INTERNATIONAL
RESEARCH
CONFERENCE

Hedayah
Countering Extremism
& Violent Extremism

8th INTERNATIONAL RESEARCH CONFERENCE

RECOMMENDATIONS FOR POLICY PROGRAMS AND RESEARCH

Written and compiled by:

Denis Suljić
Nikoline Landheim
Emma Allen

Edited by:

Kadir Akın Gözel
Anna Sherburn

The views expressed in this document are those of individuals participating in Hedayah's 2023 International Research Conference and do not necessarily reflect the views of Hedayah or the Government of the United Arab Emirates. The terms and definitions used in this policy brief are not the official terminology of Hedayah, but rather the terms and definitions used by the authors during the panel presentations and discussions.

ACKNOWLEDGEMENTS

This policy brief consolidates recommendations derived from the presentations, discussions, and debates conducted at Hedayah's International Research Conference 2023, which was held from 11-13 October 2023 in the Hague, the Kingdom of the Netherlands.

We extend our sincere gratitude to all those whose contributions made this policy brief possible. The conference organizers express deep appreciation to the speakers, moderators, facilitators, and notetakers who helped develop this brief.

INTRODUCTION

Hedayah, the International Center of Excellence for Countering Extremism and Violent Extremism, hosts an annual Research Conference to examine cutting-edge research related to current and evolving extremist, violent extremist, and terrorist threats and challenges.

The Eighth International Research Conference was convened in the Hague, the Kingdom of the Netherlands, from 11-13 October 2023. It adopted a hybrid format accommodating both in-person and online participation. Hedayah co-hosted the Research Conference with the Netherlands's International Centre for Counter-Terrorism (ICCT) and with kind support from the Ministry of Foreign Affairs of the Netherlands, the United Arab Emirates, the Government of Spain, and the Embassy of the Kingdom of the Netherlands in the UAE.

This brief provides an overview of Hedayah's 2023 Research Conference by highlighting key recommendations for countering extremism, violent extremism and terrorism aimed at informing researchers, practitioners, and policymakers. More detailed content from these presentations is available both through Hedayah's online channels and will be made available through essay contributions to an edited volume (forthcoming). The conference's Thematic Sessions are summarized below, outlining the main takeaways and recommendations derived from the presentations, discussions, and debates held during the three-day conference.

THEMATIC SESSIONS

1 Extremist Exploitation Of AI / Alt-Tech: Emerging trends and implications for intervention

The first thematic panel of the conference focused on extremist actors' harmful uses of Artificial Intelligence-based tools (AI) and social media platforms associated with the 'Alt-Tech' or 'alternative technology movement'. The session emphasized that extremists, violent extremists and terrorists are highly adaptive and continue to take advantage of the continuously evolving online ecosystems, challenging our current understanding and practices of monitoring and intervention strategies.

The panel explored the growing threat of radical right terrorism in recent years, particularly in North America and Europe. The speakers considered the threat of the radical right as the fastest-growing challenge for counterterrorism experts and law enforcement in these regions. While most radical right groups are in the preliminary stages of engaging with and discussing the potential uses of AI and Alt-Tech for harmful purposes, some groups have already utilized generative AI and social media tools for a variety of dangerous activities, including the dissemination of propaganda using synthetic media such as deepfakes, increased outreach to drive recruitment with chatbots, to research attack targets and to enable kinetic attacks.

The panelists also considered how al-Qaeda, Daesh and their respective supporters use social media platforms and AI-based tools. Examples discussed at the panel included Daesh and its supporters using popular platforms such as Telegram, Facebook, WhatsApp, and Rocket.Chat for mass file sharing via menus, as well as using AI-based tools for translation and the creation of visual propaganda. The panelists also shared examples of Bots being used for various purposes, such as adding layers of anonymity and spreading visual propaganda, which has become a common practice of al-Qaeda. ChatGPT has also been used more regularly for developing and editing text-based content and instructional materials. Furthermore, the panelists highlighted an example from Nigeria, where Daesh-associated violent extremist organizations (VEOs) use a range of digital platforms and high-tech tools such as drones, satellites, data compression and archiving softwares for planning, coordinating, and promoting their attacks.

• Challenges in Identifying Inauthenticity
• Spread of 'Rogue AI Models'
• Deployment of 'Trope Bots' on platforms

The increasing use of AI and Alt-Tech tools by extremists, violent extremists, and terrorists poses many challenges, including the challenge of identifying and responding to inauthentic content and addressing the potential dangers that may be posed by terrorist misuse of AI-models that are developing without significant regulatory constraints. The panel noted that both radical right and religiously inspired extremists have become adept at exploiting technology to enhance their reach, resiliency and impact of their online activities, including: creating and spreading visual and text-based content, including deepfakes; reaching wider audiences at a faster rate through the deployment of bots; and avoiding AI-enabled and human-based content moderation and removal. Accordingly, the panel highlighted the need to continuously stay updated on evolving online dynamics, tracking evolving propaganda and narratives, to enable policymakers and practitioners to design effective intervention, investigation and response strategies to counter VEOs' exploitation of AI and Alt-Tech in the digital space. The Breakout Session "Scanning the Horizon: Emerging Threats in Online Extremism & 'New Tech'" held during the conference complemented these findings and recommendations.

Recommendations for ***Policymakers:***

- Continue building cross-sector information sharing, collaboration and partnerships with tech companies and other relevant actors.
- Ensure that companies developing AI, AI-based tools, and providing file-sharing, social networking, and social media services are governed by mechanisms that promote or require accountability for misuse of their platforms, and provide incentives for content moderation and removal.
- Develop widespread public awareness through campaigns leveraging both traditional and new media platforms to expose the online footprints and tactics of VEOs, to build user-resilience and encourage utilization of moderation and response approaches.
- Regulate the creation and distribution of AI models.
- Strengthen cyber security infrastructures.
- Redefine counter-terrorism strategies to include more robust digital capabilities and improved tech governance.
- Dial down moral panics concerning new technology.
- Improve responsible regulation to mitigate harms that may arise as a result of AI-models and AI-based products.
- Promote blue-teaming[1] exercises related to the potential for AI & preventing and countering violent extremist (P/CVE) interventions.

Recommendations for ***Tech Sector:***

- Find solutions for the challenge of maintaining the transparency of the inner workings of AI-models and AI-based tools while diminishing the opportunities for extremist exploitation of AI technologies.
- Promote red-teaming exercises of possible extremist exploitations and uses.
- Exercise caution towards the rapid proliferation of AI products, and integrate safety by design into the development of new models and tools.
- Continue monitoring pro-Daesh online spaces with human observers, and not exclusively
- Utilize targeted approaches to disrupt extremist networks (such as targeting key 'node' accounts with bans).
- Recognize and understand how non-English and non-Arabic-speaking Daesh supporters build communities online.
- Remain updated on emerging content-moderation evasion strategies.
- Adjust intervention strategies to each platform.

[1] In the context of countering extremism and violent extremism, "red teaming" and "blue teaming" refer to strategic approaches used to identify vulnerabilities, assess risks, and improve defenses against extremist threats. Red teaming involves simulating the actions and strategies of adversaries, such as extremist groups, to understand their tactics, techniques, and procedures. The goal is to think like the enemy in order to identify weaknesses and potential attack vectors that may be exploited. Blue teaming, on the other hand, focuses on defending against the threats identified by the red team. This involves improving existing security measures, policies, and strategies to mitigate risks.

Recommendations for ***Researchers:***

- Focus on advancing research related to radical right exploitation of AI and Alt-Tech.
- Consider further research to test the effectiveness of AI in P/CVE interventions.
- Intensify research efforts to understand potential real-world threats posed by extremist, violent extremist or terrorist exploitation.
- Researchers should utilize online platforms to white-list accounts.

2 Using Strategic Communications for Engagement and Disengagement

A core tenet of terrorist attacks is that they serve a purpose beyond the immediate physical destruction caused by an attack. Terrorists use violent attacks as a means of communication, using violence to send potent messages to multiple audiences. These actions are intended to instill fear, showcase their strength, and draw attention to their causes. By targeting prominent locations or individuals, terrorists seek to provoke government responses, shape public opinion, and/or recruit new members. When attacks obtain widespread publicity, this amplifies their message, generating a psychological impact that reaches far beyond the immediate physical destruction. In this context, the panel discussion explored how differing societal responses in the aftermath of terrorist attacks can have a crucial role in determining the impact of intended communication by violent extremist or terrorist actors, exploring examples from previous attacks in Brussels, Nice, Berlin, and Manchester. The panelists explored the notion that the immediate response to a terrorist incident cannot only be operational. The symbolic dimensions of the meaning-making process following an attack – encompassing authorities' and citizens' frames, rituals, and symbols - can be key to countering the mechanisms of terrorism and enabling individuals and communities to respond collectively in a way that facilitates recovery and resilience.

The panel also explored how short-form videos can be a strategic communication tool for preventing and countering extremism and violent extremism. Platforms that emphasize short-form video content, such as TikTok, are experiencing rapid growth and widespread popularity among younger generations, including users aged 13-17 and 18-24. Accordingly, there is a pressing need to address dangerous actors' potential exploitation of these spaces. Engaging tech companies and empowering content creators with effective guidelines and resources that allow them to leverage short-form videos for countering extremism and violent extremism presents a promising approach to tackling this challenge. To increase the receptiveness of such campaigns, the panelists noted, it is important to prioritize non-technical language, focus on storytelling and localization of themes, and provide specific short-form video guidance on elements like timing and hashtags to capture the target audience's attention.

The panelists discussed pathways to increase resilience to extremist and violent extremist narratives, looking at the higher education system in Indonesia as an illustrative example. Research in this context has shown that trust in government and institutions is a major determinant of overall youth resilience to violent extremism. Moreover, challenging the violent behaviors of others is likely to boost individual and societal resilience. Other important positive resilience factors discussed during the session include diverse social networks and strong cultural identities. Regarding negative predictors, the panelists noted that those who adhere to norms justifying violence are generally less resilient to violent extremism, and generalized acceptance or support for violence against women and children correlates with low resilience. In addition, prior childhood exposure to violence or experience of violence is also considered a slight but significant negative predictor of resilience, and poor mental health and maladaptive coping mechanisms are factors that undermine resilience. Regarding future programming, the panel agreed that awareness of locally relevant resilience factors is one of the fundamental steps for designing contextual interventions.

In wrapping up the session, the panelists discussed using a strategic communications approach to build resilience to extremism and violent extremism. They stressed the need to institutionalize strategic communications in long-term programming, foster a culture of experimentation and learning, listen to what people want to learn, and work alongside local partners to craft messages for their communities. Additionally, they underscored the importance of not only equipping people with the necessary tools to disseminate narratives but also convening and providing systematic mentorship for strategic supporters. This holistic approach aims to develop an ecosystem that will turn youth into life-long advocates.

Recommendations for ***Policymakers:***

- Acknowledge the dual nature of counterterrorism and crisis management efforts – while counterterrorism operations are frequently the responsibility of the police, military, and intelligence agencies, countering the mechanism of terrorism is a collective responsibility involving all stakeholders, including citizens, communities, media, and professionals.
- Facilitate and encourage community resilience by harnessing the inherent drive of individuals to take action and leveraging the potential of solidarity.
- Institutionalize strategic communication in long-term programming and work with local partners to build messages tailored to the community.
- Collaborate with and engage tech companies in efforts to counter extremist and terrorist threats.

Recommendations for ***Practitioners:***

- Contribute evidence for strategic communications by disseminating research insights frequently so that cross-cutting teams can easily chart interventions.
- Create short, authentic, and locally themed videos focusing on storytelling. Use relevant hashtags and start with attention-grabbing visuals to capture the viewers' interest quickly.
- Work alongside local partners to build messages for their communities – sometimes innovative and online, sometimes targeted, and old school, offline.
- Convene and provide systematic mentorship for strategic supporters to create an ecosystem that will turn youth into life-long advocates.

Recommendations for ***Researchers:***

- Expand research aiming to understand terrorism's effectiveness as a 'communication strategy' and what this means for prevention and response.

3 Prevention, Moderation, and Building Resilience to Extremism and Violent Extremism Online

The third thematic session of the conference explored the online activities of extremist, violent extremist and terrorist organizations, and subsequent lessons that can be extracted for prevention, moderation, and building resilience. The panel began with a discussion on one of the most active VEOs in the Middle East region, Daesh's South-Central Asian regional branch (known as the Islamic State in Khorasan or 'IS-K'). IS-K's online activities surged following the regime change in Afghanistan in August 2021, motivated in part by a desire to maintain reach and relevance in opposition to the Taliban and to reduce the negative effects of its low-levels of field-operations in Afghanistan following regime change. IS-K has, therefore, been in direct competition with the Taliban.

The group uses social media for propaganda, recruitment, and internal communication, targeting sympathizers across South and Central Asia. The same trend has been observed in other regions, including Central Asia, Türkiye, Syria, and Iraq. IS-K integrates face-to-face and social media recruitment efforts. Social media recruitment is difficult to observe, as individuals attracted through social media platforms (mainly Telegram) are first tested and nurtured and then invited to private chats that evade tracking and detection. The panelists discussed how IS-K's online activities remain relatively unchallenged, but disruption and re-direction efforts can be key to countering them. The panel noted that one of the main difficulties in redirection is to convince prospective recruits, who already have at least some sympathies for an extremist, violent extremist or terrorist organization, to consider alternative views and engage with alternative content.

This session also explored how 'edu-tainment' e-modules can be used to educate youth about online harms, particularly extremist propaganda and misinformation. In India, for instance, SMILE (Social Media and Internet Literacy E-module) is a Mythos Lab initiative that has proven effective in enhancing students' abilities to identify and report extremist content. Endorsed by UNESCO, this e-module has been integrated into the curriculums of 35 schools across rural, urban, and metropolitan areas. Reportedly, the tool has led to major increases in the ability to identify and report extremist propaganda and misinformation, currently operating on at least 3 social media platforms. The edutainment approach has resonated well with both the audience and the press, and the SMILE project will expand to other countries in the near future, including Sri Lanka and Canada.

The panel next considered the intersection of gaming and digital socialization, radicalization risks, and resilience opportunities. While gaming can bring benefits through stress relief and community building, it is also being exploited by extremists for harmful purposes, and currently, white supremacist ideology and harassment among players are increasing rapidly. One example discussed during the panel included the role of gaming in contributing to the radicalization of the individual[s] responsible for the Buffalo Attack, a mass-shooting attack at a grocery store in Buffalo, New York, USA, which is cited to be one of the deadliest mass shooting attacks in recent American history. Other violent and/or extreme ideologies gamers are being exposed to include misogyny racism and xenophobia, antisemitism, islamophobia, and homophobia. Extremists use gaming content and gaming spaces for propaganda, grooming, communication, radicalization, recruitment, mobilization, and fundraising. To address these issues, trust and safety work aimed at improving reporting and takedown methods can be effective. More specifically, safety by design is a crucial aspect, calling for rethinking game design to anticipate potential misuse and reduce spaces for harm and abuse.

Finally, this session included an important discussion on positive interventions through gaming spaces, including strategies for utilizing the use of online gaming communities for trust building, social connection and harnessing the influence of positive influencers. In addition, applying gamification to programming to increase engagement and the scope of outreach opportunities should be one of the approaches implemented by practitioners.

Concluding the session, the panelists explored how traditional versus new media impact peoples' resilience to extremism and violent extremism. The panel highlighted insights from Sri Lanka's programming on media and resilience, which has involved training media personnel on ethical reporting methods and has engaged the youth in social media campaigns to produce viral content, as well as creating bridges to enhance exchanges between the government, religious leaders, and community members. In conclusion, Sri Lanka's experience indicates that there is a significant difference between the resilience of youth and the resilience of the general population. The panelists emphasized that those prioritizing social media as their primary source of information demonstrate lower levels of resilience to extremism.

*Recommendations for **Policymakers:***

- Convince prospective recruits to consider alternative views by offering alternative options for discharging grievances or frustrations.
- Develop tailored courses for entrepreneurial individuals seeking to prove their worth by overcoming challenges.
- Use unconventional methods, including comedy, to educate individuals about online literacy; certifications can serve as a major encouragement.
- Leverage gaming communities for trust-building and mentorship and harness the influence of positive influencers when developing P/CVE policy interventions.

*Recommendations for **Tech Sector:***

- Improve reporting & takedown methods on online platforms.
- Seek to strengthen efforts in community norm changes and online Social and Behavior Change Communication (SBCC).
- Improve both behavioural and content-based extremism and violent extremism enforcement policies.
- Enhance efforts to build "digital resilience" in gamer communities and rethink gaming design to reduce space for harm.
- Find solutions and develop methods to prevent potential abuses through gaming mechanics.
- Understand and spread awareness of narrative impacts and commit to diverse representation and accessibility.

Recommendations for ***Practitioners:***

- Apply gamification to counter extremism and violent extremism efforts to increase engagement and scope of outreach opportunities.
- Increase the impact of efforts to prevent extremism and violent extremism through the positive use of online gaming cultures, as well as identity and community formation in these spaces.
- Develop and conduct training for journalists on ethical reporting to build societal resilience against extremism and violent extremism, including through media contribution to public understanding, social cohesion and promotion of peace and stability.
- Increase focus on the programming efforts to support youth to safely use social media.
- Use of online gaming communities for trust building and mentorship.
- Facilitate positive interventions.
- Harness the influence of positive influencers.

Recommendations for ***Researchers:***

- Expand research focusing on using gaming designs as tools to reduce space for harm.
- Continue research on the narrative impacts within gaming communities.
- Utilize operational research focusing on finding whether access to media influences resilience to violent extremism.

Reimagining responses to violent extremism
INTERNATIONAL CVE RESEARCH CONFERENCE

4 Exploring Ecosystems of Online Extremism

The fourth panel explored ecosystems of online extremism, in which the presenters highlighted the need to understand evolving terrorist activities on digital platforms. This heightened understanding of evolving terrorist activities was considered to be crucial in driving efforts to prevent extremism and violent extremism in online ecosystems. The panelists noted that there are common denominators across most platforms with higher rates of terrorist content. The panel asserted that small to medium-sized file-sharing platforms in the early stages of development, primarily originating in Europe and North America, are often at significant risk of being misused by terrorist organizations. As a result, there is a need to expand public-private partnerships, particularly by increasing collaboration with start-up tech platforms to combat terrorist exploitation of their services more effectively.

The presenters also discussed patterns of online narratives among activists who are arguing for radical social change or dedicated to anti-government or anti-State agendas but who do not promote the use of violence to achieve these goals. Anti-government threat narratives, actions, and sentiments include online posts, demonstrations, riots, or other forms of agitation intended to demonstrate vocal opposition to the actions of the Government/State and to create a call to action to contest the government's legitimacy, policies, and authority through legal and non-legal means. The panelists noted that one should distinguish between anti-government extremism and anti-government sentiments – not all groups that communicate criticism of the state or government have a strong or central anti-government ideology; some rather have a set of grievances and calls to action based on their policy positions or broader anti-authority sentiments. Research from the United Kingdom has shown that religiously inspired extremists, white nationalists, and eco-radicals all have displayed animosity towards the legitimacy of the State, often justifying their hostile feelings by the incapacity of institutions to protect the social groups these organizations claim to represent and advocate on behalf of.

Subsequently, the panel conversation focused on extreme online ecosystems associated with radical right ideologies. Using Ireland as a reference point, the panel emphasized that radical right groups dedicate their online ecosystems to creating division and spreading hate-based ideologies. In some instances, this also includes a call to action. However, as explained by panelists, online activism and hate speech do not always translate into action on the ground. This calls for greater awareness of the linkage between online and offline activity. Findings also highlighted the challenge posed by the transnational nature of the threat of radical right extremism – research on the Irish context show that X (formerly Twitter) and Telegram are the most popular platforms used by Irish radical right groups, where the content identified often includes ideas imported from the US, the UK, Canada and Australia.

Finally, the panel examined pro-Daesh propaganda narratives and fundraising efforts. Examples were presented of fundraising communications from camps in eastern Syria, where extremist groups and their supporters used emotive language and imagery to solicit donations, utilising marketing tactics often seen in mainstream fundraising campaigns. Fundraising messages are disseminated in multiple languages, often via Direct Messages (DMs), to evade detection and encourage the use of various money transfer services, including cryptocurrency, for added security. In addition, some donation addresses change every 24-48 hours, and donors tend to coordinate payments in real-time with campaign operators. Donor funds are often commingled with legitimate funds at Syria-based exchanges, and funds ostensibly designated for humanitarian purposes may, in reality, be redeployed to support terrorist organization operations. The panelists explained how prominent narratives employed by violent extremist or terrorist organization include victimization, the innocence of children, desperate situations, women's purity, steadfastness against adversaries, messages of gratitude, religious citations and justification, and gendered 'guilt-tripping'. Findings demonstrate that language and imagery focusing on emotional cues have particularly been utilized in encouraging people to donate. In conclusion, the panelists agreed that pro-Daesh ecosystems need to be understood in order to develop effective counter-extremism strategies and disrupt fundraising efforts.

Recommendations for ***Policymakers:***

- Consider codifying 'hateful extremism' in legislation to support efforts to combat and prevent it.
- Enhance collaboration with start-up tech platforms to effectively combat terrorist exploitation of their services.
- Increase the security and protection of Government Officials, Lawmakers and Law Enforcement Officers involved in efforts to counter extremism and violent extremism online.
- Strengthen anti-money laundering and counter-terrorist financing initiatives in respect of emerging fundraising strategies, to continue to detect, disrupt, and mitigate pro-Daesh fundraising campaigns on their platforms.

Recommendations for ***Tech Sector and the Fintech Sector:***

- Remain aware of the language extremists use to solicit funds and how fundraising efforts may vary across platforms along with in-group signalling using specific language and imagery.
- Continue to work actively to detect, disrupt, and mitigate pro-Daesh fundraising campaigns on their platforms.
- Amplify monitoring and interventions around 'Lawful but Awful'[2] content.
- Enhance monitoring and interventions around online anti-government activism and the related potential offline harms while recognizing the legitimacy of communicating criticisms and grievances.
- Improve monitoring and interventions around countermeasures relating to circumvention of content moderation/ networked harassment/outlinking.

[2] "Lawful but awful" denotes content that is legally permissible but morally or ethically objectionable. While not breaching any laws or regulations, this content can still be considered offensive, harmful, or disturbing to some individuals or groups.

Recommendations for ***Researchers:***

- Conduct more research on why certain content is not removed from online spaces.
- Expand research on the link between online anti-government signals and offline events.
- Explore further research on soft recruitment [3] and its effectiveness.
- Increase research efforts on non-violent extremist infiltration of emerging crisis issues.
- Innovative techniques for tracking, like 'mock donations,' could be utilized to help identify terrorist financing.

5 Expanding the Field: Interdisciplinary and Cross-Sectoral Approaches in Countering and Preventing Extremism

The fifth panel of the conference focused on interdisciplinary and cross-sectoral approaches and efforts intended to counter and prevent extremism and violent extremism. Positioning conflict sensitivity and the "Do No Harm" approach as the nexus between international development and preventing and countering extremism and violent extremism opened up an engaging discussion on community resilience as part of P/CVE efforts. The presenters discussed how holistic, multi-stakeholder strategies that consider both development and P/CVE objectives are crucial in this regard. The connections between extremism and violent extremism, on the one hand, and sustainable development, on the other, go both ways—security is necessary for development, and insecurity or heavy-handed oversecuritisation can reverse development gains.

For effective programming, NGOs should promote social inclusion and address underlying grievances and factors that can affect program objectives, such as poverty, marginalization, social exclusion, gender, equal participation, inter-faith activities and inclusion of religious leaders, dialogue and cultural exchange, and injustice. Lack of consideration for such factors, the panelists argued, risks inadvertent harm and missed opportunities. Moreover, the panelists noted that NGOs could play an important role in identifying and addressing hateful speech and intolerance before it leads to extremism and that their work, skills, knowledge, and long-term experience are needed to counter existing threats. Accordingly, collaboration between traditional NGOs and CSOs seeking to develop effective programming and prevent extremism and violent extremism, as well as between tech companies, governments, communities, and implementing partners, is vital.

Interdisciplinary and cross-sectoral approaches can take many forms. The presenters encouraged stakeholders to share resources, risks, and reach. To address current multi-directional trust deficits between governments, NGOs, communities, and other actors, the panel considered it is necessary to promote transparency and inclusion in decision-making. Treating people as co-creators rather than beneficiaries can help facilitate trust-building and ownership. Governments can also support coordination by serving as a backbone institution, staying attuned to what is happening on the ground, and taking the time to listen to communities. Additionally, they should seek to remove barriers and red tape that negatively impact the effectiveness and efficacy of NGO operations. Private sector organizations,

[3] Soft recruitment to violent extremism involves the subtle and indirect approaches utilized by extremist organizations to entice and radicalize individuals. Diverging from overt and explicit recruitment tactics that openly endorse violence or extremist beliefs, soft recruitment employs nuanced and less forceful methods to lure individuals and gradually introduce them to extremist ideologies.

recognizing their vulnerabilities to extremism and violent extremism, can also contribute to supporting P/CVE networks. In sum, the panelists agreed that such efforts should be holistic and multi-disciplinary.

In adopting an interdisciplinary strategy, some key considerations highlighted during this session should be considered. First, NGOs should be wary of their approach to communities and should not repackage standard development programs as programming to counter extremism and violent extremism. Using the 'P/CVE label' can undermine NGO activities and alienate community members. Community members and partners may become suspicious that NGOs are serving a governmental or broader agenda, rather than the interests of the community. Efforts to counter extremism and violent extremism can also result in retaliation from local violent extremist actors. Consequently, it is important to distance NGOs from securitized approaches and undertake robust conflict analyses to understand local contexts and grievances before intervention. Second, host governments should be mindful of their P/CVE and counter-terrorism activities, as poorly designed programs can marginalize and stigmatize communities, which, in turn, can increase the likelihood of alienation and grievances contributing to radicalization. Third, donors should be flexible regarding their P/CVE funding. They should provide unearmarked funds to facilitate local co-design, development of cultural understanding and local credibility among personnel, and advancement of pilots and capacity-building initiatives.

Finally, the panel explored what distinguishes extremists who become involved in terrorist violence from those who do not. The presenters noted that non-involvement in terrorist violence is as much about the absence of protective factors as it is about the presence of risk factors. Relevant risk factors discussed during the session include criminal antecedents, adverse childhood experiences, access to weapons, a violent strategic logic, and gender (specifically, with males at higher risk of using violence due, in part, to socialized gender roles). Protective factors include parenting children, individual levels of self-control, and positive relationships during radicalization.

Overall, this panel underscored the need to leverage interdisciplinary approaches, increase collaboration among all relevant stakeholders, build trust within communities, and prioritize local knowledge and expertise to effectively counter and prevent extremism and violent extremism. Local approaches result in better implementation, impact, and sustainability.

Recommendations for ***Policymakers:***

- Facilitate long-term programs that enable more effective monitoring and evaluation.
- Provide flexible and unearmarked funding and commit to longer funding cycles to help make the P/CVE sector more sustainable, and to facilitate greater connectivity between P/CVE and

Recommendations for ***Practitioners:***

- Conduct needs assessment and conflict analysis regularly.
- Ensure collaboration between NGOs and other stakeholders involved in P/CVE efforts.
- Provide training to ensure that personnel have the necessary contextual and cultural understanding and local credibility before programs are initiated.
- Ensure that monitoring processes are in place and operationalized from the beginning of programs.

Recommendations for ***Researchers:***

- Conduct deep evaluative research to excavate the assumptions beneath the field of countering extremism and violent extremism. For instance, there is a need for stronger evidence that increased tolerance of difference, community connection, and inclusion reduce extremism and violent extremism.

6 Developing a Gendered Understanding of Extremism: Challenges and Responses

The sixth session of the conference explored gendered dimensions of extremism and violent extremism, focusing on challenges and responses. Security has historically been a gender-blind field. However, understanding gender dynamics and norms is essential to understanding threats and strengthening policy and programming responses. A lack of gender mainstreaming and effective gendered analysis in counterterrorism efforts leaves gaps in effectiveness, impact, and sustainability.

Further, the panelists noted that misogyny plays a key role in most extremist ideologies, and particularly across radical right ideologies and can act as a bridge from extremism to violent extremism. Where radical right ideological contexts differ, misogyny can also act as a bridge between different contexts, strengthening its 'transnational' nature.

The panel also discussed gendered dimensions in the rehabilitation and reintegration of returnees from Iraq. At the time of Hedayah's 2023 Research Conference, there were approximately 46,600 people in the al-Hol camp, with women and children making up 94%. While approximately 24,500 Iraqis remain in the camp, many have returned to Iraq. Tens of thousands are considered to be Daesh-affiliated. These people share some common features, some of which include educational disruption, female-headed households, stigmatization, rehabilitation and reintegration, and unclear long-term outcomes. Moreover, Iraq presents a complex landscape with challenges related to a post-conflict environment, outstanding grievances, documentation, legal status, and barriers to return. All of these give rise to important gender considerations, such as how these factors are experienced uniquely by men, women, boys, and girls, and how these factors can be reflected or addressed in gender-sensitive ways in rehabilitation and reintegration efforts.

Finally, the panel explored how women can be important change agents in P/CVE efforts and conflict resolution through Participatory Action Research (PAR). PAR places a strong emphasis on the participation of and action by members of local communities to understand the root causes of conflict, extremism, and violent extremism. Highlighting Somalia as an example, the presenters noted that PAR has provided safe spaces for women to engage in critical reflection, helped them understand power and agency, and legitimized their voices in driving community and grassroots-level change.

Recommendations for ***Policymakers:***

- Explore new ways to assess and address the drivers of extremism and violent extremism, especially in the transnational context of online spaces.
- Show the value of including gender mainstreaming in policies and the need for diverse perspectives at the very top.
- Focus on the role of women as community peacebuilders.
- Highlight the role of women's agency in decision-making and conflict-resolution efforts.

Recommendations for ***Practitioners:***

- Provide evidence on how and where gender mainstreaming can be included, and how it can help to improve effectiveness and impact.
- Consider factors such as age, level of development, social status, and the different experiences of men, women, and boys and girls in programming.
- Employ gender-based analysis and gender-informed support in rehabilitation and reintegration efforts.

Recommendations for ***Researchers:***

- Expand research efforts on gender dynamics to prove why gender mainstreaming is essential to security.
- Utilize research to show how gender inequality itself is a driver of insecurity, extremism, and violent extremism, and thus, why gender mainstreaming strategies need to go beyond the empowerment of women.
- Show how gaps in gender mainstreaming so far have led to failures in policy and programming.
- Empower women to drive and use research for action rather than being only the subjects of research.

7 Current Challenges in Rehabilitation and Reintegration

The seventh panel explored current challenges in rehabilitation and reintegration. Starting by examining extremism and violent extremism in Africa, the panel noted that the Sahel region has emerged as the new epicentre of violent extremism, representing 43% of global terrorism deaths. The 'center' of terrorism is moving toward countries facing political instability, conflict, and ecological degradation. Responses to extremism and violent extremism in Africa by national and international actors over the past decade have continued to be dominated by security-driven approaches. However, evidence has shown that stand-alone security responses are limited, and development-based solutions are needed to address highly localized root causes of violent extremism.

The panel explored terrorist recruitment pathways and pathways for disengagement from terrorist organizations or extremist ideologies in Africa. Reasons for recruitment include the lack of employment opportunities, low levels of access to information and communication, and the decision of family members and friends to join groups. Furthermore, the panelists noted that recent research demonstrates a relationship between a lack of religious education and susceptibility to violent extremism. The panel also noted that several recruits had experienced a trigger event, i.e. a 'tipping point' factor, such as a short, punctuated, and sharp escalation of human rights abuses, a killing of a family member or friend, or the arrest of a family member. Factors that were found to affect disengagement from terrorist groups included grievances against the group due to unmet expectations, disappointment in monetary rewards and disillusionment with the group's ideology; social influence such as disengagement by family, friends, and community members, and; government incentives and amnesty programs.

Shifting to a discussion on how strategic communication can support successful reintegration, the presenters emphasized the dangers of a one-size-fits-all approach. Highly tailored approaches to communication are required, where the community's social, political, and cultural contexts are considered. They also noted that the media plays a significant role in setting the narrative and public sentiment, and it holds considerable potential to reinforce or reduce stigma. Additionally, the panel emphasized the need to adopt long-term, whole-of-society approaches to reintegration and challenge the notion of the "job being done" when individuals are back in their communities.

Finally, the panel explored restorative and community-centered approaches to reintegrating former fighters. These approaches seek to achieve sustainable peace and reconciliation, using local definitions of justice as their roadmap while relying on investigations, facts, stories, recollections, memories, and witness statements to uncover the truth.

Recommendations for ***Policymakers:***

- Develop effective oversight of human rights compliance, rule of law, and accountability to militarized and state-centric counterterrorism responses.
- Reimagine and reinvigorate the social contract from the bottom up so that societies better serve the needs and expectations of those within them.
- Strengthen state legitimacy through improved service delivery, quality, and accountability of state service provision.
- Embed a conflict-sensitive approach in efforts to address violent extremism.
- Scale up support for localized, community-based human security approaches to prevent extremism and violent extremism.
- Reinvigorate prevention efforts within peacebuilding and sustainable development policy frameworks.
- Recalibrate commitments towards investing in cost-effective prevention and long-term development.

Recommendations for ***Practitioners:***

- Engage local communities in reintegration initiatives' design, implementation, and monitoring.
- Foster community ownership of the reintegration process.
- Contextualize programming efforts to avoid the one-size-fits-all approach and ensure early and consistent engagement and co-creation in strategic communication.
- Consider the 'emotion versus process' balance in strategic communication campaigns and ensure that strategy must prepare, mitigate, and respond to erosion risks (i.e., gradual impact and credibility weakening) to ensure intended messaging is both impactful and effective.
- Consider a long-term whole-of-society approach.

8 Understanding and Preventing Child and Youth Engagement in Extremism and Violent Extremism

The final panel of the conference discussed ways to understand and prevent child and youth engagement in extremism and violent extremism. Child association with terrorist groups presents unique protection challenges. Improving our understanding of these challenges is crucial both to enhance the capacity of professionals to devise strategies to prevent and respond to child recruitment and exploitation, and to increase the capacity of children and their environments to resist recruitment. The presenters highlighted that current counterterrorism strategies often view children who have been involved in terrorism as threats and that this sidelines child rights and development needs, and can further lead to social exclusion, stigma, and potential re-recruitment. Accordingly, there is a need for a shift towards prevention, rehabilitation, and reintegration in counterterrorism strategies.

The panel then explored research from Indonesia, Iraq, and Nigeria that has shown that children play various roles in extremist and violent extremist groups, including combat, scouting, and non-combat roles. These roles are determined by age, gender, and a range of socio-political variables - subsequently, boys and girls often face different types of violence and exploitation. While girls may suffer sexual enslavement, boys may face combat dangers and sexual assault. In addition, girls and boys face different forms of stigma and discrimination after exiting terrorist groups.

Looking at a Malaysian example, the panel discussed ways to counter and prevent violent extremism by seeking to better understand youth and rethink education approaches. This may include treating and providing support for victims of hate speech or tackling indifference and reversing sympathy towards hate speech and violent extremism. It may also include prioritizing the quest for significance and facilitating pathways to attain it, and critically, identifying and equipping young champions to counter violent extremism and hate speech. Finally, it is important to teach and advocate for non-violence, as most people would likely consider a strategy of non-violence if they were educated about its efficacy in school.

Next, the discussion shifted towards violent extremist youth subcultures in the digital space. Over the past years, there have been several mass casualty attacks tied to extremist and violent extremist subcultures online. Detection efforts have been pursued through various methods, including monitoring known sources and analyzing their output and activity, initiating investigations from a message and tracing its origins, and spotting patterns or anomalies in content trends, engagement, and sharing that might trigger further scrutiny.

Concluding the session, the panel explored ways to prevent extremism and violent extremism through youth communities, drawing insights from experiences in urban South and Southeast Asia. Examples from these contexts have demonstrated that to mobilize youth for positive action, P/CVE efforts should be relatable and fun and supported by both financial and non-financial incentives. Moreover, initiatives should focus on creating spaces for peer learning and connection-building, both at local and regional levels.

Recommendations for ***Policymakers:***

- Protect children from recruitment and actively support children's exit from terrorist groups.
- Prioritize children's rehabilitation and reintegration, and support communities to protect children.
- Expand P/CVE in education and place greater emphasis on the 'pursuit of significance' and provide children with 'options of significance' and 'routes to achieve significance' through education systems.
- Pursue social media regulation that focuses on systemic risk mitigation and transparency rather than just content removal, recognizing platform design problems that facilitate the growth of extremist and violent extremist movements.
- Recognize the transnational nature of online extremist and violent extremist youth subcultures and identify mechanisms for international collaboration that are not narrowly rooted in countering specific VEOs.
- Target urban youth in P/CVE efforts.
- Ensure flexible and long-term support, as P/CVE requires changes that take time, e.g. changes in attitudes, behaviours, and relationships.
- Aim for comprehensive P/CVE approaches by considering interconnected and context-relevant issues like disinformation, democracy, and the environment.
- Identify training and deploy young 'champions' (such as youth ambassadors) to counter violent extremism and hate speech.

Recommendations for ***Practitioners:***

- Develop new offline and online interventions to address a wide range of other extremist movements and bring people out of extremist ecosystems.
- Explore innovative approaches when designing P/CVE activities, such as sports, arts, and culture.
- Consider programmes, including curricula and community initiatives, required to raise awareness of and build resilience against threats from extremist and violent extremist online subcultures.
- Tackle indifference and 'reverse sympathy' [4] towards hate speech and violent extremism.
- Reach and teach the teachers, and build the capacity of education actors such as teachers on nonviolent conflict resolution.
- Engage external support of victims and their families and get such individuals involved electronically.
- Support communities to protect their children through awareness raising, capacity building, or other forms of targeted support.

Recommendations for ***Researchers:***

- Expand research efforts to address the lack of reliable and comparable data and evidence on child association with terrorist groups.
- Examine the unique protection risks faced by children recruited to or involved in terrorism, and the kinds of specialized responses required.
- Work to tackle indifference and reverse sympathy towards hate speech and violent extremism through continued research.

[4] "Reverse sympathy" towards hate speech and violent extremism refers to a phenomenon where individuals or groups exhibit understanding, empathy, or even support for such harmful ideologies or behaviors.

Hedayah

Countering Extremism
& Violent Extremism