STIMSON

REPORT

**Asia & Indo-Pacific**
Southeast Asia
Mekong-U.S. Partnership Track 1.5
Policy Dialogue


# Mekong-U.S. Partnership Track 1.5 Policy Dialogue on Countering Online Scam Operations

## Summary Report

April 2025

**The Mekong – U.S. Partnership** promotes the stability, peace, prosperity, and sustainable development of the lower Mekong sub-region. It further reinforces the strong and longstanding relationship among the United States, Cambodia, Lao PDR, Myanmar, Thailand, and Viet Nam. The Partnership builds upon 11 years of cooperation and progress from 2009-2020 through the Lower Mekong Initiative (LMI) to expand collaboration in the face of new challenges and opportunities. The Partnership supports the implementation of the ASEAN Community Vision 2025 and is an integral part of support and cooperation between the United States and ASEAN.

Find more about the Partnership at mekonguspartnership.org/.

**The Stimson Center** promotes international security, shared prosperity and justice through applied research and independent analysis, deep engagement, and policy innovation. For three decades, Stimson has been a leading voice on urgent global issues. Founded in the twilight years of the Cold War, the Stimson Center pioneered practical new steps toward stability and security in an uncertain world. Today, as changes in power and technology usher in a challenging new era, Stimson is at the forefront: Engaging new voices, generating innovative ideas and analysis, and building solutions to promote international security, prosperity, and justice. Learn more at stimson.org.

Note: This report reflects the combined analysis and recommendations of participants in the Policy Dialogue event. The views expressed within do not necessarily represent the views of the Department of State or the U.S. government.

Cover Photo 3D illustration of data phishing concept. Adobe Stock Image.

# ABOUT THE POLICY DIALOGUE SERIES

This summary report provides an outline and recommendations derived from discussions on needs and gaps in the Mekong region related to online scam operations, held as part of the Mekong-U.S. Partnership Track 1.5 Policy Dialogue series. The Policy Dialogues are a series of eleven conferences taking place between 2021 and 2025 that are generously supported by a grant from the U.S. Department of State's Mekong-U.S. Partnership. Cross cutting principles of inclusivity, resilience (including climate), and collaboration are applied to all conferences in this series.

The U.S. Government launched the Mekong-U.S. Partnership in 2020 to expand cooperation with the five countries of the Mekong sub-region on strategic challenges and shared priorities under the Partnership's four areas of cooperation (non-traditional security, natural resources management, economic connectivity, and human resource development). The Mekong-U.S. Partnership builds on the strengths of the Lower Mekong Initiative's development-focused agenda by cooperating on strategic sub-regional issues and challenges. Each area of engagement under the Mekong-U.S. Partnership is supported by a flagship project. The Partnership's Track 1.5 Policy Dialogue series serves as the flagship program of the Mekong-U.S. Partnership's human resources development area of engagement

# CONTENTS

# KEY ACRONYMS

| | |
|---|---|
| ASEAN | ASSOCIATION OF SOUTHEAST ASIAN NATIONS |
| CSO | CIVIL SOCIETY ORGANIZATION |
| FATF | FINANCIAL ACTION TASK FORCE |
| GASA | GLOBAL ANTI-SCAM ALLIANCE |
| GITOC | GLOBAL INITIATIVE AGAINST TRANSNATIONAL ORGANIZED CRIME |
| INGO | INTERNATIONAL NON-GOVERNMENTAL ORGANIZATION |
| INTERPOL | INTERNATIONAL CRIMINAL POLICE ORGANIZATION |
| IOM | INTERNATIONAL ORGANIZATION FOR MIGRATION |
| LEAS | LAW ENFORCEMENT AGENCIES |
| MLAT | MUTUAL LEGAL ASSISTANCE TREATIES |
| MOU | MEMORANDUM OF UNDERSTANDING |
| MUSP | MEKONG-U.S. PARTNERSHIP |
| NBTC | NATIONAL BROADCASTING AND TELECOMMUNICATIONS COMMISSION (THAILAND) |
| NGO | NON-GOVERNMENTAL ORGANIZATION |
| SEZ | SPECIAL ECONOMIC ZONE |
| SOM | SENIOR OFFICIALS MEETING |
| SOP | STANDARD OPERATING PROCEDURES |
| TOC | TRANSNATIONAL ORGANIZED CRIME |
| UN | UNITED NATIONS |
| UNODC | UNITED NATIONS OFFICE ON DRUGS AND CRIME |
| UNOHCHR | UNITED NATIONS OFFICE OF THE HIGH COMMISSIONER FOR HUMAN RIGHTS |
| USIP | U.S. INSTITUTE OF PEACE |
| VOIP | VOICE OVER INTERNET PROTOCOL |
| YSEALI | YOUNG SOUTHEAST ASIAN LEADERS INITIATIVE |

# A NOTE FROM THE CONFERENCE CHAIRS

The ninth Mekong-U.S. Partnership Track 1.5 Policy Dialogue on Countering Online Scam Operations was held in Bangkok, Thailand from October 16-18, 2024. The Policy Dialogues are a series of eleven conferences taking place between 2021 and 2025 which explore solutions to key policy and sustainability challenges in the Mekong sub-region. This ninth Policy Dialogue focused on online scam operations in the Mekong sub-region, with a particular focus on preventing scams and trafficking, role of media and civil society, assisting trafficking victims, multilateral collaboration, and regulatory efforts related to special economic zones and casinos, digital finance, and telecommunications.

Over 90 experts and civil society members participated in in-person activities throughout the three days of the Policy Dialogue in Bangkok. Approximately 46% of the attendees came from one of the five Mekong countries, with 20% coming from the United States and 16% coming from other countries in ASEAN, India, and China. The remaining expert speakers came from development partner countries including the United Kingdom, Australia, Canada, Japan, France, Austria, and Italy. Over half of the attendees (56%) were women. Government institutions were well represented at 38% of all attendees, with 27% from civil society organizations, 13% from the private sector, 11% from academia and/or think tanks, 8% from international organizations, and the remaining participants from the media. Just over a quarter of the speakers were rising experts under forty.

We deeply appreciated support from the U.S. Department of State and the Mekong-U.S. Partnership for this Policy Dialogue. In particular, the team would like to thank Katie Jo Younkins, Joshua Boyce, and Mackenzie Hale at the U.S. Department of State Bureau of East Asian and Pacific Affairs. We also appreciate the support from Adam Ross and Caratlux Liumpetch with the U.S. Embassy in Bangkok. We owe appreciation to Kristina Amerhauser with the Global Initiative against Transnational Organized Crime (GITOC) and Himal Ojha with the UN Office on Drugs and Crime (UNODC) for networking support and outreach to speakers.

All of these and others contributed to an interactive and impactful Policy Dialogue. We would also like to thank our over ninety presenters and attendees for engaging actively during the discussions. While this dialogue has concluded, the Stimson Center's Cyber and Southeast Asia programs will continue to promote international coordination and harmonization in this area, including to better understand how laws, norms, and standards can help to counter the negative impacts of online scam operations in coming years, and cultivate a community of practice.

Sincerely,

Courtney Weatherby
The Stimson Center Southeast Asia Program
Co-Chair

Allison Pytlak
The Stimson Center Cyber Program
Co-Chair

# EXECUTIVE SUMMARY

The ninth Mekong-U.S. Partnership Track 1.5 Policy Dialogue took place on October 16-18 in Bangkok, Thailand to explore gaps, challenges, and opportunities to counter online scam operations across themes such as prevention of scams, role of media and civil society, multilateral collaboration, and regulatory efforts related to special economic zones (SEZs) and casinos, digital finance, and telecommunications.

Photo: Conference photo taken on October 16, 2024, in Bangkok, Thailand.

This ninth dialogue was a deep dive into needs and gaps in the Mekong sub-region related to countering the rapid expansion of online scam operations and cyber scam compounds, with a focus on ways to prevent scams and trafficking, the important roles that civil society and media play in exposing and responding to scams, multilateral collaboration, and ways that technical and regulatory responses in key sectors like SEZs, casinos, telecommunications, and digital finance can help counter scams and fraud. Cyber-enabled crime was discussed in May 2023 at the sixth Policy Dialogue, and this October 2024 Policy Dialogue built on previous explorations with a deeper focus on cyber scam compounds. Participants explored policy challenges, best practices, and case studies from the Mekong sub-region, ASEAN, and international partners including the United States, Australia, and the UK. Cross-cutting values of inclusivity, resilience (including climate), and collaboration framed the sessions and were woven into the key takeaways and recommendations.

## POLICY RECOMMENDATIONS INCLUDE:

- **Develop governance and oversight systems that provide guidance on the complexity of scams.** Given that scams are often run by transnational organized crime networks, feed into complex systems of money laundering, and involve a wide range of actors, it can be difficult for working level law enforcement officials to appropriately respond. International organizations and national authorities should monitor and evaluate the guidelines provided to frontline law enforcement officials, ensuring they are up-to-date and have sufficient context for identifying next steps. Analysts should explore the current state of scamming to raise awareness and lay out a plan for future actions. NGOs and civil society organizations (CSOs) should workshop best practices for investigations with a victim centered approach.
- **Legally binding codes or laws are needed for companies to actively address scam operations on their platforms.** Voluntary approaches by companies are beneficial and should actively guide legislation but currently are insufficient given the proliferation of platforms. G20 nations should coordinate licensing standards to prohibit online platforms from facilitating online scam operations. Social media companies and other platforms which unwillingly host scam posts should improve support for users and improve reporting on responsive activities to government agencies and the public.
- **Convene specialists from communities of practice related to the scam operations issue to collaborate, educate, and act.** Existing mechanisms and communities of practice are unprepared for the complexity and cross-cutting nature of scam operations, and many operate within sectoral bubbles. Governments should form working groups across agencies and levels to share intelligence for the purpose of taking action at strategic and operational levels. CSOs and NGOs should expand on convenings for information-sharing and coordination on best practices. Private sector actors should create a shared platform and process to share lists of suspicious or flagged individuals.
- **Strengthen the national implementation of existing agreements and regional efforts.** Regional bodies like ASEAN may set priorities and inform regional standards, but implementation is hampered by a lack of political will as well as corruption. National authorities should develop action plans for implementation of regional commitments. International organizations, think tanks, and development agencies should provide capacity building on a range of technical, legal, and policy gaps to relevant agencies.

# AGENDA FOR MEKONG–U.S. PARTNERSHIP TRACK 1.5 POLICY DIALOGUE

| DAY 1 | October 16, 2024, from 9:00 AM - 7:00 PM<br>Bangkok, Thailand |
|---|---|
| 8:30–10:00 am | **Opening Plenary**<br><br>**Overview of Scam Center Threat**<br>This panel session included brief overviews of the challenges that scam compounds and transnational criminal organizations pose to both regional citizens and governments as well as the broader world.<br><br>**Sectoral Scam Challenges**<br>This panel session hosted experts from the media, local civil society organizations, and social media to explore how scams pose specific challenges to their sectors and workstreams. |
| 10:30 - 11:00 am | **Coffee and Tea Break** |
| 11:00 am - 12:00 pm | **Breakout Group Discussions**<br>*Attendees joined one of five assigned breakout groups for a facilitated interactive discussion exploring responses to the opening keynote presentations.* |
| 12:00 - 1:30 pm | **Lunch** |
| 1:30 pm - 2:15 pm | **Session A: Preventing Scams and Trafficking**<br>This panel session convened private sector and non-government stakeholders to explore what can be done to prevent citizens from becoming victims of scams and trafficking to work in scam centers. Points of discussion included how social media companies and government agencies work to raise awareness among potential victims of trafficking and/or fraud , how social media platforms can prevent scams from reaching target audiences. and what type of tracking and information-sharing approaches are needed to identify likely scammers or scam posts and deter such behavior. |
| 2:15 pm - 3:00 pm | **Session B: Role of Media and Civil Society in Countering Scam Centers**<br>This session explored the role of civil society and media in countering scams, as well as highlighted the current threats facing these institutions and actors, including but not limited to arrest or physical safety considerations. Topics of discussion included press regulation and freedom, the need for journalism and non-governmental organization (NGO) rescue and assistance efforts, and ways to do-no-harm and manage risks to the actors addressing scam center operations and issues. |
| 3:00 pm - 3:30 pm | **Coffee and Tea Break** |
| 3:30 pm - 4:30 pm | **Breakout Group Discussions** |
| 4:30 pm - 5:30 pm | **Session C: Discussion: Prioritizing Lines of Effort**<br>There are numerous lines of effort to tackle online scam operations, including education and awareness raising to reduce the likelihood people will fall for scams as well as regulatory and technical efforts to prevent and disrupt scam activities. This session hosted a constructive discussion between three experts, each of whom laid out a pathway to address low-hanging fruit related to either educational or regulatory lines of effort and make a case for prioritizing related activities. Panelists discussed which lines of efffort have the greatest low hanging fruit and should be prioritized for urgent attention as well as how civil society, private sector, and other non-government stakeholders can drive innovative policy efforts and support rapid responses. |

| DAY 2 | October 17, 2024, from 9:00 AM - 5:00 PM<br>Bangkok, Thailand |
|---|---|
| 9:00 am - 9:45 am | **Session D: Protecting and Assisting Trafficking Victims**<br>This session focused on the necessary resources and processes to assist trafficking victims trapped in scam compounds, challenges related to helping them get out, and case studies of what has worked and what new challenges have emerged over the last year as scam centers moved location and responded to crackdowns. The session covered a range of efforts by civil society actors, including consideration of how to address the forced criminality aspect of these trafficking victims. |
| 9:45 am - 10:30 am | **Session E: Multilateral Collaboration and Coordination**<br>Overseas scam operations currently operate out of Southeast Asia, but this issue has begun metastasizing to other regions and the victims of both scamming and trafficking are global. What multilateral tools and processes are needed to help combat scam centers? How do existing international laws and institutions addressing cyber-crime and trafficking-in-persons provide opportunities for effective response? And what opportunities exist for coordination between key multilateral institutions and non-government actors working to address cyber scams? This session explored these questions, including discussion of existing legal frameworks which could be applied to scam compounds. |
| 10:30 am - 11:00 am | **Coffee Break** |
| 11:00 am - 12:00 pm | **Breakout Group Discussions** |
| 12:00 - 1:30 pm | **Lunch** |
| 1:30 - 2:15 pm | **Session F: SEZ and Casino Regulations and Fighting Scam Centers**<br>Investigations have indicated that scam center operations are often located in areas such as special economic zones, which tend to operate outside normal policing jurisdictions. This session explored how better regulation of special economic zones (SEZs), casinos, and the key means of exchange that they use—including but not limited to cell tower access, electricity access, and transport routes—could help prevent the use of these locations for scam operations. |
| 2:15 pm - 3:00 pm | **Session G: Regulating Digital Finance to Counter Scams**<br>Government regulations and business practices can help prevent the use of cryptocurrencies and financial systems for use in scams, while still facilitating legitimate business. How could existing financial regulations and cautionary screening measures by financing institutions be improved to prevent fraud? This session highlighted case studies of success and gaps given recent technological trends, with reference to applicable lessons from similar efforts for other financial crimes. |
| 3:00 pm - 3:30 pm | **Coffee Break** |
| 3:30 pm - 4:15 pm | **Session H: Role of Telecommunications Regulators to Counter Online Scams**<br>This session addressed the role of telecommunications providers and regulators to counter online scams by preventing avenues of outreach and contact through efforts such as reducing robocalls, managing Voice over Internet Protocols (VOIP) calls, and improving verification of text and phone calls. The session highlighted case studies of improved security and verification standards and protocolsto reduce scams as well as challenges or obstacles in adopting such standards. |
| 4:15 pm - 5:30 pm | **Breakout Group Discussions** |

| DAY 3 | October 18, 2024 from 8:30 AM - 1:30 PM ICT<br>Bangkok, Thailand |
|---|---|
| 8:30 am - 11:30 am | **Synthesis Workshop: Key Takeaways Polling & Discussion**<br><br>*This session included an interactive Mentimeter poll where participants ranked the top challenges identified during Days 1 and 2. They then moved into breakout groups for a facilitated, participatory discussion and group work to identify potential solutions, policy recommendations, and key actors in addressing their chosen theme's challenges.* |
| 11::30 am - 12:15 pm | Closing Plenary Panel |
| 12:00 - 1:30 pm | Lunch |

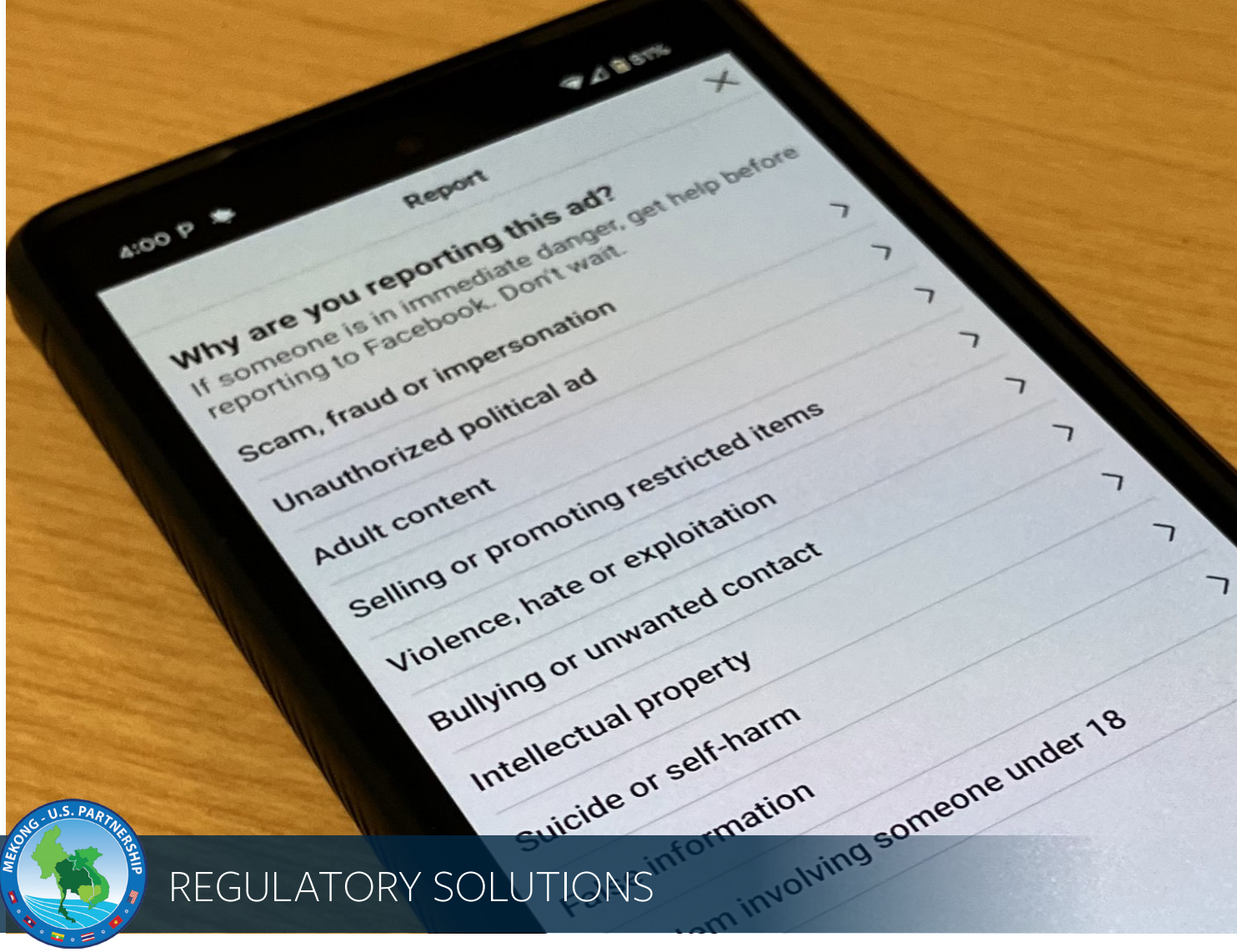
Photo: Synthesis workshop activities at the Policy Dialogue in Bangkok, Thailand on October 18, 2024. Photo courtesy of Courtney Weatherby.

## THEMATIC AREAS AND RECOMMENDATIONS

The key concerns and recommendations related to the thematic categories discussed in this report are the result of an interactive workshopping process conducted with Dialogue participants on Day 3. Throughout the conference on Days 1 and 2, the organizing team took detailed notes on the specific concerns, challenges, and gaps that were identified during session presentations and discussions. Key problems were identified across six thematic cross-cutting categories covered during the conference sessions: technical solutions, regulatory solutions, effective implementation, education and awareness-raising, risk mitigation, and regional collaboration and coordination.

Attendees ranked the top problems in each category through an interactive Mentimeter poll and then split into self-selected thematic breakout groups to collaboratively identify and draft policy recommendations to address the top issues identified in the poll. The breakout groups collectively drafted policy recommendations and solutions for seventeen individual issues and presented them to the group for a final voting process. The top two to three recommendations for each theme, as determined by the participants through this voting process, are included in this summary report.

Photo: Synthesis workshop activities at the Policy Dialogue in Bangkok, Thailand on October 18, 2024. Photo courtesy of Courtney Weatherby.




# REGULATORY SOLUTIONS

While online scam operations thrive in ungoverned spaces, regulatory frameworks and legislation passed by both national governments and coordinated through major regional bodies can improve both prevention and enforcement efforts. Many private sector actors who control social media or finance platforms will voluntarily identify gaps and weaknesses to protect their businesses, but there is a need for further information-sharing and standardization both within industry and through governmental frameworks to ensure that such approaches are widely adopted in ways that can help limit or deter scams. Improved regulation and harmonization of legal frameworks related to issues as wide-ranging as human trafficking, money laundering and virtual assets, investigation, and information-sharing could pose significant obstacles to scammers.

Regulatory solutions were woven into the fabric of multiple sessions across the Policy Dialogue. Suggested responses from sessions on Day 1 included establishing national scam centers to centralize reporting and improve information sharing with key industries; improving control over access to new bank accounts and phone numbers; taking steps to make government or authority figures harder to impersonate; as well as protecting freedom of speech and press to ensure coverage of scam and fraud issues. An often-highlighted gap was the lack of awareness or education among regulatory agencies of technical details of how scams operate, with implications for evidence collection and resourcing for investigation. Regulatory responses to scam challenges within individual industries were discussed in targeted sessions on SEZs and casinos, digital finance and cryptocurrency, and telecommunications during Day 2. Relevant takeaways for these sectors included improved use of AI detection systems for social media and financial monitoring to flag bad actors; regulating telecommunications services to avoid deception or impersonation; establishing mutual legal assistance treaties (MLATs) to improve information and evidence sharing across national borders; and improving information-sharing between key industry actors on bad actors to prevent them simply jumping between companies.

Photo: Cell phone screen showing Facebook scam or fraud report option, courtesy of Pamela Kennedy.

## PRIORITY ISSUES AND POLICY RECOMMENDATIONS:

1. **Legally binding codes or laws are needed for companies to actively address scam operations on their platforms.** Participants reported that while major social media platforms do have avenues to report scam posts or actors, reports often do not result in any obvious action and there is no way to follow up to see what was done. Voluntary approaches by companies are a beneficial start and should actively guide legislation but currently are insufficient given the proliferation of platforms.
    - G20 nations should coordinate enactment and enforcement of consumer protection laws and licensing standards to prohibit online platforms from facilitating online scam operations.
    - Social media companies and other platforms which unwillingly host scam posts should improve support for users and partner organizations when reporting fraud. They should also improve reporting to government agencies and the public on responsive activities.
    - Tech companies, regulators in individual countries, and multinational industry groups like the Global Anti-Scam Alliance should engage with one another more regularly to identify ways to effectively improve information sharing with respect to privacy and freedom of speech considerations and then build these into law. Such information sharing can also help streamline regulations across national boundaries, avoiding patchwork solutions.

2. **Global institutions, regional and subregional organizations like ASEAN, and national governments should adopt UNODC indicators of "Trafficking-in-persons for forced criminality" for screening potential victims of trafficking for cyber enabled crime.** Currently, forced online scammers are often not treated as victims due to poor screening processes, limited judicial regulations and protections, as well as insufficient evidence of trafficking under existing definitions. The UNODC has proposed specific indicators and definitions for Trafficking in Persons for forced criminality. Improving screening is vital as the situation inside scam compounds becomes more complex, with increased criminal professionalization of the cyber scam industry.
    - National governments should adopt and apply shared definitions in domestic legal and regulatory frameworks.
    - International organizations, NGOs, and labor agencies should provide training to law enforcement and other frontline actors on the latest tools and screening procedures.
    - Governmental and non-governmental frontline agencies including law enforcement, rescue organizations, lawyers, and civil society organizations should build up-to-date screening indicators on TIP for FC to accurately identify victims into processes.
    - Rescuers and post-rescue support should prioritize reintegration and support as victims navigate the legal process to help victims avoid being trafficked again.

3. **Governments should create legal mechanisms that facilitate the collection and sharing of investigative information by law enforcement agencies (LEAs) and its application as evidence to prosecute crimes.** In many cases countries lack evidence to conduct specialized investigations across national borders and jurisdictions, despite the transboundary nature of the crimes. Even when evidence is collected, privacy and information-sharing regulations limit the ability to share information across agencies or across national borders where it could be used for prosecution.
    - National governments should establish independent external bodies to support and hold law enforcement accountable for investigating and prosecuting scam operations, including preventing and penalizing corruption.
    - The international community should exert pressure on national governments as needed to achieve accountability frameworks.
    - Judicial systems and law enforcement investigators should modernize regulations and approaches to allow for remote investigative discussions and video or call-in testimony across jurisdictions to ensure that victims can testify after being rescued and returning home.


# TECHNICAL SOLUTIONS

Although organizations responsible for coordinating online scam operations have proven to be flexible and quick to respond to barriers, technical solutions can hinder scammers' access to key sectors like telecommunications or banking. While these are not copy-and-paste approaches, successful efforts in individual countries can be adapted to inform effective approaches in other countries. Adopting multi-pronged approaches which block or inhibit scammers' access to victims, improve identification and tracking of problematic accounts, and improve information-sharing between government and other actors can help reduce scam success rates and thus losses to scams. In Australia, adopting a series of such measures resulted in over a 30% reduction in financial losses between 2022 and 2023.

While case studies of effective responses were discussed in many of the Policy Dialogue sessions, four sessions at this Policy Dialogue touched specifically on technical and regulatory solutions to inhibit or limit online scam operations. The first focused on prioritizing lines of effort to make the best use of limited resources, with speakers sharing case studies from Australia related to improved information-sharing between government and financial institutions, highlighting the need to improve transparency and accountability to make it harder for scammers to imitate governments, and opportunities to address online scam operations through existing mechanisms to reduce exploitation for migrant workers. The other three sessions focused on key industries, looking at regulations and technical responses related to special economic zones and casinos, digital finance regulations, and telecommunications.

Photo: Photo of computer screen with security information courtesy of Flickr user Jim_McGlone and used under a creative commons license.

## PRIORITY ISSUES AND POLICY RECOMMENDATIONS:

1. **Convene specialists from communities of practice related to the scam operations issue to collaborate, educate, and act.** Existing mechanisms and communities of practice are currently unprepared for the complexity and cross-cutting nature of scam operations, and many operate within sectoral bubbles. Illicit actors have a high degree of connectivity across sectors, requiring a multifaceted response. Effectively identifying and implementing technical solutions to deter, prevent, or limit scam access requires coordination across silos.
    - National government agencies should form working groups of specialists across sectors at the global, regional, and national levels to share regular updates, intelligence, and trends in-person and online for the purpose of taking action at the strategic and operational levels.
    - Civil society organizations (CSOs), NGOs, and private sector groups should similarly create and expand on convenings such as the Global Anti-Scam Summits run by the nonprofit Global Anti-Scam Alliance (GASA) for information-sharing and coordination on best practices.
    - Private sector actors should create a shared platform and process to share lists of suspicious, flagged, or banned individuals and accounts with other businesses and government agencies.
    - Create a diverse, multi-track study group drawing from government and non-government experts to identify and share information on infrastructure, technology, and suspicious behaviors connected to scam activity.

2. **Develop collaborative frameworks to increase, consolidate, and share aggregated, non-personal scam data among key stakeholders, while ensuring privacy.** Currently, insufficient data on victims, impact, scamming approaches and techniques, and scale of scamming and fraud operations make it hard for governments to respond in a targeted way. Sensitivities and legal requirements to ensure privacy can complicate information-sharing efforts. And many actors view scams as individual cases rather than a coordinated effort by criminal actors, inhibiting resourcing and attention to the issue set.
    - Researchers, analysts, and open-source intelligence experts should focus on data trends, case studies, and insights to create targeted responses and share them widely through communities of practice and information-sharing efforts.
    - The intergovernmental Financial Action Task Force (FATF) and other anti-money-laundering efforts should include scam activities within their scopes of mandate given connections to organized crime and money laundering.
    - The FATF should allow non-financial institutions such as social media platforms or messaging apps to file suspicious transaction reports related to suspected scam activities since they often initiate outside the financial network.
    - Think tanks, civil society organizations, and research institutions should convene regular study groups to share information and seek to fill data gaps about the techniques that scammers use and the broader threat landscape.
    - National governments and international development organizations should increase funding for researchers and NGOs to collect needed data, and the private sector should increase budgets for data management and analysis.
    - Governments should consider targeted legal amendments as needed to allow for data sharing between private sector actors, which is often inhibited by current privacy mandates.

# EFFECTIVE IMPLEMENTATION

Online scam operations are rapidly diversifying their activities and using increasingly sophisticated technologies to evade detection. A smarter tactical approach can improve information sharing and reporting on problematic accounts. Lessons can be learned and scaled up such as the adoption of national anti-scam centers, mutual legal assistance treaties that can lead to effective cross-agency collaboration on investigations and arrests, and public-private partnerships to improve information-sharing and reporting on problematic accounts. However, even when laws or regulations provide a framework, barriers to implementation can inhibit effective responses.

Effective implementation of efforts to combat scams—and barriers to them—underpinned most discussion throughout the Policy Dialogue. Positive case studies presented included methods to identify and halt mule bank accounts, efforts from social media platforms, governments, and other actors to enhance AI detection and monitoring, as well as building close and effective collaborative ties between civil society groups and with relevant government agencies to respond to reports. Key challenges to effective policy implementation included capacity and resourcing limitations, corruption and influence of criminal organizations, economic crisis being a push factor for migration and vulnerable workers, and the rapidly increasing availability and accessibility of AI, deepfakes, malware, and other new technology services for bad actors.

Photo: Raided gang-run internet 'scam farm' in Manila, the Philippines. Photo courtesy of United Nations Office on Drugs and Crime Flickr account and used under a creative commons license.

## PRIORITY ISSUES AND POLICY RECOMMENDATIONS:

1. **Improve corporate accountability for social media owners and platforms through improving regulations and responses to scam posts.** Social media platforms are often a starting point for both fake job posts and advertisements that lead to human trafficking and for outreach to potential scam victims. However, navigating social media platform processes to report and remove false posts is complicated and often a black box for those who report. Follow up information is often not provided and somtimes no clear actions are observed after scam accounts or posts are reported through identified channels, creating uncertainty among some practitioners about the effectiveness of such channels for reporting scams and bad behavior.
    - Data privacy rules such as the General Data Protection Regulation (GDPR) in the EU should be scaled up and enforced as a tool to prevent circulation of personal information which can be easily accessed by cyber and other criminals for scams. Social media platforms should engage CSOs and international development organizations in developing and revising community standards.
    - Telecoms regulators, in coordination with law enforcement, should be tasked and empowered to monitor and verify fake job postings that attract victims of human trafficking. They should also coordinate with social media platforms to flag problematic posts that slipped past internal monitoring mechanisms.
    - To address technical capacity gaps, national governments should require social media operators to report on monitoring and effective responses, including data on algorithms used and their effectiveness.
    - Private sector companies—particularly social media and other hosting companies—should proactively verify and remove fake profiles or job posts when reported. They should also provide follow up information after a report to avoid perceptions that reporting mechanisms are black boxes.

2. **Governments, international development partners, and private sector actors should take steps to mitigate both grand-level corruption and low-level corruption through a mix of top-down and ground-up efforts to raise accountability and make corruption more costly for bad actors.** Corruption inhibits policy and regulatory implementation, particularly in relatively unregulated areas such as special economic zones.
    - National governments should improve scrutiny on political appointee roles susceptible to corruption.
    - National authorities should define and distinguish roles and responsibilities for different agencies and empower specific bodies to do specific functions related to oversight.
    - Anti-corruption bodies similar to Malaysia's Anti-Corruption Commission should be created in countries which do not have them and provided with independence.
    - International and regional platforms should prioritize efforts to tackle corruption amid existing mandates, such as for the ASEAN Intellectual Property Working Group, the ASEAN Senior Officials Meeting on Transnational Crime (SOMTC), and ASEAN Ministerial Meeting on Transnational Crime.
    - Establish channels for high-level law enforcement and government authorities to access grassroots stakeholders directly and bypass middlemen, similar to the National Broadcasting and Telecommunications Commission (NBTC) in Thailand.
    - Raise awareness-building and public discourse to address low-level corruption.

    Corruption is particularly pervasive in SEZs and other areas which currently host scam compounds with relative impunity. To address corruption in SEZs and other underregulated areas:
    - National governments should identify and empower task forces for regulating SEZs and enable easier access to SEZs by enacting relevant laws.
    - Researchers from government agencies, think tanks, and consultancies should objectively evaluate the performance of provincial bodies in SEZs and identify those bodies which need greater oversight or resourcing from national authorities.
    - International fora should be utilized to advocate for specific policies and regulations with national governments and the private sector to reduce risk and improve accountability in SEZs and other unregulated zones without inhibiting economically productive activities.
    - International development partners should make corruption more costly for bad actors through utilizing foreign policy tools such as targeted sanctions and acting to empower and protect whistle blowers.


# RISK MITIGATION

Journalists who cover online scam operations, civil society groups which provide support to victims, and other advocates often put themselves at risk by opposing the interests of powerful, well-funded criminal groups which run online scam operations. This is compounded by the location of scam compounds in relatively ungoverned areas with operating environments not conducive to free press or civil society access. Many organizations which provide victim support can do so in part because they work under the radar and preserve the anonymity or privacy of those who provide support. Even while government agencies are increasingly aware of the negative impacts of online scam operations, forging effective partnerships can be difficult given complicated and sometimes fraught relations between government agencies, media, and civil society organizations. And cyber crime laws which provide some mechanisms to respond to online scam operations can often be driven by security considerations, but have broader implications for human rights, freedom of speech, and digital economic growth and innovation.

Managing risk to key actors and following “do no harm” principles through interventions were given particular attention in two sessions at the Policy Dialogue. The session on preventing scams and trafficking included insights about the need to build trust between civil society and government agencies through MOUs and clear communication on shared goals of combatting trafficking, as well as active engagement with often marginalized communities which are targets for trafficking or scams. The session on the role of media and civil society highlighted the physical dangers that can be faced by journalists and frontline actors seeking to provide victim assistance, with experts emphasizing that without information such actors provide, governments and other international actors will not have the necessary data and insights to address online scam operations. Experts further emphasized additional funding and human resourcing is needed to ensure effective coverage.

## PRIORITY ISSUES AND POLICY RECOMMENDATIONS:

1. **Lessen distrust between government and non-governmental stakeholders.** In many localities there is a lack of trust and effective communication between government agencies and non-government actors such as media, civil society, and non-government organizations. Government agencies often view non-governmental actors as potentially interfering with their activities.
    - UN agencies such as UNODC or the UN Office of the High Commissioner on Human Rights can share case studies of effective coordination and help to broker greater trust between key frontline actors.
    - International development partners such as the United States, Australia, the UK, and others can better provide resources and technical assistance to CSOs to incentivize engagement on this issue set.
    - ASEAN and the Mekong-U.S. Partnership should utilize existing SOMs and other high-level meetings to identify successful partnerships between governments, private sector, and civil society.
    - Media outlets can broaden coverage and support journalists through cross-posting reporting from countries with less censorship, such as Thailand, to outlets in countries with more controlled space.
    - International NGOs, development agencies, and think tanks can do more to support effective relationships through bringing government and civil society to the same table, such as at this Policy Dialogue.

2. **Police and law enforcement should take steps to build trust in hotlines and government agencies among victims and civil society actors**. Governments often adopt a paternalistic approach toward victims of scams and trafficking, but this can lead to victim-blaming and erodes trust in a government's ability to respond to trafficking and scams.
    - Police and ministries of justice should provide equitable and appropriate resources for reporting hotlines and should mandate and incentivize rapid responses from hotline reports.
    - Tech companies such as Google should ensure that the top results for assistance hotlines are to legitimate sources rather than to faux hotlines run by scam compounds.
    - International partners and organizations such as INTERPOL and UNODC should increase law enforcement capacity building for victim centered approaches, interview sensitivity, and other best practices.
    - Law enforcement agencies should establish cooperation mechanisms with embassies and CSOs through MLATs, MOUs, and appointment of liaison officers where appropriate.
    - International embassies should coordinate with law enforcement to ensure translation and other support for victims from their countries.
    - Funders should increase support and resourcing for NGO-run hotlines and victim assistance.

3. **The community of practice working on trafficking and online scam operations should collectively take steps to reduce security risks to a wide range of frontline actors**. Currently uncertainty about security and a lack of physical safety in operating environments inhibits reporting and reduces the ability of some CSO/NGO organizations to achieve full impact. These risks may come from government, scammers and TOCs, or even the media inadvertently doing harm through reporting on ongoing investigations.
    - UN agencies and the international community should speak publicly in support of frontline practitioners from CSOs, NGOs, and the media.
    - Regional and local CSOs should create a trusted information-sharing platform to refer cases to the most suitable organization and ensure families and victims can verify hotlines and credentials.
    - The UN and international organizations should strengthen independent monitoring of the security situation of victims and practitioners.
    - National governments should improve laws to provide more protection of frontline actors from media and civil society.
    - Law enforcement, civil society organizations, media, and other frontline actors should receive baseline training on trauma to inform their care and engagement approaches.

Photo on Opposite Page: Photo of communication through storytelling training program for counter-trafficking issues by USAID Thailand Counter Trafficking in Persons, courtesy of Winrock USAID Thailand CTIP.


# EDUCATION AND AWARENESS RAISING

Online scams have become a major scourge in recent years, with INTERPOL estimating that they now bring in about $3 trillion USD a year in illicit finances globally. Scam compounds across Southeast Asia are estimated to host approximately 300,000 people, many of whom were lured in by posts for legitimate jobs and then trapped, held against their will, and forced to participate in criminal scam and fraud activities. This issue has metastasized since the COVID-19 pandemic, and there are awareness gaps across the board. Traffickers have historically targeted vulnerable populations, but increasingly workers targeted by scam operators are well-educated people who do not fit historic victim profiles and may not be aware of the prevalence of job recruiting scams. Victims of scams can be of any age and can be targeted by scams ranging from romance scams to cryptocurrency investment to government impersonation. Targets include both those who lack digital literacy and those who are young and considered digital natives. Online scams are among the most experienced crimes globally, yet victims are often stigmatized for having fallen for them, do not report them to authorities, and do not talk about their experiences. And when they do report them, in many cases law enforcement lacks the technical expertise to investigate or may be unwilling to take on cases where victims sent money willingly under fraudulent circumstances.

Awareness of online scams—and education about how to identify or avoid them—came up numerous times and in different contexts throughout the Policy Dialogue. Most conversations touching on education and awareness raising included improvements to digital literacy amid rapidly expanding digital economy, as well as improving general awareness about scams among the general public and improving nuanced understanding about how scams happen among law enforcement and industry representatives. Three sessions focused specifically on awareness. On Day 1, speakers and participants raised the need for more outreach to targeted communities through social media and community engagements, as well as more support for media reporting on these issues for public education purposes. Participants also identified low-hanging fruit for governments to improve transparency and make authority figures or government websites harder to impersonate.

Photo: Spot a scam poster, Belfast (March 2018). Photo courtesy of ALbert Bridge and reused under a creative commons license.

## PRIORITY ISSUES AND POLICY RECOMMENDATIONS:

1. **Develop governance and oversight systems that provide guidance on the complexity of scams.** Given that scams are often run by transnational organized crime, feed into complex systems of money laundering, and involve a wide range of actors from different sectors, it can be difficult for working level law enforcement officials to appropriately respond. Education about appropriate responses and steps for investigating scams is needed for law enforcement and judicial system officials who deal with cases.
    - International agencies like INTERPOL, international organizations, and national authorities should monitor and evaluate the current guidelines provided to frontline law enforcement officials, ensuring they are up-to-date and provide sufficient context for identifying next steps.
    - Analysts working for think tanks, international organizations, and government researchers should explore the current state of scamming to raise awareness among key actors and lay out a plan for future actions to address it.
    - International NGOs and civil society organizations should workshop best practices on investigations with a victim centered approach and engage more comprehensively with law enforcement to put them into practice.
    - Tech companies, social media platforms, and government agencies should mandate higher levels of cybersecurity training and standard operating procedures (SOP) for responding to cybercrimes.

2. **Develop a comprehensive definition of the scale and scope of scam operations at the regional level.** Currently there is insufficient data in most countries about the scale of impact of online scam operations in both countries targeted for scams and those targeted for trafficking of workers. Policy makers and researchers need to better articulate the scale and scope of online scam operations impacts at the local and national levels, as this is necessary for national governments to prioritize addressing it and step up resources.
    - National authorities including police and key line agencies should improve information-sharing and research to identify and improve understanding of the scale of impact from online scam operations at financial, societal, and human levels. This could be done through the creation of a dedicated national task force or central reporting agency.
    - National police and relevant researchers in academic institutions and think tanks should support studies on victim profiles, as better understanding of targeted demographics and approaches will support better education and awareness among the public.
    - Intergovernmental organizations like UNODC, INTERPOL, or IOM should work with a range of civil society and non-governmental stakeholders to improve indicators and guidance on identifying and responding to victims and provide sufficient support post-rescue or post-report of being scammed.

3. **The financial and information technology (IT) ecosystems should develop safe practices for citizens and employees.** Digital or technical literacy is a problem, for both individual citizens vulnerable to being scammed and employees who can lead to data breaches.
    - Companies and government agencies should strengthen security standards and training protocols for employees.
    - National governments should create stronger regulatory standards for finance and technology companies to incentivize prevention of data breaches and active monitoring of platform uses by bad actors.
    - Community hubs such as schools, universities, banks, and social media should promote awareness campaigns to help educate vulnerable actors about how to identify and avoid scams.


# REGIONAL COLLABORATION AND COORDINATION

While most scam compounds are currently situated in Southeast Asia, they are metastasizing to new localities in the Middle East and Africa. Trafficked victims who have been rescued from scam compounds come from more than twenty-five countries, and victims of online scam operations from these scam compounds are found around the world. While individual countries which are targets of scams are taking national steps to reduce vulnerability or go after individual scam compounds, these steps can have a "whack-a-mole" effect of simply inspiring scammers to shift operations elsewhere or shift targets to new countries or vulnerable groups. Multilateral tools and processes are needed to effectively combat scam centers.

The transnational nature of online scam operations, role of transnational criminal organizations in driving trafficking and scams and the need for a coordinated response was discussed on nearly every panel throughout the Policy Dialogue. However, one session was dedicated specifically to exploring how multilateral collaboration and coordination can address the rapid growth and expansion of online scam operations both to new host countries and in shifting targets. Speakers on this session provided case studies of existing frameworks—such as the Bali Process—as well as existing gaps such as difficulty with incorporating technical elements of cryptocurrency and AI into legal protocols; the displacement of compounds by enforcement efforts rather than dismantling of criminal networks; and insufficient legal frameworks and widespread loopholes of which TOCs take advantage.

Photo: Dr. Wibawanto Nugroho Widodo at Global Cyber Policy Dialogue: Southeast Asia at ASEAN Cybersecurity Center of Excellence, Singapore on July 4, 2023. Courtesy of Wikimedia Commons and used under a Creative Commons license.

## PRIORITY ISSUES AND POLICY RECOMMENDATIONS:

1. **Strengthen the national implementation of existing agreements and regional efforts.** Regional bodies like ASEAN may set priorities and help inform regional standards and agreements, but implementation is hampered by a lack of political will as well as issues of corruption which weaken accountability structures.
    - Analysts from respected think tanks or research institutes should conduct a stakeholder mapping to identify points of contact at all levels – national governments, regional bodies like ASEAN or INTERPOL, and relevant non-governmental stakeholders--to improve cross-border cooperation at the working level.
    - National authorities should develop national action plans for implementation of regional or other commitments. Formal guidance for implementation would be beneficial, which could draw on the support and input from a wide range of actors including IOs, CSOs, NGOs, and international organizations.
    - International organizations such as UNODC, INTERPOL, think tanks like the Stimson Center or USIP, and development agencies should provide capacity building on a range of technical, legal, and policy gaps to government agencies including immigration authorities, law enforcement, and local authorities.
    - Ministries of foreign affairs and the ASEAN Secretariat should coordinate with relevant line agencies in charge of justice, information, telecommunications, and finance to create regional guidelines to help standardize law enforcement procedures.

2. **Improve data collection and information-sharing across national boundaries.** Jurisdictional issues are a significant challenge, especially in relation to evidence collection, and require greater cooperation.
    - ASEAN governments, international organizations like INTERPOL or UNODC, and development partners should better cooperate on information-sharing about scams and bad actors through existing mechanisms such as the ASEAN Senior Officials Meeting (SOM) on Transnational Crime, the Bali Process, ASEAN Commission on the Promotion and Protection of the Rights of Women and Children, and ASEAN Intergovernmental Commission on Human Rights.
    - The private sector—particularly internet platforms and airlines—should engage with law enforcement agencies (LEAs) to identify feasible avenues for greater cooperation.
    - National law enforcement agencies should push for stronger regulation and enforcement of reporting and response from platforms which are prevalent hosts of scams, such as messaging platforms like Telegram and social media platforms.
    - International organizations should foster communication between relevant communities and improve awareness of ongoing activities through convenings and working groups.
    - Local CSOs should foster trust building through informal channels to clarify respective data collection and sharing processes.

# FEEDBACK

Forty of the 90 attendees shared feedback in a survey following the Policy Dialogue, and most attendees indicated that the dialogue was an extremely positive and productive experience.

Key takeaways from the anonymous evaluation surveys are:

- 93% of attendees indicated that they learned some, a lot, or all new information through participating in the Dialogue, with 65% indicating they learned a lot of or all new information.
- 100% indicated that they would definitely or probably use the knowledge gained in their work.
- 93% of attendees said they would recommend participating in a future Dialogue to a colleague.
- 93% felt that they developed insight into a relevant policy, human resources, or sustainability challenge facing the region.
- 88% said that the Dialogue helped them identify a local Mekong sub-region stakeholder(s) with whom they shared common interest, and 85% said the same for identifying US-based and international development partner stakeholders.
- 95% of attendees found the breakout groups to be a good opportunity to actively engage and 98% felt the synthesis workshop was valuable as a wrap-up exercise to identify recommendations.

Many survey respondents shared that they benefited from understanding the immense scale of online scam issues, learning about how other countries or companies are tackling scam issues, and the opportunity to learn from new and diverse actors and gain cross-sector perspectives from TIP, cyber, banking, and technology industries. Many participants particularly valued that the Policy Dialogue was outcome focused, included opportunities to network and build partnerships across nationalities, sectors, and level of actors, and the emphasis on cross-cutting and multi-disciplinary information-sharing. A fifth of attendees flagged that their favorite session was on Regulating Digital Finance, with respondents valuing the insights into evolving tech and financial elements of the crimes and preventative efforts.

Photo: Synthesis workshop discussion on October 18, 2024, at Policy Dialogue in Bangkok, Thailand. Photo courtesy of Courtney Weatherby.

# FEEDBACK

There were a few areas of improvement identified. While most attendees indicated that the right people were in the room to participate in the Track 1.5 Policy Dialogue, about a quarter of the survey respondents felt that law enforcement should have been more present in the discussions. Five participants flagged it would be valuable to include more technical experts on online scam operations and cyber security responses. Six participants suggested government representation from more diverse agencies. Recommendations for improving future Dialogues included asks to share contact information or provide further networking opportunities beyond the Dialogue, providing suggested reference materials, convening outside the capital city to avoid drop-off from locally based participants, and doing a field engagement.

# NEXT STEPS

This was the ninth Mekong-U.S. Partnership Track 1.5 Policy Dialogues planned in this multi-year series of eleven workshops. Two more Policy Dialogues will be held in 2025 on topics to be determined with the U.S. Department of State but which will build on previous conversations and gaps identified in the previous Policy Dialogues. The Policy Dialogues serve as an opportunity for stakeholders from the Lower Mekong sub-region, the United States, relevant NGOs, and development partners to identify lessons-learned, build collaborative partnerships, transfer best practices, and suggest joint-pathways to meeting policy needs. In order for the Track 1.5 Dialogues to continue strengthening the Mekong-U.S. Partnership at large, participants will continue to be drawn from a wide range of government and non-government sectors, and the invite list will consider gender balance, youth participation, and inclusion of under-represented stakeholder groups to ensure a diversity of voices.


STIMSON

## ABOUT THE POLICY DIALOGUE SERIES

This summary report provides an outline and recommendations derived from discussions held as a part of the Mekong-U.S. Partnership Track 1.5 Policy Dialogue series. The Partnership Policy Dialogues are a series of eleven conferences taking place between 2021 and 2025 that are generously supported by a grant from the U.S. Department of State's Mekong-U.S. Partnership. Cross cutting principles of inclusivity, resilience (including climate), and collaboration will be applied to all conferences in this series.

The U.S. Government launched the Mekong-U.S. Partnership in 2020 to expand cooperation with the five countries of the Lower Mekong sub-region on strategic challenges and shared priorities under the Partnership's four areas of cooperation (nontraditional security, natural resources management, economic connectivity, and human resource development). The Mekong-U.S. Partnership builds on the strengths of the Lower Mekong Initiative's development-focused agenda by cooperating on strategic sub-regional issues and challenges. Each area of engagement under the Mekong-U.S. Partnership is supported by a flagship project. The Mekong-U.S. Partnership's Track 1.5 Policy Dialogue series serves as the flagship program of the Mekong-U.S. Partnership's human resources development area of engagement.