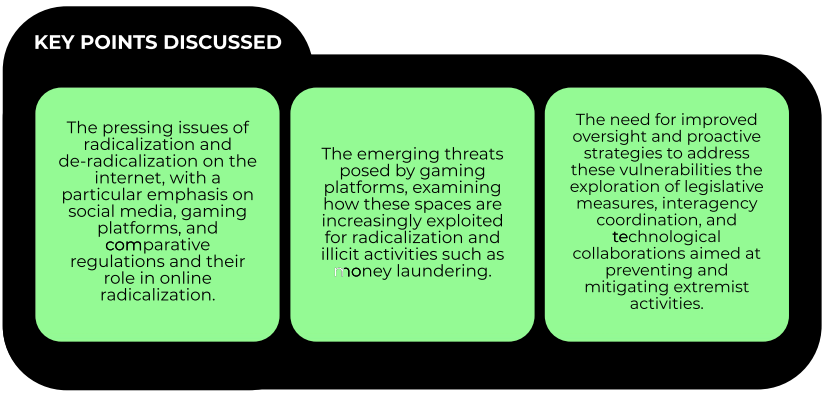
Session 4
Cybersecurity and radicalization

Overview

The fourth session on "Cybersecurity and Radicalization" explored the complex relationship between the internet, social media, gaming platforms, and radicalization. The session emphasized the multifaceted nature of online radicalization, and the diverse strategies required to counter it effectively.

Introduction

The focus in session four was on understanding how radicalization occurs in digital spaces and the roles that social media platforms, gaming environments, and legislative frameworks play in this process. The session was initiated with presentations from experts, followed by an in-depth discussion among participants from various countries.



MAJOR INSIGHTS AND PERSPECTIVES

Multifaceted role of social media

The role of social media in addressing and de-radicalizing extremist content is multifaceted. Simply removing extremist content is insufficient. As one participant observed: "just removing the contents is not the best solution to this problem. Here is what should be included in establishments of counter-narratives." Establishing robust counter-narratives is crucial due to the dynamic nature of social media and messaging platforms, which requires constant adaptation. The use of social media platforms like Facebook and Telegram act as conduits that can lead to significant influence on individuals, especially female users, by facilitating terrorist propaganda and recruitment through easily accessible content and fostering a sense of community among sympathizers. At the same time, social media is also used for rehabilitation and reintegration efforts through counter-narratives that use former rebels' life stories to dissuade others from joining extremist groups, to prevent further radicalization. One participant brought up an important point on vulnerable groups. This participant said: "various different intersecting vulnerabilities on people joining radicalised groups and it is very difficult to analyse the vulnerabilities. People with lack of opportunities, minority groups, isolated from communities among others." This points to the need for greater inclusion in counternarrative measures and, as mentioned earlier, the constant need for adaptation.

Counter-narratives should be implemented in educational systems, with schools playing a critical role in preventing radicalization, complementing police-led counter-radicalization strategies. Governments engage with social media companies like Telegram and Meta to regulate and control extremist content, applying legal pressures to ensure cooperation from these platforms. Existing laws in some countries address cyber-terrorism and extremism, but there is a need for comprehensive legislation to tackle the unique challenges posed by all digital platforms. To this a participant added that his country: "… has had a law to which technology companies have to comply with authorities in criminal investigations. When companies are extremely big and already end-to-end encrypted it becomes more difficult."

Emerging threats posed by gaming platforms

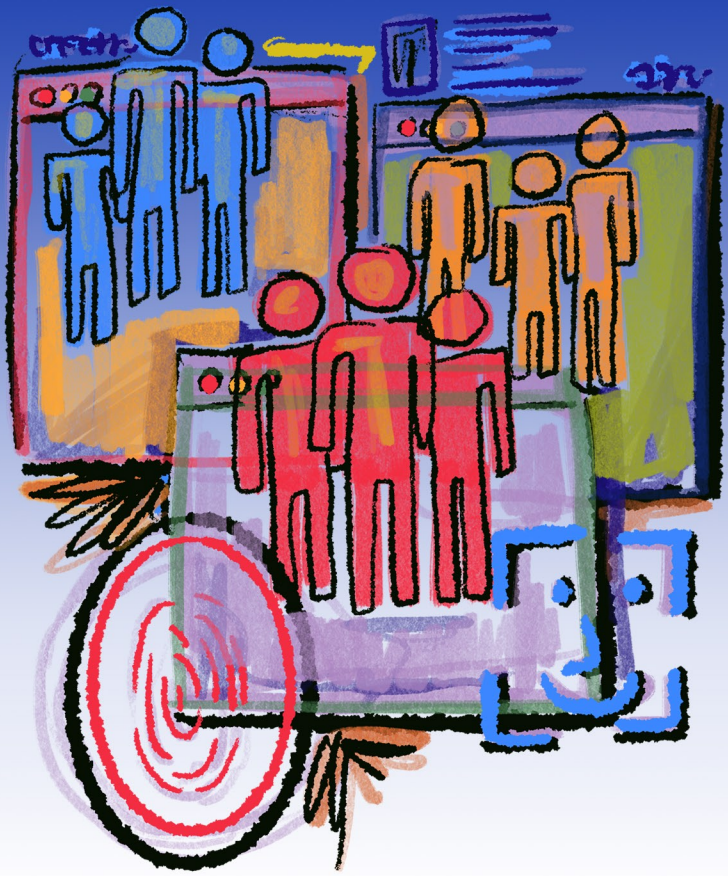
Radicalization in gaming presents emerging threats as gaming platforms are increasingly used for radicalization, knowledge sharing, and financing through activities like money laundering. An interesting point brought up by one of the participants explain how gaming platforms help in the radicalization process: "Gaming offers extremists the tools to spread their values, recruit, and even fundraise much like social media. It goes further by providing an immersive experience that deepens radicalization and allows for specific profiling based on in-game behaviour. This unique capability, along with the anonymity gaming platforms offer, makes them a powerful tool for extremists." This points to the need for proactive measures are necessary to prevent these platforms from being exploited by extremists. Additionally, gaming platforms are less monitored by governments, making them attractive to radical actors. The lack of oversight allows extremists to plan and coordinate attacks, highlighting the need for improved monitoring and regulation of these digital spaces.

Extremism and radicalisation on gaming platforms

Comparative regulations on radicalization and extremism on online and offline platforms involve several key approaches. Legal enforcement in some countries has seen the revision of laws to compel social media platforms to provide information for investigations, including the threat of bans if platforms do not comply. National action plans and regulations often involve interagency efforts, with multiple agencies working together to counter extremism, which is essential for comprehensive counterterrorism strategies. Judicial approaches in some countries provide courts with the authority to take measures against cyberterrorism, complementing other counterterrorism efforts. Effective counterterrorism also requires collaboration with the tech community, raising awareness about the dangers of cyberspace, and engaging stakeholders to manage and mitigate threats.

Key Findings and Recommendations

- The limitations of merely removing extremist content are evident; robust counter-narratives are crucial to effectively counter radical ideologies.
- Social media platforms such as Facebook and Telegram significantly influence radicalization by providing accessible content and fostering communities among sympathizers.
- Rehabilitation and reintegration of former extremists, using their narratives to dissuade others, is a strategy to prevent radicalization.
- Schools play a critical role in implementing counter-narratives, complementing police-led counterterrorism efforts.
- Governments engage with social media companies to regulate extremist content, applying legal pressures to ensure cooperation.
- There is a need for comprehensive legislation to address the unique challenges posed by digital platforms. in the realm of gaming, there is an emerging threat of radicalization and gaming platforms are used for radicalization, knowledge sharing, and financing through activities like money laundering.
- Collaboration with the tech community is crucial for effective counterterrorism, emphasizing the importance of raising awareness about cyberspace dangers and engaging stakeholders to manage and mitigate threats.



Session 5
Social media's effect on political polarization

Overview

The fifth session of the Focus Group Discussion (FGD) zoomed in on the impact of social media on political polarization, particularly within ASEAN Member States. The session examined how social media platforms contribute to both the exacerbation and potential mitigation of political polarization. Discussions also addressed the role of cyber threats in destabilizing political environments and explored strategies to reduce the negative effects of social media on political discourse.

Introduction

Social media has become a critical platform for political discourse in ASEAN Member States. However, its role in deepening political divides and fueling polarization presents significant challenges. This session aimed to explore these challenges by analyzing the effects of social media on political polarization, considering the different modalities of social media platforms, and discussing the implications for political stability and social cohesion in the region.

KEY POINTS DISCUSSED

- How social media platforms amplify political tensions, create echo chambers, and spread divisive narratives.
- Demographic shifts in social media usage.
- Different social media platforms' contributions to polarization, noting that platforms with richer modalities (such as Facebook and YouTube) might have a stronger impact than those with limited features.
- Media literacy programs, greater transparency and accountability from social media platforms, and the development of early warning systems for detecting and responding to political polarization

MAJOR INSIGHTS AND PERSPECTIVES

Social media platforms were identified as powerful tools for amplifying political polarization, with algorithms often prioritizing emotionally charged content that deepens societal divisions. As one participant noted: "social media has blurred the lines between online and offline political polarization, turning digital platforms into battlegrounds for political influence." This effect is seen across various demographics, with both younger and older users contributing to online political tensions. Participants highlighted how disinformation significantly escalates conflicts and creates social instability. The difficulty of combating false narratives in real-time was emphasized, given the speed and reach of social media. The session also underscored a growing intergenerational divide in social media usage, with younger generations traditionally dominating online political discourse, while older demographics increasingly engage with social media, often bringing different political perspectives that contribute to polarization. As one participant commented: "social media and cyberspace have become arenas of competition between generations, with younger and older people using these platforms to push their political aims. This shift has intensified political polarization, making it increasingly difficult to distinguish between true and false information."

Further discussions revealed that the features of different social media platforms influence the extent of their impact on political polarization. Platforms like Facebook and YouTube, which support rich multimedia content, were seen as having a stronger polarizing effect compared to platforms like Twitter, which limits communication to shorter, text-based interactions. One participant commented that: "actors use multiple social media platforms strategically, leading users from one to another until they reach the point where the audience fully connects with their content, often through longer, more impactful videos" Participants also noted that emotionally charged posts tend to gain more engagement due to the design of these platforms' algorithms, leading to a "rabbit hole" effect where users are continuously exposed to content that reinforces their existing views. This was highlighted by a participant: "many people in certain regions only know the internet through social media. With algorithms biased towards emotionally charged content, users are constantly exposed to polarizing and divisive information, deepening the rabbit hole of existing views."

The challenges of regulating social media without infringing on freedom of expression were also explored. Participants debated the role of governments versus social media companies in mitigating the negative effects of online polarization. It was noted that regulation is complex, as it often involves balancing content moderation with the right to free speech. As noted by one participant: "the challenge lies in balancing the regulation of social media to prevent polarization while safeguarding freedom of expression." Regional cooperation among ASEAN Member States was identified as a critical need to address the shared challenges of political polarization and cyber threats. Collective action was seen as more effective in pressuring social media companies to improve transparency and accountability.

Participants also discussed the seasonal nature of political polarization, which intensifies during critical political events like elections. In such periods, the online space often becomes a battleground for political influence, with increased activity from both domestic and foreign actors. The discussion highlighted the need for early warning systems and strategic approaches to manage political polarization during these high-risk periods. These insights underline the complexity of social media's impact on political polarization and the need for a multi-faceted approach to address the associated challenges.

Key Findings and Recommendations

- ASEAN Member States should consider developing a regional framework for social media accountability and transparency, leveraging collective bargaining power to negotiate with major platforms.
- Media literacy programs should be expanded to focus not only on user responsibility but also on the integrity of online content and the algorithms that drive social media platforms.
- There is a need to develop early warning systems for detecting political polarization and cyber threats, particularly during critical political events.
- Enhancing cross-border collaboration to combat disinformation and misinformation campaigns should be a priority. This includes sharing best practices and coordinating efforts across ASEAN Member States.
- Social media companies should be encouraged, or mandated, to increase transparency in their algorithmic decision-making processes to reduce the amplification of polarizing content.

SUMMARY OF FINDINGS AND MOVING FORWARD

SESSION 1

Understanding the landscape of cybersecurity and peacebuilding by ASEAN member countries involves examining how various actors define and contextualize cybersecurity. Definitions of cybersecurity differ based on objectives, generally focusing on protecting sensitive information within computer systems and networks. There's an increasing call to incorporate human security into these definitions, reflecting its broader implications for individuals, communities, and societies. This expanded view includes economic and social aspects, emphasizing the importance of understanding the nexus between cyber and physical domains, which is crucial for both peace and conflict dynamics. Building trust in cybersecurity necessitates a shared understanding and adherence to international agreements.

In the realm of peacebuilding, cybersecurity is seen as critical for creating safe spaces for dialogue in conflict resolution, ensuring trust and process integrity. The concept of cyber peacebuilding has gained importance in the context of widespread cyber conflicts and digital transformations, suggesting that "Cyber Operations" might be a more encompassing term. Responsible state behaviour and collective expectations are vital, along with the application of international law in cyberspace to manage cybercrimes and disputes effectively.

Contextualizing cybersecurity within recent threats reveals the significant impact of data breaches on physical security, blurring the line between criminal and high-level threat actors. Cybersecurity involves cross-border issues and has geopolitical implications, making it challenging to distinguish between cyberattacks and conflicts, with the focus often shifting to the impact of attacks. Questions arise regarding whether state-supported cyberattacks constitute cyber conflicts and what the appropriate responses might be.

Integrating cybersecurity from technical to human security issues highlights the need for human empowerment and procedural protections, with examples of protecting critical users. Comprehensive capacity building should extend beyond IT departments to include human resources and legal departments, ensuring a thorough understanding of cybersecurity. From a community perspective, cross-border institutions including the human element are crucial components. Personalized interventions, especially for small business owners and combating election misinformation, are necessary for resilience, extending cybersecurity awareness beyond IT roles to broader community engagement. Finally, cyber peacebuilding can be promoted as a national concept, involving the use of IT tools to create peace among conflicting parties both online and offline.

SESSION 2

The dual nature of IT in the context of war and peace is multifaceted, offering both significant opportunities and serious threats. IT's rapid spread and its essentially neutral stance mean its impact is determined by human motivation. For example, social media can be a tool to counter misinformation or propagate bias. Similarly, AI, although the technology is intrinsically neutral, often serves attackers more effectively than defenders due to human motives. It is essential to harness AI responsibility and for influencers to promote the positive use of cyber tools. The dominance of private tech companies in developing IT also raises questions about their responsibilities in peacebuilding.

Digital inclusion is crucial as it empowers conflict stakeholders, promotes legitimacy, and fosters community transformation. Technology aids policy-making, demanding a shift in how it is utilized. To leverage IT positively, digital literacy and connectivity are key, alongside community access to cyber initiatives. Supporting policies based on digital inclusion allows conflict stakeholders to participate in the policy-making process, ensuring more inclusive and effective outcomes. These initiatives should be combined with traditional approaches, such as collaboration between peacemakers and IT developers, which is vital for effective solutions. Strengthening AI for defensive purposes necessitates building regulatory

knowledge, enhancing engagement, and supporting policy-making. By defensive purposes, we refer to the use of AI to protect systems, individuals, and institutions from threats such as cyberattacks, misinformation, fraud, and other digital risks. This includes employing AI to enhance cybersecurity, detect and counter misinformation, prevent financial fraud, and defend against physical threats from autonomous systems. Data-driven peacebuilding is also crucial for understanding conflicts and facilitating online dialogue. Furthermore, digital tools bring diverse perspectives to peace processes, emphasizing whether IT is a threat or an opportunity and the measures needed to accelerate its use for peace. AI's role in cybersecurity is pivotal for global security, requiring secure, unbiased data. Dialogue with tech companies is essential to counter misinformation algorithms, and a critical mindset towards cybersecurity must prioritize human rights and well-being. Balancing confidentiality and transparency in peace processes is vital for maintaining trust and managing expectations.

SESSION 3

Understanding gender and human rights in the context of cybersecurity requires examining how these perspectives intersect with digital technology, digital policies, and online behaviours. Cybersecurity, through a gender lens, highlights that while digital technology can democratize access and opportunities, cybersecurity policies often fail to consider gender-specific issues. Inclusive design of cyber infrastructure is crucial because non-inclusive systems tend to replicate and exacerbate societal marginalization, online. Furthermore, the intersection of gender with peace and security is frequently overlooked, underscoring the need for gender-sensitive cybersecurity policies and practices.

Gender-based violence (GBV) in cyberspace mirrors the violence found in the physical world, necessitating comprehensive state interventions. Countries like the Philippines and South Korea exemplify multi-agency approaches that support victims through legal, psychological, and protective assistance. Effective legislation and its enforcement are vital, along with gender-focused training for legal and law enforcement personnel to address these issues adequately, professionally and in a gender-sensitive manner.

The risks posed by emerging technologies are heightened when gender-inclusive perspectives are absent in their creation, leading to increased online discrimination and violence. Encouraging more women into STEM fields and fostering critical thinking can help bridge these gaps. Governments and organizations need to develop gender-responsive frameworks and mechanisms to protect women in digital spaces.

Creating safe digital spaces for dialogue and reconciliation is essential, especially as social media, despite its potential for advocacy, poses risks for women involved in social movements. The misuse of digital spaces and online vigilantism call for balanced policies that protect individual rights while ensuring safety. Active participation of women in policymaking can foster more inclusive and peaceful digital environments.

Social media plays a dual role in gender advocacy and conflict. While it can enhance inclusive participation, its algorithms can also perpetuate harmful content. This necessitates regulatory oversight to ensure responsible platform design. Digital platforms can also facilitate feminist movements and targeted advocacy, pressuring policymakers to address gender issues. Moreover, these platforms should be leveraged for educating the public on gender rights and building supportive communities.

When it comes to children, incorporating children's rights into the cybersecurity framework involves balancing their digital access with protections against online harms. Governments must work with tech companies to block harmful content and raise awareness about cyber safety. Integrating cybersecurity education into school curricula empowers children and parents with the knowledge to navigate digital spaces safely.

SESSION 4

The discussion on the role of social media in addressing and de-radicalizing extremist content highlights several key points. First, the limitations of merely removing extremist content are evident; robust counter-narratives are crucial to effectively counter radical ideologies. Social media platforms such as Facebook and Telegram significantly influence radicalization by providing accessible content and fostering communities among sympathizers. Rehabilitation and reintegration of former extremists, using their narratives to dissuade others, is a strategy to prevent radicalization. Schools play a critical role in implementing counter-narratives, complementing police-led counterterrorism efforts. Governments engage with social media companies to regulate extremist content, applying legal pressures to ensure cooperation. Additionally, there is a need for comprehensive legislation to address the unique challenges posed by digital platforms.

In the realm of gaming, there is an emerging threat of radicalization. Gaming platforms are used for radicalization, knowledge sharing, and financing through activities like money laundering. These platforms are less monitored by governments, making them attractive to extremists for planning and coordination due to the lack of oversight.

Comparatively, regulations on radicalization and extremism on online and offline platforms involve multiple facets. Some countries have revised laws to compel social media platforms to cooperate with investigations, including threats of bans for non-compliance. National action plans and regulations often involve interagency efforts, which are essential for a comprehensive counterterrorism strategy. Judicial approaches in some countries empower courts to take measures against cyberterrorism, complementing other counterterrorism efforts. Collaboration with the tech community is crucial for effective counterterrorism, emphasizing the importance of raising awareness about cyberspace dangers and engaging stakeholders to manage and mitigate threats.

SESSION 5

Cyber threats pose significant challenges to domestic political stabilization within ASEAN Member States and their partners. These threats are broadly defined, which raises questions about balancing political and social stability. Political polarization, driven by misinformation and social media, can naturally arise in democratic societies but often leads to social unrest. Social media platforms tend to amplify polarizing content, creating echo chambers and deepening societal divisions. Misinformation can escalate conflicts and contribute to social instability, with both younger and older generations playing roles in political tensions online. Algorithms on social media reinforce existing views, further increasing polarization.

In ASEAN Member States, social media is a key factor in political polarization, affecting local politics and potentially leading to cyber-attacks. There is a complex interplay between online and offline events, where social media can exacerbate real-world conflicts. Geopolitical tensions in the region have heightened the risk of cyber-attacks, underscoring the vulnerability of political processes. The manipulation of public opinion through social media undermines government policies, contributing to a post-truth era.

To mitigate the political polarization caused by social media, media literacy programs need to focus not only on user responsibility but also on the integrity of online content and infrastructure. Governments must implement strategic solutions to address the root causes of polarization. Accountability and transparency from social media companies are crucial, especially regarding their algorithms. Regional cooperation is vital in exerting pressure on these companies for better regulation, although some countries might prefer bilateral approaches.

Lessons from cases outside ASEAN, such as in Republic of Korea, highlight the extensive use of social media during elections, with state-sponsored cyber-attacks and 'hacktivism' influencing political outcomes. In one ASEAN Member State (AMS), social media was used to distort and manipulate online information, inciting violence among the population. This case underscores a broader pattern, showing how misinformation, even by state actors, can become mainstream and further complicate efforts to manage political polarization.

The FGD conducted over two days provided a robust platform for ASEAN Member States to delve into the multifaceted landscape of cybersecurity, particularly its intersection with cyber peacebuilding, the dual role of IT, and the integration of gender and human rights perspectives. Representatives from various countries, through their enthusiastic participation both offline and online, engaged in comprehensive discussions that highlighted several critical areas:

Comprehensive understanding of

CYBERSECURITY & CYBER PEACEBUILDING

Cybersecurity definitions and human security

Participants explored the varying definitions of cybersecurity, emphasizing the necessity to incorporate human security aspects. This broader understanding connects cybersecurity to economic and social dimensions, underscoring its importance for individuals, communities, and societal stability.

Discussions highlighted the need for a shared understanding and adherence to international agreements to build trust in cybersecurity practices.

Participants universally agreed that cybersecurity should extend beyond technical aspects to include human security, reflecting its broader economic and social implications. This holistic view emphasizes protecting individuals and communities alongside systems and networks.

Cyber peacebuilding as a concept

Cyber peacebuilding is a holistic approach that goes beyond traditional cybersecurity to encompass technical safeguards, human security elements, and international cooperation. It involves embedding cybersecurity at the core of peacebuilding interventions to ensure trust, confidentiality, and process integrity.

The integration of international norms, trust-building mechanisms, and multi-stakeholder cooperation are critical to navigating the complexities of modern cyber threats and fostering sustainable peace in the digital age.

Responsible state behaviour, the application of international law, and managing cybercrimes and disputes were identified as crucial components for effective cyber peacebuilding.

Dual role of Information Technology (IT)

IT's neutral stance was acknowledged, with its impact being determined by human motivations and use. The discussions stressed the need to harness IT positively, promoting its use for peacebuilding and countering its potential for propagating bias and misinformation.

Participants called for collaboration between peacemakers and IT developers to create solutions that leverage digital tools for peace, such as AI for defensive purposes and data-driven peacebuilding strategies.

Participants acknowledged the dual nature of IT, advocating for its use in promoting peace and countering misinformation and bias. The need to harness AI for defensive purposes and leverage digital tools for peacebuilding was widely supported.

Integrating gender and human rights in cybersecurity

The FGD highlighted the importance of gender-sensitive cybersecurity policies. Non-inclusive cyber infrastructures tend to replicate societal marginalization, which needs to be addressed to ensure equitable digital spaces.

Addressing gender-based violence in cyberspace through comprehensive state interventions and fostering the participation of women in policymaking were identified as necessary steps.

Participants highlighted the importance of multi-agency approaches to support victims of gender-based violence (GBV) online, with examples from countries like the Philippines and South Korea serving as models for legal, psychological, and protective assistance.

Case study contexts: social media, gaming, and political polarization

Participants recognized that the removal of extremist content from online platforms is insufficient in combating radical ideologies. While content moderation is necessary, it does not address the underlying factors that contribute to radicalization. Participants argued for the development of robust counter-narratives that challenge extremist ideologies and promote alternative viewpoints. This approach requires a nuanced understanding of the motivations behind radicalization and the social dynamics that facilitate it.

Governments were encouraged to establish proactive partnerships with social media companies to effectively monitor and regulate extremist content online. In addition to fostering collaboration with these platforms, it was recommended that comprehensive legislation be developed to not only mandate greater accountability from tech companies but also to empower authorities with the legal tools necessary to investigate and counteract the spread of radical ideologies. This dual approach aims to create a more robust framework for addressing the evolving challenges posed by online extremism.

Gaming offers extrimists the tools to spead their values, recruit and even fundraise much like social media. It goes further by providing an immersive experience that deepens radicalization and allows for specific profiling based on in-game behavior. This unique capability along with the anonymity gaming platforms offer, makes them a powerful tool for extremists.

Protecting vulnerable groups

Creating safe digital spaces for women, children, and marginalized communities was emphasized. Governments were urged to develop frameworks to block harmful content and raise awareness about cyber safety.

The importance of digital literacy and the development of critical thinking skills was emphasized to help individuals, including women, navigate and participate safely in digital environments

There was a strong consensus on the need for media literacy programs to educate the public on the responsible use of social media, focusing on both content integrity and user responsibility.

Emerging threats in gaming

Gaming platforms were identified as emerging venues for radicalization and illicit activities like money laundering. The FGDs highlighted the need for increased monitoring and proactive measures to prevent extremist exploitation of these platforms.

Political polarization

The discussions underscored the impact of social media on political polarization, contributing to social instability and cyber-attacks. Strategies to mitigate this included media literacy programs focusing on content integrity, user responsibility and holding social media companies accountable for their algorithms.

Regional cooperation and strategic solutions to address the root causes of polarization were deemed essential.



DIFFERING VIEWPOINTS



Definitions and scope of cybersecurity

While there was agreement on the need to incorporate human security, the exact definitions of cybersecurity varied among participants, reflecting different national priorities and objectives. Some focused more on protecting critical infrastructure, while others emphasized broader societal impacts.



Role of social media companies

There was a divergence in views on how to hold social media companies accountable. Some participants called for more aggressive legal pressures and threats of bans for non-compliance, while others favoured collaborative engagement and transparency in algorithm adjustments.



Strategies for combating political polarization

While there was agreement on the role of social media in exacerbating political polarization, opinions differed on the best strategies to mitigate this. Some advocated for stringent regulatory oversight of social media platforms, while others emphasized regional cooperation and strategic bilateral approaches.

In summary, the FGD provided a rich and detailed exploration of cybersecurity challenges and opportunities in the ASEAN region. By addressing the dual role of IT, integrating gender and human rights perspectives, and focusing on social media, gaming, and political polarization, the discussions laid the groundwork for actionable recommendations that can enhance regional cybersecurity and promote peacebuilding efforts.

Potential Topics/Themes



CYBERSECURITY CONFERENCE 2025

SESSION 1 — Understanding the cybersecurity landscape

- The role of ASEAN member states in cybersecurity and peacebuilding: challenges and opportunities
- Integrating human security into cybersecurity: a comprehensive approach
- Cross-border cybersecurity cooperation: building trust and shared norms in the ASEAN region
- The impact of cybersecurity on peacebuilding: bridging the cyber and physical domains

SESSION 2 — IT, cybersecurity, and peace

- State actors and critical approaches to cybersecurity: balancing security and human rights
- The role of AI in cybersecurity and peacebuilding: opportunities and risks
- Digital inclusion as a peacebuilding tool: empowering communities through cyber initiatives
- Collaboration between governments and private tech companies in promoting cyber peace

SESSION 3 — Gender, human-rights, and cybersecurity

- Gender-inclusive cybersecurity policies: addressing online violence and discrimination
- Intersection of gender, peace, and cybersecurity: creating safe digital spaces for all
- Empowering women in STEM: closing the gender gap in cybersecurity
- Protecting children's rights in the digital age: cybersecurity challenges and solutions

SESSION 4

Social media, gaming, and cybersecurity

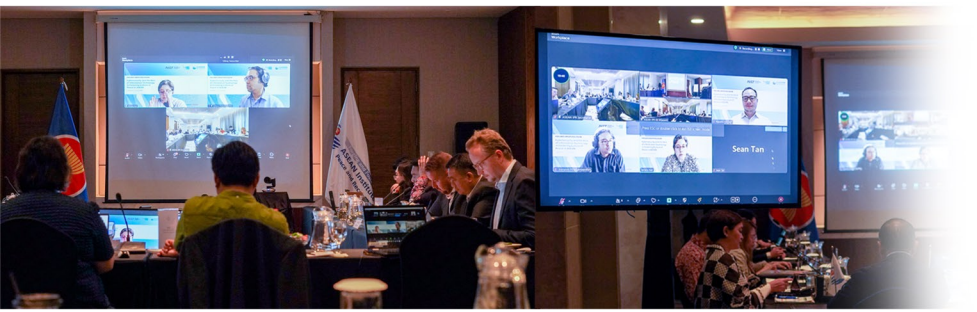
- Public-private partnerships in cybersecurity: success stories and lessons learned
- Countering radicalization through social media: the role of governments and tech companies
- The threat of radicalization in online gaming: emerging challenges and solutions
- Legal and regulatory frameworks for addressing online extremism

SESSION 5

Cyber threats and political stability

- Mitigating political polarization through cybersecurity measures: A regional perspective
- The role of social media in political instability: strategies for ASEAN member states
- Regional cooperation in cybersecurity: addressing geopolitical tensions in ASEAN
- Lessons from global cybersecurity challenges: implications for ASEAN's political stability

RECOMMENDATIONS



1 *Develop comprehensive cybersecurity policies, capacity, and confidence building*

Incorporate human security elements
Ensure cybersecurity policies include aspects of human security, focusing on protecting individuals, communities, and societies. This involves integrating economic and social considerations alongside traditional cybersecurity measures.

Expand training programs
Extend cybersecurity training beyond IT departments to human resources, legal departments, and community leaders. Provide targeted programs for small business owners and initiatives to combat election misinformation.

Promote cyber peacebuilding
Integrate cyber peacebuilding concepts into national policies, using IT tools to foster peace among conflicting parties both online and offline. Encourage cross-border cooperation and community engagement to address cybersecurity threats comprehensively.

Establish an ASEAN regional Early Warning System (EWS)
Develop an ASEAN regional EWS to monitor and respond to cyber threats in real-time. Enhance regional collaboration by sharing threat intelligence and coordinating responses to cyber incidents. Provide regular updates and alerts to member states to pre-emptively address potential cyber-attacks and mitigate their impacts.

2 Harness technology for defensive and peacebuilding purposes

Leverage AI and Digital Tools
Collaborate with tech companies to develop AI tools focused on defending against cyber threats. Promote digital literacy and connectivity, ensuring community-wide participation in cyber initiatives.

Digital Inclusion and Community Empowerment
Empower conflict stakeholders through digital tools, enhancing legitimacy and fostering community transformation. Combine digital tools with traditional peacebuilding approaches for more effective conflict resolution.

3 Enhance Legal and Regulatory Frameworks

Gender-Sensitive Policies and Training
Ensure cybersecurity policies consider gender-specific issues and provide gender-focused training for legal and law enforcement personnel. Create mechanisms to protect women in digital spaces and support their active participation in policy-making.

Strengthen Legal Measures
Revise laws to ensure social media platforms cooperate with investigations and prevent extremist content. Foster inter-agency collaboration for a comprehensive counterterrorism strategy, including judicial approaches to tackle cyber terrorism.

4 Monitor and Regulate Digital Platforms

Accountability of Social Media Companies
Ensure transparency and accountability from social media companies, particularly concerning their algorithms. Exert regional pressure on these companies for better regulation, while allowing for bilateral approaches where necessary.

Gaming Platform Oversight
Increase government monitoring of gaming platforms to prevent their use for radicalization and other extremist activities. Implement proactive measures to address the misuse of these platforms.

5 Mitigate Political Polarization and Promote Media Literacy

Media Literacy Programs
Extend media literacy programs to focus on the integrity of online content and infrastructure, not just user responsibility. Implement strategic solutions to address the root causes of political polarization.

Regional and Bilateral Cooperation
Foster regional cooperation to exert pressure on social media companies for better regulation. Study international cases to understand the impact of social media on elections and political outcomes, developing strategies to counter misinformation and state-sponsored cyber-attacks.

ANNEX I

Focused Group Discussion - Detailed Agenda

ASEAN-IPR REGIONAL CONFERENCE ON CYBERSECURITY AND THE ROLE OF INFORMATION TECHNOLOGY IN FOSTERING CULTURE OF PEACE IN ASEAN

Focused Group Discussion

Day 1: Thursday, 11 July 2024				
08:30-09:00	30 minutes	REGISTRATION		
Opening Session				
09:00-09:15	15 minutes	Opening/Welcome Remarks – ASEAN-IPR	***H.E. Amb. Lee Jang-Keun (TBC)*** ***Mr. I Gusti Agung Wesaka Puja****, Executive Director of ASEAN-IPR*	
Session 1: Cybersecurity and Peacebuilding - Understanding the Landscape This session will provide an overarching view of how cybersecurity intersects with peacebuilding efforts. It will explore the definition of cybersecurity, extending it beyond technical aspects to include human security and community welfare. The session aims to highlight the dual nature of cybersecurity as both a threat and a support mechanism for peace initiatives.				
09:15-10:45	90 minutes		1 *Expanding the Definition of Cybersecurity* 2 *Cybersecurity in Peacebuilding Efforts* 3 *Review of Recent Cyberthreats and Their Impacts* 4 *Distinguishing Between Cyberattacks and Cyber Conflicts*	Facilitator : TBC
			5 *Integrated Approach to Human and Technical Security* 6 *Cybersecurity from a Community Perspective* 7 *Defining Cyber Peacebuilding*	Discussant : TBC
10:45-11:00	15 minutes	Coffee/Tea Break		
Session 2: IT's Dual Role in War and Peace This session will delve into the dual nature of information technology (IT), examining its use as both a tool for conflict and an instrument for peace. The discussions will explore the various ways IT can be leveraged to prevent conflict, promote peace, and enhance humanitarian efforts.				
11:00 -12:00	60 minutes		1 *Explore the dual nature of IT as both a tool for conflict and an instrument for peace* 2 *Develop strategies for leveraging IT to build a culture of peace and prevent conflict* 3 *How does peacebuilding in cyberspace contribute to global security in a broader framework*	Facilitator : Mr. Felix Kufus (TBC) Discussant : Dr. Ulum
12:00-13:00	60 minutes	LUNCH BREAK		
Session 3: Gender and Human Rights – Approaches to Cybersecurity Focusing on the intersection of gender, human rights, and cybersecurity, this session will explore how cybersecurity policies and practices affect different gender groups. It will address online harassment, gender-based violence, and the creation of safe digital spaces for dialogue and reconciliation.				
13:00 -14:30	90 minutes		1 *Cybersecurity Through a Gender and Intersectional Lens* 2 *Online Harassment and Gender-Based Violence in Cyberspace* 3 *Gendered Risks of Emerging Technologies* 4 *Safe Digital Spaces for Dialogue and Reconciliation* 5 *Role of Social Media in Gender Advocacy and Conflict* 6 *Incorporating children's rights in the cybersecurity framework*	Facilitator : Dr. Tamara Nair Discussant : Dr. Jompon
14:30-14:45	15 minutes	Coffee/Tea Break		
Session 4: Cybersecurity and Radicalization				

ANNEX I

Focused Group Discussion - Detailed Agenda

This session will focus on the role of cybersecurity in addressing and preventing radicalization. It will discuss the responsibilities of social media platforms, the use of gaming for radical purposes, and the legislative frameworks in place to counter radicalization efforts.				
14:45-16:15	90 minutes		*1 Role of Social Media Platforms in Addressing and De-Radicalizing Extremist Content* *2 Radicalization in Gaming* *3 Comparative legislation on social media's role in the radicalization and counter-radicalization*	Facilitator : Dr. Park Bora Discussant : Dr. Ulum
18:00-19:00	60 minutes	Dinner for Participants Who Stay at the Hotel		
END OF DAY 1				
Day 2: Friday, 12 July 2024				
08:30-09:00	30 minutes	REGISTRATION		
Session 5: Social Media's Effect on Political Polarization				
This session will examine the role of social media in political polarization, particularly within ASEAN Member States. It will identify the effects of cyber threats on political stability and explore ways to mitigate and depolarize political discourse through social media.				
09:00-10:30	90 minutes		*1 Identify the effects of cyber threats on domestic political stabilization* *2 Discuss the use of social media for political polarization in ASEAN Member States* *3 Brainstorm ways to mitigate political polarization caused by social media* *4 Explore cases outside ASEAN, such as South Korea Lesson learned*	Facilitator : Mr. Beltsazar Discussant : Mr. Whisnu Triwibowo
10:30-10:55	25 minutes	Coffee/Tea Break		
Closing session				
10:55-11:15	20 minutes	Wrap Up Session – Expert.	***Dr. Tamara Nair***	
11:15-13:00	105 minutes	Friday Prayer and Lunch		
END OF FGD SESSION				

ANNEX II

ASEAN Cybersecurity Policy Assessment

ASEAN Cybersecurity Policy Assessment

How do you perceive the current state of cybersecurity policy within ASEAN in terms of promoting security and preventing con?ict? Please include both positive and negative aspects in your answer.

• ASEAN has been on the right track with the advancement
(Vietnam)

• There is great clamor for having a binding mechanism for cybersecurity for ASEAN states. The current state of cybersecurity policy within ASEAN demonstrates a mixed landscape of progress and challenges. On the positive side, ASEAN has made signiGcant strides in fostering regional cooperation and creating frameworks to address cybersecurity threats.
However, there are notable challenges. Disparities in cybersecurity maturity across ASEAN countries hinder cohesive regional action. While some nations have advanced capabilities and robust policies, others lag, creating vulnerabilities that can be exploited. Additionally, the lack of a uniGed, binding cybersecurity policy limits the effectiveness of implementation.
(Philippines)

• Indonesia still ongoing to build policy framework and regulation related on the Geld of cybersecurity. For now, Indonesia dont have speciGc regulation in the Geld of cybersecurity and still looking on the UU ITE or UU PDP as regulation basis on ICT so BSSN as cybersecurity agency dont have authority to do law enforcement especially when cyber crime occured
(Indonesia)

• ASEAN has established frameworks like the ASEAN Cybersecurity Cooperation Strategy (2021-2025) to promote information sharing, capacity building, and joint efforts against cybercrime. This fosters a collaborative environment for tackling regional threats. However, there is uneven implementation among states. Member states have varying levels of cybersecurity infrastructure and legal frameworks. This inconsistency creates vulnerabilities and hinders collective defense.
(Philippines)

• Not advance enough to cover peace building aspect and its implication. The ASEAN Cybersecurity Cooperation Strategy 2021-2025 does not speciGcally cover the issue peace building.
(Indonesia)

• At national level, most ASEAN countries already have their own cybersecurity policy, nonetheless at the ASEAN multilateral level, policy and strategy development still at early stage, where its integrated implementation plan still in process of growth
(Malaysia)

• Having cybersecurity policy within ASEAN is very important in promoting peace and security. In today's era, Information Technology plays a pivotal role in the advancement of human society and its nation. Without such policies and regulations, information technology can be abused and used to create conXict among nations.
(Philippines)

• The current state of cybersecurity policy within ASEAN has both strengths and challenges. Positively, increased collaboration among member states, capacity-building programs, and regional frameworks like the ASEAN Cybersecurity Cooperation Strategy have strengthened collective defense mechanisms. Public-private partnerships and awareness campaigns have also been effective in enhancing cybersecurity measures.

However, challenges remain. Technological disparities among member states, gaps in policy implementation, limited resources, and the rapid evolution of cyber threats pose signiGcant hurdles. Additionally, balancing cybersecurity with individual privacy rights is delicate, risking public backlash if not handled carefully. Despite progress, ongoing efforts are needed to address these challenges and ensure a secure digital environment in ASEAN.
(Indonesia)

• It appears that individual countries in ASEAN have their own laws and policies regarding cybersecurity. However, ASEAN still lacks a regional legal and operational framework that individual countries agree upon. In addition, I have not seen any tangible efforts to implement measures to prevent conXict yet.
(Thailand)

• The current condition of cybersecurity policy in ASEAN has both strengths and weaknesses. Positively, greater engagement among member states, capacity-building programs, and regional frameworks such as the ASEAN Cybersecurity Cooperation Strategy have improved
collective defense mechanisms. Public-private collaborations and awareness initiatives have also been beneGcial in improving cybersecurity. However, issues remain. Technological discrepancies between member nations, limitations in policy implementation, limited resources, and the rapid evolution of cyber threats all provide signiGcant challenges. Furthermore, striking a balance between cybersecurity and individual privacy rights is tricky, and if not handled appropriately, it risks public reaction. Despite improvements, continuous efforts are required to solve these concerns and ensure ASEAN's digital security.
(Indonesia)

• There are differences and similarities among ASEAN member states in regard with cybersecurity. While it is positive that efforts are being made to strengthen cybersecurity for the entire ASEAN region, considering the cross-border nature of cybersecurity, not only regional
cooperation but also enhancing international cooperation is necessary.
(Republic of Korea)

Cyber-Attack Vulnerabilities and Targets

Which institutions or communities are most threatened by cyber-attacks, and for what purposes? Think of institutions like: state institutions, local population, private sector etc.

• In the Philippines, government institutions and banking instutions are the most threatened by cyber-attacks. The purpose is usually to gather as much information that can be used against the government and for the Gnancial institutions are their client's information that can be used for identity theft and similar activities.
(Philippines)

• Government then military for high level Intel. then retail industry for monetary gain and local populace for small scale scams.
(Philippines)

• Government administration and CII sectors are the most institution who have big vulnerability towards cyber attacks because this sector impacted on the society life and when it get attacked, the situation more chaotic
(Indonesia)

• In the latest cyber threat landscape report of the Philippines National Computer Emergency Response Team (CERT-PH), the sector with the highest number of cyber incidents from January to June of this year is the Government and Emergency Services sector. Type of incident most prevalent is data exGltration and data leak.
(Philippines)

• The National Data Center for ransomware.
(Indonesia)

• In Malaysia, based on the threat landscape study by Cybersecurity Malaysia,too sectoral threats are government/public sector, followed by Telecom and Financial sector
(Malaysia)

• The prime target is the private sector, especially commercial banks and companies that hold a lot of personal data (such as telecommunication companies). The second target is public/governmental organizations, such as public hospitals. In my opinion, the main purposes are to steal data stored in the systems (for selling on the darknet) and to disrupt the normal operation of the systems.
(Thailand)

• In Indonesia, state institutions, the private sector, the local population, the healthcare sector, and educational institutions face signiGcant threats from cyber-attacks. State institutions are targeted to disrupt national security and steal sensitive data, while businesses, especially in Gnance and e-commerce, face threats aimed at stealing Gnancial information and intellectual property. The local population is vulnerable to phishing, identity theft, and fraud, largely due to lower digital literacy. The healthcare sector risks theft of medical records and service
disruptions, and educational institutions are targeted for their research data and personal information of students and staff. These attacks are motivated by Gnancial gain, disruption of services, and theft of sensitive information.
(Indonesia)

• For the case of Korea, state institutions(public sector) were the most frequently attacked by foreign actors. The number of attack against state institutions was 1.62 million in average per day in 2023. Approximately 80% of the attacks were attributed to one speciGc country and the purpose for those attacs were to steal some informations (tech, foreign policy etc)
(Republic of Korea)

Major Cybersecurity Threat Actors

Which actors do you perceive as the biggest threats in cybersecurity: local actors, foreign state-funded actors, or criminal actors?

• Criminal Actors and State Spomsored are on top of the list due to the sheer amount of damage they could cause.
(Philippines)

• criminal actors
(Indonesia)

• Based on personal experience as the network security administrator, it is very challenging to identy speciGcally who are the biggest threat in cyber security without the proper tools and resources to monitor and secure the cyberspace.
(Philippines)

• It's a mixture of these actors.
(Philippines)

• Foreign state-funded actors and criminal actors.
(Indonesia)

• Cyber criminal threat actors, regardless from local or foreign threat actors where their key motives are Gnancial. At Cyber999, fraud/scam is the top incidents (consisting of 70% of the total incident reported to Cybersecurity Malaysia)
(Malaysia)

• foreign state-funded actors and interantional criminal organizations
(Thailand)

• In Indonesia, criminal actors are a major cybersecurity threat. They're responsible for a large portion of cyberattacks, including data breaches, phishing attacks and malware attacks.
These attacks aim to steal sensitive information, disrupt business operations, or extort money.
While foreign state-funded actors and local actors also pose a threat, criminal actors are currently the biggest concern in Indonesia.
(Indonesia)

• So far, foreign actors/foreign state-funded actors (e.g. hacking groups) have been the biggest to my country. However, the landscape of cyber theats is changing. State actor (I cannot point out who it is but I guess you know already) started funding to individual actors too and it started selling hacked data to criminal actors, too.
(Republic of Korea)

National Cybersecurity Improvement Recommendations

Please formulate a recommendation on how to improve the current state of cybersecurity in your country.

• To enhance cybersecurity in the Philippines, it is crucial to update and enforce comprehensive laws with strict compliance requirements and penalties. Integrating cybersecurity education into school curriculums, conducting public awareness campaigns, and providing continuous training for IT professionals are essential. Additionally, investing in the development of a skilled cybersecurity workforce and fostering public private partnerships will strengthen the country's overall cybersecurity posture.
(Philippines)

• Increasing cyber professional and build capacity building programme to boost cyber professional skills. Aside of that, the current state must create cybersecurity policy framework and regulation as a strategy to improve cybersecurity resilience
(Indonesia)

• In our country, we have already stablished several laws and regulations in terms of cybersecurity. What I can recommend to improve the current state of cybersecurity is to regularly update the policies, laws and regulations, and conduct information dissemination as the
technology evolves rapidly.
(Philippines)

• The enactment of a Cybersecurity Law. Currently, the Philippines does not have a cybersecurity law, only the Cybercrime Prevention Act. *(Philippines)*

• Fill in the lack of a strategic mindset and policy preparedness.
Also focus on conXict analysis.
Develop digital technologies for peace process.
(Indonesia)

• 1) Strengten policy and the governance of cybersecurity ecosystem in Malaysia
2) Enforce strong Governance, Risk and Compliance best practices at national Level
3) Build more local talents in Cybersecurity for the nation
4) Develop more aggressive cybersecurity awareness education at all levels of society
5) Strengthen Technical Competencies through establishment of Internationally complied labs to protect nation
3)
(Malaysia)

• We already have relevant laws in place. However, effective enforcement is the biggest challenge. This is due to the lack of proper
technologies, expertise, and cooperation from the private sector. Furthermore, it is also diecult to receive collaboration from foreign
authorities and companies, especially for crimes other than the dissemination of sexually abusive images of children.
(Thailand)

• To improve Indonesia's existing cybersecurity situation, a multifaceted approach is required. It is critical to strengthen legal and regulatory frameworks by updating cybersecurity laws and enforcing compliance requirements. Improved public-private collaboration through
information sharing and cooperative projects can lead to a more resilient cybersecurity environment. Educating, training, and certifying a qualiGed cybersecurity workforce will help to close the talent gap. Investing in sophisticated technologies like artiGcial intelligence, machine learning, and blockchain can help with proactive threat detection and safe transactions. Regular risk assessments and resilience planning guarantee that important infrastructure is protected and can recover quickly from cyberattacks. Promoting cyber hygiene through public awareness campaigns and employee training lowers the possibility of human mistake. Improving incident response and recovery through a national framework and simulation exercises boosts preparedness. Finally, boosting international collaboration through global alliances and cybersecurity treaties promotes a coordinated approach to confronting global cyber threats. Implementing these measures will dramatically strengthen Indonesia's cybersecurity posture, protecting digital assets and providing a safer online environment for individuals and
enterprises.
(Indonesia)

• We should enact the law on cybersecurity in a comprehensive manner. My country tried to enact legislation on cybersecurity for the past decade, but it failed.
(Republic of Korea)

Civil Society and Private Sector Roles in Cyber-Resilience

What role should civil society and the private sector play in increasing cyber-resilience?

• Civil society and the private sector play crucial roles in enhancing cyber-resilience in the Philippines. Civil society can raise awareness about cybersecurity issues, advocate for stronger policies, and educate the public on best practices. The private sector can invest in advanced cybersecurity technologies, share threat intelligence with the government, and implement robust security measures within their
organizations. Collaboration between these sectors and the government is essential for creating a resilient cyber ecosystem.
(Philippines)

• Private sector must actively participate with government sector to work and collaborate to facilitate the gaps between government and private sector especially on policy bureaucracy and increase sharing information and experiences between private sector and government *(Indonesia)*

• There should be a whole-of-nation approach in cybersecurity, involving all stakeholders including the private sector in the development of policies is crucial to ensure eecient implementation.
(Philippines)

• The civil society and the private sector plays a signiGcant role in cyber-resileince by providing support to the government and promoting best practices in cybersecurity.
(Philippines)

• Important partner for the Government.
(Indonesia)

• Collaboration with all key stakeholders (public, private, academia and civil society) at both local and international platform is key to success *(Malaysia)*

• For civil society, they need to play more active roles, especially by providing education to the public. For the private sector, they need to give more cooperation to the enforcement authorities, particularly by providing all relevant information. However, it is understandable that, by doing so, they may lose the trust of their customers and, in turn, proGts.
(Thailand)

• Civil society and the commercial sector play critical roles in increasing cyber resilience, and their participation is required to build a comprehensive and resilient cybersecurity ecosystem. Civil society organizations (CSOs) can spearhead efforts to educate the public about cybersecurity best practices, push for improved cybersecurity policies, and hold community workshops to promote digital literacy. They can also create support networks for victims of cybercrime and conduct research to better understand future dangers, resulting in informed policy recommendations. The private sector may help by installing strong cybersecurity measures, performing frequent security audits, and developing cutting-edge cybersecurity solutions. Collaboration with startups, training initiatives, and partnerships with educational institutions can all help to generate a qualiGed cybersecurity workforce. Public-private partnerships to share information and perform cooperative cybersecurity activities, as well as the creation of corporate social responsibility programs aimed at raising cybersecurity awareness, are also crucial. Working collaboratively with the government, public society, and the commercial sector, we can develop a more resilient cybersecurity environment that protects individuals and enterprises from cyber threats.
(Indonesia)

• They should participate more actively in the cooperation. There is a pirvate sector self-governance organization, but its memebers are oriented to some big techs. Another is, even for the big techs, preventing/countering hate speech or disinformation is not mandatory yet. *(Republic of Korea)*

Extremism Assessment and Countermeasures Evaluation

How do you assess the extremist landscape in your country and how do you evaluate your countrys effort in countering it?

• The extremist landscape in the Philippines is marked by groups like Abu Sayyaf and the NPA. While military operations and regional cooperation have made progress, challenges persist due to poverty, education gaps, and regional disparities. Effective counter-extremism requires ongoing socio-economic development, robust security strategies, and international collaboration.
(Philippines)

• Cooperate with other stakeholders who have responsible on the prevention of extremist content and identify what kind of extremism occured to make national action or strategy plan to counter it
(Indonesia)

• There are efforts to address extremism in the Philippines. We have a National Action Plan on Preventing and Countering Violent Extremism (NAP-PCVE).
(Philippines)

• The extremest landscape in the Philippines is very broad, the government has crafted principles of comprehensive peace process including initiatives that promote and reinforce rational reconciliation and unity in order to achieve a just and lasting peace for the national and for all the Filipino people.
(Philippines)

• The Government's top priority.
(Indonesia)

• So far, not a major issue. Current legislation is being used to mitigate extremism through 3R (Royal, Religion & Race) related legislations *(Malaysia)*

• At the moment, it is diecult to say whether Thailand has this problem or not. The media rarely reports on this matter nowadays.
(Thailand)

• Indonesia faces a variety of extremist threats, including Jemaah Islamiyah (JI) and ISIS-aeliated forces. These groups take advantage of social, economic, and political concerns, using the internet and social media to radicalize and recruit. Due to past conXicts and socioeconomic inequities, certain areas, such as Poso in Central Sulawesi, have become centers for extremist activity. Youth, particularly those who are unemployed or have limited educational options, are especially vulnerable to radical ideas. Indonesia has tightened its legal framework by enacting legislation targeting terrorism Gnancing, hate speech, and cybercrime, as well as establishing the National Counterterrorism Agency (BNPT) to coordinate activities. Enhanced intelligence operations and international cooperation have foiled several radical schemes, while routine security actions have degraded many networks. Deradicalization programs aimed at imprisoned extremists and at-risk individuals emphasize intellectual re-education, vocational training, and reintegration into society. The government also works with religious leaders and community organizations to promote moderate views of Islam and counter extremist narratives, as well as public awareness campaigns and educational programs to strengthen resilience against radicalization, particularly among young people. Despite these attempts, issues remain, such as the survival of extreme beliefs online and the dieculty of monitoring encrypted communications. It is critical to address the socioeconomic conditions that drive radicalization completely, with an emphasis on education, employment, and social inclusion. While great progress has been accomplished, ongoing efforts and a comprehensive approach encompassing socioeconomic development, education, and international cooperation are required for long-term success in combating extremism in Indonesia.
(Indonesia)

• Getting worse and diverse but the levels of countering effort are different from the government agencies and private actors.
(Republic of Korea)

End of questionnaire

What else should we consider?

• Gender and education as well as participative form of development with cyber for peace building efforts.
(Philippines)

• These dialogues are crucial in ensuring states speak a common language on responsible state behavior in cyberspace.
(Philippines)

• CMI more role in SEA region on digital peace building.
(Indonesia)

• Holistic approach to cybersecurity beyond technical
(Malaysia)

• With the advancement in information technology, and the establishment of policies, rules and regulations, it is also important to invest in the physical resources and provide capacity building in cybersecurity in order to promote peace.
(Philippines)

• How to persuade tech companies to collaborate on these challenges.
(Thailand)

• Development of international/regional norsm in cybersecurity
(Republic of Korea)



ASEAN Institute for Peace and Reconciliation (ASEAN-IPR)

https://asean-aipr.org/
asean_ipr
@ASEAN_IPR
ASEAN Institute for Peace and Reconciliation
ASEAN Institute for Peace and Reconciliation
ASEAN IPR

ASEAN-Republic of Korea Cooperation Fund (AKCF)

https://www.aseanrokfund.com/
@akcf_pmt

ISBN 978-623-10-8634-1

9 786231 086341