Australian Government
Australian Institute of Criminology

Regional Support Office
The Bali Process

AIC reports
Consultancy report

Gender, technology and trafficking in persons: Women's experiences of forced criminality in South-East Asia's cyber-scam centres

Siobhan Lawler
Samantha Lyneham
Christopher Dowling

ISBN 978 1 922878 27 4 (Online)
https://doi.org/10.52922/sp78274

Published by the Australian Institute of Criminology
GPO Box 1936 Canberra ACT 2601
Tel: (02) 6268 7166
Email: front.desk@aic.gov.au
Website: www.aic.gov.au

Please note: Minor revisions are occasionally made to publications after release. The online versions available on the AIC website will always include any revisions.

Disclaimer: This research report does not necessarily reflect the policy position of the Australian Government.

General editor: Dr Rick Brown, Deputy Director, Australian Institute of Criminology

Edited and typeset by the Australian Institute of Criminology

A full list of publications in the AIC Reports series can be found on the Australian Institute of Criminology website at **aic.gov.au**

Contents

Acknowledgements

We sincerely thank the victim-survivors who courageously shared their experiences, and recognise the commitment of stakeholders across the region who generously contributed their time and expertise to inform the research.

The important contributions of our project partners at the Regional Support Office of the Bali Process on People Smuggling, Trafficking in Persons and Related Transnational Crime are gratefully acknowledged, particularly for commissioning the research, providing technical input and facilitating data collection opportunities.

Appreciation is also extended to UN Women's Regional Office for Asia and the Pacific for their valuable technical support.

Acronyms and abbreviations

AI	artificial intelligence
ASEAN	Association of Southeast Asian Nations
GI-TOC	Global Initiative Against Transnational Organized Crime
NGO	non-government organisation
OHCHR	Office of the High Commissioner for Human Rights
RSO	Regional Support Office (of the Bali Process on People Smuggling, Trafficking in Persons and Related Transnational Crime)
TIP	trafficking in persons
UNODC	United Nations Office on Drugs and Crime

Abstract

Over the past decade, cyber-scam centres dedicated to running online scams at a massive scale have proliferated across areas of South-East Asia, partly fuelled by a workforce of persons who have been trafficked for the purpose of forced criminality. Alongside the scams, which affect victims globally, these centres themselves have become sites of significant exploitation. Historically, women and girls constitute the majority of victim-survivors of trafficking overall, but the extent to which gender shapes pathways into, and experiences of, exploitation in this context is only beginning to be explored.

To understand women and girls' experiences of trafficking into cyber-scam centres for forced criminality, the research involved qualitative consultations with 86 stakeholders in the South-East Asian region and in-depth interviews with three victim-survivors.

Women and girls are predominantly recruited into cyber-scam centres through someone they know, using strategies that exploit relational trust. Women in cyber-scam centres commonly experience compounded forms of exploitation, most often forced criminality (online scamming) as well as sexual exploitation. Sex work, threats and extreme forms of violence are routine control mechanisms used by criminal organisations to make people of all genders perform and conform in this environment.

Gender-responsive approaches are imperative for addressing the complex and multiple forms of exploitation that women experience while inside cyber-scam centres and post-release. Recommendations are made for developing gendered awareness campaigns, trauma-informed victim identification processes and aftercare, and strengthening partnerships across the region.

Content warning

This report contains discussion of sensitive topics such as serious violence, abuse and exploitation, including sexual assault. People who have experienced these forms of violence may find some of this content difficult. Similarly, those who have not been exposed to this content before may find the information confronting and challenging.

A note about language

This report uses both 'victim' and 'victim-survivor' when referring to people who have been subjected to trafficking. The term 'victim' is often used in sections relating to monitoring, service systems, legal frameworks and policy settings, reflecting the established terminology used by the United Nations Office on Drugs and Crime and other relevant research reporting about victimisation and identification processes. The term 'victim' is also used when juxtaposing this experience against other forms of involvement, specifically perpetration and the overlap between the two. The term 'victim-survivor' is used when discussing the lived experience of individuals and post-exploitation experiences, including those related by victim-survivors in the interviews conducted as part of this project. The latter term recognises agency, resilience and self-identification; however, the use of both terms reflects both diversity in experiences and specificity of context, and is intended to promote clarity over consistency.

Executive summary

Background

The trafficking of people for forced criminality in cyber-scam centres in South-East Asia represents a significant human rights crisis for the region and, increasingly, the world. Moreover, cyber-scam centres are emerging as major sites of exploitation for women and girls. The precise modus operandi of, and conditions within, cyber-scam centres in South-East Asia vary across the region, influenced by local political economies, the intensity and complicity of law enforcement, the extent of regulatory oversight and the criminal syndicates operating them. In some areas, cyber-scam centres operate in compounds alongside casinos and other entertainment venues, or in special economic zones that may be loosely regulated or follow rules that are distinct from the rest of the country where they are based.

The number of people being trafficked for the purpose of forced criminality has been increasing (UN Office on Drugs and Crime (UNODC) 2024a). During the COVID-19 pandemic, cyber-scam centres proliferated, along with the trafficking of persons into them. Historically, women and girls have constituted the majority of trafficking victims overall, with the most recent global monitoring data showing they constitute 61 percent of victims (UNODC 2024a). However, emerging evidence about the gender dynamics underlying trafficking into cyber-scam centres suggests that women represent a sizeable minority of victims and there is considerable diversity characterising this profile of victims compared to other forms of trafficking, such as trafficking for the purposes of sexual exploitation and forced labour (Franceschini et al. 2024; International Organization for Migration 2024; UNODC 2024a, 2023a).

Emerging evidence highlights the gendered experiences of those trafficked into cyber-scam centres for forced criminality. Women are assigned to positions that exploit their femininity to manipulate others, such as 'models', recruiters, facilitators and administrative roles, and are subjected to significant levels of sexual exploitation and abuse. Evidence suggests thousands of women in service roles in cyber-scam centres are being forced to engage in sexual activity with managers and other employees, while others may be forced to engage in sexual video calls and phone calls with fraud victims (Global Initiative Against Transnational Organized Crime (GI-TOC) 2025; Franceschini, Li & Bo 2023). Women's involvement in recruiting and facilitating the trafficking of other women is a common theme in the literature examining trafficking in persons (TIP) for sexual exploitation, but their involvement in facilitating trafficking for forced criminality in cyber-scam centres has not yet been examined in depth.

Deepening understanding about women's experiences and the gender dynamics underpinning TIP for forced criminality in cyber-scam centres has important policy implications. The application of UN Women's Gender Mainstreaming principles to analyse the gender dynamics of trafficking, combined with a Women, Peace and Security lens, can strengthen the development of responses that are both harm-reductive and gender-responsive. However, building the evidence around women's experiences to inform this is a critical first step. Without this analysis, policy and intervention risk overlooking specific vulnerabilities and support needs required to prevent future exploitation.

Good practices for preventing the trafficking of persons, including women, into cyber-scam centres are still developing, and this emerging form of trafficking presents novel challenges for regional law enforcement, consular officials and policymakers. Most insights are drawn from non-government organisation (NGO) reports and media coverage, which rely heavily on the accounts of victim-survivors and others with direct experience. While important to informing understanding of this problem and efforts to address it, evidence derived from other sources (eg law enforcement and other government-held data) is scarce. Research indicates that dedicated responses to this type of trafficking, and even recognition of it, vary considerably across the region. Political instability, corruption and declining support for many of the NGOs working on the front lines of this issue all pose major challenges (GI-TOC 2025). Given that TIP into cyber-scam centres is a relatively new and rapidly evolving phenomenon, integrating a gender lens is critical to understanding the different experiences and impacts on women, girls, men and boys. The extent to which gender shapes pathways into exploitation, roles within cyber-scam centres, and barriers to exiting and support, requires closer examination.

Methods

This research aims to understand women and girls' experiences of trafficking into cyber-scam centres for forced criminality. This includes specific examination of recruitment pathways, organisational roles, experiences of exploitation, exit routes and current responses.

The findings presented in this report are primarily informed by qualitative consultations with 86 stakeholders in the South-East Asian region. Data collection was conducted through consultations held between August and October 2024 in Bangkok and Chiang Mai (Thailand) and in Manila (the Philippines). In-depth interviews were also conducted with stakeholders who have extensive knowledge and expertise of this form of trafficking and the experiences of women. Stakeholders had backgrounds in civil society and NGOs, government, police and other law enforcement, immigration, journalism and academia. These interviews were conducted in-person and online via videoconference between August 2024 and February 2025.

In addition, three in-depth interviews were conducted with victim-survivors with lived experience of trafficking for forced criminality into a cyber-scam centre in South-East Asia, who validated and deepened the initial findings of the focus group discussions and in-depth interviews. The experiences of victim-survivors are summarised and captured through case studies incorporated into the main findings of the report to illustrate the themes emerging from the stakeholder consultations.

A validation workshop was held in August 2025 with 13 experts from across the region, including one victim-survivor, to discuss and critique the findings of the draft report and identify any areas of data misalignment, inaccuracies or potential sensitives in the themes identified.

Technical experts from the Regional Support Office of the Bali Process on People Smuggling, Trafficking in Persons and Related Transnational Crime (RSO) and UN Women provided further feedback on the findings of the report and held detailed discussions with the researchers on effectively incorporating the feedback provided during the validation workshop.

Key findings

Women and girls are predominantly recruited into cyber-scam centres through personal networks such as friends, family members, acquaintances and romantic partners. This strategy exploits social and emotional trust and reflects women's greater general hesitation to travel alone abroad for work compared to men. However, women and girls are also being recruited via fake online job advertisements, the primary mechanism through which men have been recruited.

Stakeholders' reports about women's experiences in cyber-scam centres reveal a dynamic and evolving pattern of exploitation. While the most common form of exploitation is forced criminality—particularly involvement in online scamming—many also face sexual exploitation, either concurrently or at a different stage of their exploitation. Women also disproportionately occupy the role of 'models', who conduct video calls and voice calls with fraud victims to reassure them so that they continue to engage. Women's experience of exploitation may be compounded by expectations that they will perform additional service roles and tasks, and many are coerced to recruit new victims. These layered and shifting roles highlight the complex and compounded nature of women's exploitation in cyber-scam centres.

Many women are rescued from exploitation in cyber-scam centres through diplomatic intervention. A number are also released after making ransom payments, often with money either borrowed from friends and families or earned during their time working in the cyber-scam centre. Unique to women, pregnancy can be a catalyst for release, as centre operators come to see them as a liability. Finally, there are instances of women being released after persistently refusing to work, although findings suggest that this is not common and that recalcitrance more often prompts re-trafficking into other cyber-scam centres or forms of exploitation including, for women, sexual servitude.

Targeted education and awareness raising campaigns that provide information about localised and gendered trends in recruitment and experiences in cyber-scam centres are important prevention mechanisms. Stakeholders identified key areas for improving victim identification processes and tailoring intervention to be more gender-responsive. Recommendations for improving institutional responses for both men and women include increasing consistency across the region in how forced criminality is defined in policy and legislation. Continuing to enhance coordination and information sharing between sectors—including the local and international NGOs, government, police and the private sector—is important for effective prevention and intervention.

Introduction

Trafficking for forced criminality in cyber-scam centres has emerged as a growing security concern in South-East Asia (UN Development Programme 2023; UNODC 2024a, 2023a). This region has become one of the world's fastest growing digital economies, with 460 million internet users in 2022 (Moore 2023). At the same time, South-East Asia is witnessing a shift in TIP patterns as criminal operations increasingly move online. The reach and power of the organised crime groups involved in TIP has increased since 2021, and they now constitute a significant threat to nation-states around the world (GI-TOC 2025).

Despite the large proportion of women identified as trafficking victims and perpetrators (UNODC 2024a, 2023b, 2018), there is little information about the gender dynamics of TIP for forced criminality in cyber-scam centres. Gender-focused analysis of TIP into cyber-scam centres is crucial for understanding how social norms, power imbalances and economic inequality contribute to recruitment, experiences of victimisation and perpetration of this crime. This information is critical for developing effective prevention and awareness interventions, policy and legislative responses and tailored survivor support to address the unique needs of women and men who experience forced criminality and related forms of exploitation in this context.

Trafficking into cyber-scam centres for forced criminality

TIP in South-East Asia is underpinned by poverty, regional instability and inequality. The United Nations Protocol to Prevent, Suppress and Punish Trafficking in Persons Especially Women and Children (the Palermo Protocol) is an international treaty adopted by the United Nations General Assembly in 2000 which supplements the United Nations Convention against Transnational Organised Crime. The following definition of trafficking is provided in the Palermo Protocol:

> "Trafficking in persons" shall mean the recruitment, transportation, transfer, harbouring or receipt of persons, by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation. Exploitation shall include, at a minimum, the exploitation of the prostitution of others or other forms of sexual exploitation, forced labour or services, slavery or practices similar to slavery, servitude or the removal of organs … (UN General Assembly 2000, Article 3(a))

According to this definition, the consent of a person is negated where any element outlined above is present. Because consent is negated in situations characterised by coercion, abuse and deception, determining whether participation reflects genuine willingness is particularly complex in cases where people appear to engage in criminal activity but may in fact be acting under duress.

TIP for the purposes of forced criminality is emerging as a distinct and particularly challenging form of trafficking, characterised by exploitation of victims who are coerced into committing criminal acts for the financial gain of their traffickers or exploiters (UNODC 2023a). It is often perpetrated alongside other forms of trafficking such as sexual exploitation, forced labour and domestic servitude.

Cyber-scam centres emerged in South-East Asia in the mid- to late 2010s and have since expanded into large-scale, highly structured operations run by transnational criminal syndicates, supported by networks of money launderers, human traffickers, data vendors and other specialist facilitators (UNODC 2025). These centres, often constituting large prison-like compounds, are akin to call centres except workers, many of whom have been trafficked into them, are forced to carry out a variety of online scams on a massive scale. Recent research mapping the organisational structure of cyber-scam centres has highlighted their pyramidal hierarchy, with organised crime group leaders at the top, casino and cyber-scam centre owners or developers immediately underneath them, followed by directors, controllers, agents, recruiters and transporters (UNODC 2023a). The controllers are responsible for managing the trafficking victims and ensuring they meet their fraud quotas. Emerging evidence suggests that some of these individuals may be former victims who have secured their own release by moving into roles that control other groups of victims (UNODC 2023b).

According to the United Nations, there was a rapid increase in TIP for forced criminality in cyber-scam centres in 2020, when the COVID-19 pandemic halted the development of casinos and hotels in the Mekong region and workers were advised to return home, stemming the number of people crossing the border to participate in the economy of the border casinos (UNODC 2025). Criminal enterprises addressed the labour gap by using established trafficking routes to recruit jobseekers into cyber-scam centres, where they would be held captive and forced to conduct scams online (UNODC 2023a; GI-TOC 2025). This was accompanied by significant global increases in online activity and the use of cryptocurrency, as well as downturns in law enforcement investigative capacity (UNODC 2023a).

Cyber-scam centres in South-East Asia tend to differ from other cybercrime and cyber-fraud networks, which are often much smaller, less hierarchical and more geographically dispersed, and which rarely rely on forced labour (Broadhurst et al. 2014). They also exhibit important differences in structure and modus operandi to 'boiler room' schemes, which involve selling dubious stocks using deceptive or high-pressure sales tactics to uninformed investors (Cross 2024). Cyber-scam centres are now an established industry in the region, supported by some local elites (who may occupy multiple roles in business, government and crime) and weak governance, often operating under the guise of legitimate businesses, in special economic zones and entertainment districts as well as hotels and casinos (GI-TOC 2025; UNODC 2025, 2024b). For example, Philippine offshore gaming operators are online gambling businesses that cater to international markets that restrict gambling. While originally legal and regulated in the Philippines, various operators have been identified as fronts for cyber-scam operations and related criminal activities such as TIP and money laundering. By early 2025, the Philippine government had moved to phase out these services, setting a deadline of December 2024 for all remaining licences to expire (Office of the High Commissioner for Human Rights (OHCHR) 2023; UNODC 2024b).

Within South-East Asia, there are regional differences influencing and facilitating TIP into cyber-scam centres. Clusters of cyber-scam centres have been identified in Cambodia, Laos and Myanmar (OHCHR 2023). The growth of casinos and other businesses in the region has been associated with an increase in sex trafficking and forced labour among local women and girls, and efforts to recover losses from pre-COVID investments in casinos and hotels for tourism led to developments being repurposed for online scamming (UNODC 2023a; GI-TOC 2025). Evidence suggests that Thailand has become a major transit node for victims of trafficking into these countries by virtue of sharing borders with them.

Given the scale at which cyber-scam centres now operate, TIP has come to play a significant role in supplying the required labour force. Experts suggest that organised crime groups prefer trafficked victims to professionals as they are low-cost and easier to control (UNODC 2023a). Research suggests there are at least 300,000 people of over 60 nationalities in cyber-scam centres in the Mekong region (OHCHR 2026). Many workers are deceptively recruited through false online job advertisements that often mimic legitimate recruitment pathways (Jesperson et al. 2023). Individuals trafficked into cyber-scam centres commonly report being transported by land to a cyber-scam centre, where their passport was taken away from them upon arrival (UNODC 2025).

While traditionally people with limited education seeking unskilled or low-wage jobs have been particularly vulnerable to trafficking in South-East Asia, the pool of people targeted for recruitment into cyber-scam centres has expanded (OHCHR 2023). Multilingual university graduates who have skills and technical knowledge in information technology (IT), marketing and social media, and an understanding of cryptocurrency, are valuable assets for organised criminal syndicates running cyber-fraud operations. Skilled candidates can fit into a variety of roles, ranging from scamming to programming and money laundering (UNODC 2023a).

Criminal syndicates are increasingly integrating and investing in technologies including artificial intelligence (AI), cryptocurrency, malware and deepfakes to facilitate their scamming and money laundering operations (UNODC 2024a). The extent to which women's experiences of victimisation in cyber-scam centres and their roles as recruiters and exploiters are being shaped by technology is unknown (Organization for Security and Co-operation in Europe 2023). There is evidence that perpetrators use dating sites, chatrooms and online classifieds to recruit and exploit victims, but there is no firm data on women's experiences (Raets & Janssens 2021). There is some evidence of an increase in women using social media to recruit and exploit victims (Organization for Security and Co-operation in Europe 2023).

In line with the scale and rapid growth of this criminal enterprise in South-East Asia, attention to the issue has increased, as has the body of evidence dedicated to understanding cyber-scam centres. Most of the existing work that has documented women's roles and experiences of TIP analyse data collected prior to the COVID-19 pandemic, and therefore before the industrialisation of cyber-scam centres in South-East Asia and the significant increase of trafficking into them. However, the gender dynamics of this trafficking and, more specifically, women's experiences of exploitation within cyber-scam centres, remain underexplored.

Intersection of gender and trafficking for forced criminality

Gender comprises constellations of characteristics and roles that a given society considers appropriate for men and women, and the related behaviours, duties, privileges and barriers associated with belonging to either category, as well as other diverse gender and sexual identities (UN Women 2022a; World Health Organization 2026). Using a gendered lens to analyse and understand the concept of forced criminality requires consideration of the importance of social and family relationships for women, including family and childcare responsibilities, and how gender influences the 'resources, opportunities and rights afforded to individuals, as well as their power in relation to others' (UN Women & ODI 2020: 27).

Examining the prevalence of trafficking victimisation is beset by challenges, including ongoing variation and contention in the definitions used by researchers and governments, gaps and biases in detection and identification, and trends in reporting. Some of these challenges are exacerbated in relation to women and transgender victims, who can face additional barriers to reporting and identification, and who may be overcounted as trafficking victims while legally or voluntarily undertaking certain activities like migration or sex work. Nevertheless, it is estimated that, globally, women account for 61 percent of detected victims and 28 percent of convicted perpetrators of trafficking (UNODC 2024a). Only 12 countries report data on transgender victims, who constitute an estimated two percent of all trafficking victims (UNODC 2023b). Women and girls make up about 80 percent of detected trafficking victims in East Asia and the Pacific and about 61 percent in South Asia (UNODC 2024a). While women have historically constituted the majority of trafficking victims, the gender breakdown differs by trafficking type. For example, women and girls constitute the vast majority of victims of trafficking for sexual exploitation (91% total, 64% women and 27% girls) whereas most victims of forced labour trafficking are men and boys (73% total, 56% men and 12% boys; UNODC 2023b).

Monitoring shows recent increases in the proportion of people being trafficked for the purpose of criminal activity, which can include forms of labour undertaken illegally (eg mining, fishing) as well as criminal activities such as drug trafficking or scamming (UNODC 2024a). People trafficked for criminal activity constituted one percent of all trafficking victims in 2016, increasing to six percent in 2018, and eight percent in 2022 (UNODC 2024a). Recent research documenting gendered trends in victimisation shows that the majority of people trafficked into cyber-scam centres appear to be men (UNODC 2023a). However, findings also suggest that women in cyber-scam centres experience a number of unique risks and challenges.

Recent research drawing on in-depth interviews with eight female victim-survivors trafficked into cyber-scam centres in the region examined women's experiences from pre-recruitment through to post-release (Li, Liu & Franceschini 2026). The study highlights the difficult social circumstances shared by participants prior to entering the cyber-scam centre, specifically social isolation, family dysfunction and obligations, and economic insecurity. These factors increased their vulnerability to recruitment, which was frequently facilitated by someone they knew and trusted, such as a friend or family member.

While victims of all genders are forced to undertake a variety of roles in cyber-scam centres, and can be subjected to significant abuses including confinement and the denial of liberties, torture and violence, women are at increased risk of sexual violence and harassment, as well as gendered forms of exploitation (eg being forced into service, domestic or modelling roles; Baxter & Chazal 2022; GI-TOC 2025; OHCHR 2023; Raziur Rahman 2025; Rodríguez-López 2022; UNODC 2024b, 2023a; Veldhuizen-Ochodničanová & Jeglic 2021). This was reflected through Li, Liu and Franceschini's (2026) consultations with victim-survivors:

> … although men and women in scam compounds often endured similar exploitative labor conditions, women's experiences were shaped by an added layer of physical, sexual, and psychological abuse. Their bodies, reproductive choices, and emotional attachments were systematically controlled, monitored, or weaponized as tools of coercion. (Li, Liu & Franceschini 2026: 52)

While the leaders or 'kingpins' of these criminal syndicates are often men, there is evidence that women from influential families have also held visible leadership roles within these networks. In many cases, women have inherited or exercised authority through family-based power structures, reflecting the patriarchal and dynastic nature of political and economic influence in the region.

Upon exit from the cyber-scam centres, women who have experienced sexual violence may be re-victimised if they are interviewed by untrained male officers (Franceschini, Li & Bo 2025). Many victim-survivors experience distress related to unresolved trauma which is compounded by gender-specific vulnerabilities such as pregnancy and postpartum recovery, and the incapacity (or failure) of shelters to provide appropriate psychosocial support. Finally, when women return to their communities, the factors that contributed to their initial vulnerability to trafficking—family dysfunction, economic deprivation and social isolation—often remain (Li, Liu & Franceschini 2026).

Current responses to trafficking into cyber-scam centres

Responses to TIP in South-East Asia generally involve a combination of local and international government and non-government initiatives supported by Association of Southeast Asian Nations (ASEAN) frameworks, national anti-trafficking laws and victim protection initiatives (OHCHR 2023). As recognition of the scale and harm of cyber-scam centres has increased, so too has collaboration between many affected countries and international organisations such as the United Nations and Interpol in combatting it. Enforcement-based responses to TIP into cyber-scam centres include sanctions; improved information sharing and coordination between international, state and non-state law enforcement partners; and the strengthening of border security measures (GI-TOC 2025). Broader efforts to strengthen financial and other intelligence capacity, such as improved tracking of cryptocurrency transactions, have been directed at disrupting the (particularly financial) activities of criminal networks profiting from cyber-scam centres (UNODC 2025). Additionally, education and awareness campaigns have been used to stem the flow of people from their countries of origin into exploitative work conditions (OHCHR 2025).

Victim-centred responses encompass protections for victims of forced criminality that are consistent with frameworks such as the Palermo Protocol and the non-punishment principle, now enshrined in legislation to varying degrees across South-East Asia. Victim identification processes and systems for providing post-rescue support and repatriation to victims are important but delivery can be challenging due to difficulties distinguishing victims from perpetrators (Fitzgerald 2024). Further, the capacity of NGOs to support victims may be limited when local authorities are not cooperative, highlighting the importance of consistent referral mechanisms for victims (Li 2023). An example of such an established process is Thailand's National Referral Mechanism, which is designed to facilitate information sharing and cooperation between government and non-government agencies involved in helping trafficking victims to access relevant services.

A key challenge in responding to TIP for forced criminality is that authorities often misidentify trafficked individuals as willing perpetrators, which may result in their prosecution for the crimes they were forced to commit (Li 2024; Sarkar & Shukla 2024). This practice contradicts the non-punishment principle now advocated for by many national and international NGOs and academic experts:

> … trafficked persons should not be subject to arrest, charge, detention, prosecution, or be penalized or otherwise punished for illegal conduct that they committed as a direct consequence of being trafficked. (Inter-Agency Coordination Group against Trafficking in Persons 2020: 1)

The non-punishment principle should safeguard victims of trafficking for forced criminality and protect these individuals from prosecution for crimes that they committed under coercion. However, research suggests that this principle is inconsistently applied, leaving many victims at risk of secondary victimisation and trauma, and without adequate protection by legislation (Fitzgerald 2024).

Efforts to improve cross-national collaboration include an agreement between Thailand and China to establish coordination centres in Bangkok and Mae Sot in Thailand to investigate and respond to organised crime and cyber-scam centres operating over the Thai border in Myanmar and Cambodia (Thepgumpanat & Wongcha-um 2025). In addition, the Thailand–Myanmar–China Coordination Meeting on Combatting Telecommunications Fraud in Bangkok reaffirmed their strong commitment to work closely to combat cybercrime and to strengthen cooperation through the Thailand–China–Myanmar coordination mechanism, particularly in law enforcement collaboration and information sharing (Thai Ministry of Foreign Affairs 2025). Domestically, some countries in the region have strengthened anti-trafficking legislation. For example, Malaysia has enshrined in legislation a definition of trafficking that explicitly includes exploitation (UNODC 2023a). Further, the Philippine ban on offshore gaming operators represents a legislative response to TIP and recognition that the financial benefits were not worth the human cost.

ASEAN's Regional Plan of Action on Women, Peace and Security highlights the need to uphold the safety and dignity of trafficking victims and ensure access to support services during relief and recovery. While progress has been made on this front in the Asia-Pacific region over the past 25 years (UN Women 2025), gaps remain between the ambitions expressed through international commitments and the political will and financial support given to these efforts. Indeed, research with victim-survivors navigating victim identification processes following exit from cyber-scam centres across the region has highlighted the 'gender-blindness' of these systems, alongside other practical and legal challenges with identification and repatriation (Franceschini, Li & Bo 2025; Li, Liu & Franceschini 2026).

The nature and drivers of conflict are evolving, with gendered aspects to emerging security threats—such as TIP and cybercrime—creating new and complex challenges that demand innovative responses (UN Women 2023). In line with this, UN Security Council Resolution 2331/2016 highlights growing concerns around the changing nature of trafficking, particularly of women and girls, in both traditional and non-traditional conflict settings, as well as criminal exploitation of new technologies in its facilitation. These developments have significant negative consequences for women's rights, regional stability and security in South-East Asia (OHCHR 2023; UNODC 2024b; UN Women 2023).

In early 2019, Thailand committed to adapting ASEAN's (2016) *Gender sensitive guideline for handling women victims of trafficking in persons* to the local context, with the aim of strengthening the capacity of frontline responders working with female victim-survivors of trafficking and increase gender-responsive service provision. Priority activities included capacity-building workshops, awareness raising, and advocacy activities which involved frontline responders (including officers from the Anti-Human Trafficking Division of the Royal Thai Police), local women's groups and key community members (UN Women 2019). Since then, Thailand has continued investing in capacity building through training and development with law enforcement and community groups, regional partnerships and the nationwide implementation of the National Referral Mechanism (Royal Thai Government 2023).

Despite the relatively high proportion of women among TIP perpetrators compared to perpetrators of other crimes (UNODC 2024a), and the intense efforts to prevent and respond to this issue, little information exists about the gender dynamics of TIP for forced criminality in cyber-scam centres. Previous research has examined victim-survivors' experiences of trafficking into cyber-scam centres broadly using NGO datasets, police case files, court transcripts and sentencing remarks and analysis of media and news reports (UNODC 2024b), with few studies analysing the gender dynamics using primary data collected from stakeholders or victim-survivors themselves (Li 2024; Li, Liu & Franceschini 2026; UNODC 2023a). This research aims to fill this gap.

Aim and methods

This research aims to understand women's experiences of trafficking in cyber-scam centres, and how their experiences differ to men's experiences. Current understanding on this topic was collated through consultations with stakeholders who have direct and secondary experience engaging with victim-survivors and perpetrators of TIP for forced criminality in cyber-scam centres. Interviews with three victim-survivors were also conducted, and summaries of their experiences are included as case studies. Their experiences are also integrated into the findings to highlight alignment with themes emerging from the stakeholder consultations.

Research partners

The Australian Institute of Criminology led the research in partnership with the Regional Support Office of the Bali Process on People Smuggling, Trafficking in Persons and Related Transnational Crime, with UN Women providing input as required.

Research questions

The research is intended to be used by policymakers and practitioners to inform evidence-based responses to TIP for forced criminality in cyber-scam centres in South-East Asia. High-level research questions include:

1. What is known about women's and girls' experiences of TIP for forced criminality in cyber-scam centres in South-East Asia?
2. What technologies are being used to recruit and exploit women and girls, how are they being used, and by whom?
3. How are women and girls accused of TIP for forced criminality treated by the criminal justice system?
4. What lessons can be learned from women and girls' experiences of TIP for forced criminality in cyber-scam centres to strengthen prevention and response initiatives?

To address these research questions, a series of focus groups and interviews with stakeholders and victim-survivors were conducted.

Data collection

A qualitative methodology was selected as it allows for an in-depth analysis of the gender dynamics underpinning victim-survivor experiences in cyber-scam centres. A total of 89 qualitative consultations were conducted with 86 stakeholders and three victim-survivors who experienced TIP for forced criminality in the South-East Asian region. In-depth interviews allowed for detailed personal accounts, while focus groups provided insight into broader, collective perspectives.

Workshop and focus groups

One workshop and two focus groups were conducted between August and October 2024 in Bangkok and Chiang Mai (Thailand) and in Manila (the Philippines) with a total sample of 64 participants.

The first workshop was held in Bangkok in August 2024 as part of a larger event jointly led by the RSO and the International Organization for Migration. The aim of the regional consultation was to facilitate structured discussion around the applicability of existing national legal frameworks that guide law enforcement, border, immigration and legal officers when responding to TIP, with particular focus on TIP for forced criminality in cyber-scam centres. The workshop involved seven small groups comprising 44 representatives from 12 Bali Process member states including Cambodia, India, Indonesia, Laos, Malaysia, the Maldives, Nepal, the Philippines, Sri Lanka, Thailand, Timor-Leste and Vietnam. Representatives primarily held government roles including prosecutors, special investigators, victim support representatives and legal, law enforcement, border and immigration officers.

The second focus group was held in Manila in October 2024. It involved two small groups and a total of 20 participants from civil society organisations with experience monitoring or responding to TIP in the region.

The third and final focus group was held in Chiang Mai and involved 12 participants. Participants were non-governmental representatives involved in responding to TIP in northern Thailand.

Interviews with stakeholders

Interviews with stakeholders included questions about women's pathways into cyber-scam centres and how they differ from men's, the technologies and online platforms involved, whether there are gender differences in the roles of men and women inside cyber-scam centres, and how this knowledge can be harnessed for prevention and response initiatives. Technologies, online platforms and contexts of interest could include the use of social media, encrypted messaging applications, AI and types of cyber-scams.

Semi-structured interviews were conducted between August 2024 and February 2025. A total of 22 in-depth interviews were conducted with representatives from different sectors involved in responding to TIP for forced criminality in cyber-scam centres in South-East Asia. Interviewees had a range of roles, including in civil society organisations, local and international NGOs, and as government officials, police and other law enforcement officers, immigration officials, media professionals and academics. Interviews were conducted in person in Bangkok, Chiang Mai and Manila, and via online videoconference.

Interviews with victim-survivors

Three in-depth interviews were conducted with victim-survivors of trafficking for the purpose of forced criminality in cyber-scam centres. The sample comprised two women and one man with lived experience from Uganda, South Africa and Sri Lanka. All interviews with victim-survivors were conducted online via video-conference. Recruitment was facilitated by project partners at the RSO through their established networks in South-East Asia. Participants were informed of who the interviewers were (ie two Australian women and an Australian man).

The interviews followed the guidelines for safe and ethical practice when interviewing victim-survivors as outlined in UN Women's (2022b) *Safe consultations with survivors of violence against women and girls*. Specifically, research staff were careful to:

- take a survivor-centred and rights-based approach;
- provide consistent information to ensure informed consent and confidentiality;
- conduct interviews only in a private, safe and accessible setting;
- give victim-survivors autonomy to speak about what they were comfortable discussing and end the interview at any time; and
- follow ethical data collection procedures to ensure their views were accurately captured.

Participants were asked questions relating to their background, how they became involved in the cyber-scam centre, their role and the roles of others, how they exited the situation and what life has been like for them since they left. Participants were paid the equivalent of A$25 for their time.

Ethics approval

This research was approved by the Australian Institute of Criminology's Human Research Ethics Committee (P0341A.A). This ethics committee is registered with the National Health and Medical Research Council and ensures that the Institute's research is conducted in accordance with the principles and guidelines set out in the *National Statement on Ethical Conduct in Human Research* (National Health and Medical Research Council 2025).

Analysis

All materials were uploaded to MAXQDA 24 for analysis, including notes from the focus groups and interviews with stakeholders and victim-survivors. Coding was guided by Saldaña's (2011) approach. Data were analysed iteratively; documents were read and re-read multiple times and coding was performed by assigning labels to meaningful segments of text. Coding involved a combination of deductive and inductive approaches. A set of codes were determined prior to analysis and developed in line with the research questions and key areas of interest. New themes were also allowed to emerge from the data, with additional codes assigned in vivo to capture these insights.

Once coding was complete, dominant themes and categories were identified across the dataset. These were analysed to explore patterns, differences and intersections, particularly with regard to gender, experiences of coercion and technology. Evidence related to different stages of the trafficking experience (eg recruitment, women's roles, exit routes, intervention) was also recorded.

The data from the focus groups and the individual interviews were analysed together to capture shared patterns and divergent themes across stakeholders as a whole. The decision to analyse these data sources collectively was related to the similarity between the participants and the aim to build a complete picture of regional knowledge on this issue.

The three interviews with victim-survivors were analysed and case summaries of their experiences were created, with some details, including their names, changed for anonymity. Themes from this material were synthesised within the broader thematic analysis to illustrate key findings and draw links of commonality between evidence provided by stakeholders and the lived experiences of victim-survivors.

A validation workshop was held in August 2025 with 13 expert stakeholders to review the findings, ensure the accuracy of the interpretations and identify any gaps or misrepresentations. All attendees were given a draft version of the report to review prior to the workshop. The event provided an opportunity to incorporate new perspectives from stakeholders who had not been involved in the research, as well as discuss themes and conclusions with some individuals who were consulted. During the workshop attendees provided verbal feedback and a number of attendees also provided subsequent written feedback. This informed refinement of the analysis and recommendations section to ensure that the final report contained information that was relevant and actionable.

Limitations

This study acknowledges important limitations regarding the scope and depth of the analysis. While a small number of interviews were undertaken with victim-survivors, findings are mostly based on second-hand accounts of cyber-scam centres provided by those with expertise in these centres through their work, their research or their investigations or responses to them. Without discounting the validity and utility of these accounts, they are nonetheless limited by the nature of stakeholders' contact with cyber-scam centres, as well as their professional and personal biases. Importantly, the large number of consultations undertaken, and efforts to consult with stakeholders across a variety of sectors and professions, partially accounts for this, but it still warrants mentioning as a potential limitation. Additionally, only three victim-survivors, all from outside of South-East Asia, could be interviewed, which further limits the generalisability of findings.

While the study centres on the experiences of women in cyber-scam centres in the South-East Asian region, it is acknowledged that women are not a homogeneous group and that women's experiences are diverse and shaped by multiple intersecting factors such as nationality, ethnicity, migration status, social class and other vulnerabilities. Due to the nature of the data collected and the sampling strategy, these nuances could not be fully explored. For related reasons, differences in the experiences of men and women in cyber-scam centres could not be systematically explored or tested. Data collection also yielded little information on how women accused of TIP for forced criminality are treated by the criminal justice system, making it difficult to examine this in much depth.

Further related to the approach to data collection, country-by-country analyses could not be conducted. This is partly due to inconsistencies in how data on trafficking and forced criminality in cyber-scam centres (and the experiences of women in this context) are recorded across the region. Consequently, the findings here should be interpreted as reflecting broader regional patterns only. Relatedly, it should be noted that the findings do not offer completely balanced regional coverage, with some countries represented more than others. This partially reflects differences in data collection opportunities, and differences in how developed each country's monitoring mechanisms are.

The need for cautious interpretation of the trends identified here is emphasised, as they may not reflect the unique context of any particular country in the region, or the diverse gender and intersectional identities of women with lived experience of this form of trafficking. It is recommended that future studies undertake more detailed comparative analysis of the experiences and trajectories of women and girls from diverse countries within South-East Asia and beyond, to better reflect cultural differences and distinct challenges faced by women and girls who have experienced TIP for forced criminality in cyber-scam centres.

Results

Characteristics and backgrounds of women trafficked into cyber-scam centres

Stakeholders agreed that most victim-survivors trafficked into cyber-scam centres are men, with women constituting a significant minority. Stakeholders from law enforcement and victim-survivor support services estimate that women and girls account for between 10 and 40 percent of victim-survivors of trafficking into cyber-scam centres for forced criminality, based on data captured in the course of their work.

There are undoubtedly varied and complex reasons why more men are being trafficked into cyber-scam centres compared to women, but stakeholders suggested two important explanations for this disparity. First, stakeholders proposed that men are more willing to seek work abroad in the absence of viable employment in their home country. In contrast, women were described as generally more cautious about travelling overseas alone for work due to safety concerns or less able to migrate due to family or caregiving duties. Another factor contributing to this difference is the type of work traffickers are advertising to deceptively recruit individuals into exploitation. Generally, stakeholders perceived that most job offers were seeking employees with IT, computer science and data analysis skills, which tend to attract a great number of applicants who are men. Women trafficked into cyber-scam centres were more often responding to employment opportunities involving marketing, sales and service roles, which comprise a smaller proportion of job offers.

As with men, women victim-survivors tend to be young adults, between the ages of 18 and 30, who are seeking jobs after school or university. Stakeholders also identified a cohort of girls aged under 18, some as young as 11 but mostly aged between 14 and 16, who are being recruited into cyber-scam centres. However, multiple stakeholders argued that children tend not to be targeted by the criminal syndicates for recruitment into cyber-scam centres as scammers as they are more likely to draw the attention of authorities and to be the focus of rescue efforts and law enforcement activity:

> … this 16-year-old girl told me that the scam boss actually doesn't want to receive her … [the] scam compound doesn't want minors because they are more problematic and the law enforcement or United Nations will go after chasing the minor cases more than others so they don't want them. (SH12, Researcher)

Some stakeholders also highlighted that due to their age some girls may lack the skills and experience required to be effective scammers. For these reasons, girls are regularly turned away from cyber-scam centres upon arrival, with reports of some girls even using fake identification to gain access to a scamming role.

Information from stakeholders suggests that women and girls from diverse nationalities are being exploited in cyber-scam centres across South-East Asia and are primarily being trafficked from other countries within South-East Asia, as well as South Asia, Central Asia, the Middle East, Africa and Europe. In particular, several stakeholders had observed an increase in the number of women from African countries being trafficked into cyber-scam centres over time:

> We have clients from Nepal, Africa, Thailand, the Philippines. We've had people reaching out to us from Indonesia, Malaysia. It's a mix. (SH4, NGO)
>
> I think, lately, the victims have been more from the African countries [than] in the past that I have engaged with. (SH9, NGO)

Likewise, stakeholders reported variance in the socio-economic and educational status of victim-survivors. In general, women victim-survivors came from lower socio-economic and educational backgrounds and were recruited for low-skill jobs:

> … they are mostly from low educational background and looking for manual jobs like hairdressing, working in nail salon, working in a cafeteria … (SH11, NGO)
>
> [The work is] quite basic—typing, knowing how to use dating apps, knowing how to communicate. (SH1, NGO)

Women may also come from disadvantaged family backgrounds characterised by poverty, unemployment, family and domestic violence, and debt. In many cases, women come from countries where there is conflict or instability, and a lack of work opportunities. However, several stakeholders had also supported highly educated victim-survivors with tertiary qualifications, as well as computer, IT and multilingual skills:

> I talked to an Ethiopian woman … She's a very educated woman in her own country, she has a degree in linguistics, she speaks perfect English. (SH5, Journalist)
>
> Overall, the women recruited are young, and often quite well educated—they are looking for professional and service-oriented jobs. (SH8, NGO)

Broadly speaking, the profile of victim-survivors (and women specifically) is diverse in terms of background, ethnicity and socio-economic status. However, this represents a high-level snapshot of women and girls across the region, and the nature of the data analysed here precludes more detailed examination of relevant country-level trends.

Recruitment of women into cyber-scam centres

Personal networks

It was the view of a number of stakeholders that women are more likely than men to be recruited by someone they have a pre-existing relationship with, such as a friend, family member, romantic partner or acquaintance. Some stakeholders interpreted this trend as reflecting the exploitation of social and emotional trust, as well as the increased reluctance among women to travel abroad or across a border alone for work simply in response to an online job advertisement.

It was common for women to be recruited by men and women from their own communities, including by romantic partners. This seduction-recruitment tactic appears to be a common pathway for girls who are dating adult men online. These findings highlight that traffickers are exploiting relational trust in their efforts to recruit women and girls into cyber-scam centres. Multiple stakeholders reported that girls from the age of 11, but mostly in their late teens and early twenties, are entering cyber-scam centres, often after being recruited by men posing as romantic partners in exclusively online relationships:

> Most of the children that cross the [Thai-Cambodia] border to be a scammer … they had a problem in their family and they don't want to live with their parent or families anymore … they escape with their boyfriend or their friends and cross the border to Cambodia to be a scammer … (SH14, Law enforcement)
>
> Most of them they come for boyfriend, either the one inside or their trafficker are their boyfriends back in their own country. (SH12, Researcher)

The relationship between the recruiter and the trafficking target can be familial, platonic or romantic, but the recruiter attempts to build and then exploit the trust in the relationship to lure the victim-survivor into exploitation:

> Compared to men, women are being targeted more through offline networks, through friends and family … They don't really trust an ad online, but they will trust even a distant relative … The guy is a recruiter, he is getting paid a commission, he is like 'Ok, if I date this girl and get some emotional control over her maybe it will be easier.' (SH2, NGO)

Evidence that women are more likely to be recruited through personal networks while men are more likely to be recruited online through job advertisements may reflect traffickers' strategic efforts to exploit stereotypically gendered motivations and vulnerabilities, such as women relying more on relationships to inform significant life decisions.

Online job advertisements

Despite the trends above, women are also being recruited into cyber-scam centres through online job advertisements. This occurs when a person applies for a job deceptively advertised on mainstream social media platforms, websites and in group chats (eg Facebook, LinkedIn, Jobstreet, TikTok and Telegram). They go through a recruitment process that often closely resembles a legitimate job application process prior to being trafficked into a cyber-scam centre. Advertisements closely mimic real job postings, companies and positions. Some of these advertisements are clearly fake, emphasising unreasonably high pay or not requesting proof of qualifications or experience for roles described as being highly professional. However, others are extremely difficult to distinguish from legitimate job advertisements. After applying, the 'company' may ask applicants to provide their resume and work history, and there can be a series of online interviews before they are offered the role.

A common theme in the interviews was that many women applied for a purported marketing job in Bangkok before being trafficked into a cyber-scam centre in Myanmar, Cambodia or Laos. However, fake job advertisements targeted specifically at women appear to be isolated to the recruitment of 'models', attractive women whose task it is to have video calls with fraud victims. These women may be actively recruited or they may be given this role on the basis of their appearance after being recruited for another role. Women from specific regions (eg Eastern Europe) are regularly targeted to work in modelling and film production, or as entertainers in casinos, bars and clubs. These women may work remotely (online only) or in-person within cyber-scam centres, or they may be assigned to work in other parts of the criminal enterprise adjacent to scamming, such as entertainment for syndicate leaders, or to work in a casino:

> Audio and video calls are an easier job compared to sex work. It doesn't really require that much trauma I guess, and if you can do calls every day and make money then why not. (SH1, NGO)

> For each company you have models, women from eastern Europe who are lured into same job, come to work in a bar, club, production cinema company, any kind of deceiving description of the job, then they arrive in Myawaddy. (SH5, Journalist)

Despite reports of targeted recruitment for specialised roles (such as models) occurring, the basic requirements for scamming roles are the same for men and women. This includes some knowledge of computers and IT skills, typing, experience with social media, and communication and language skills, predominantly English and Chinese. Specialist education is not necessary for individuals to be effective scammers, as training, resources and equipment are typically provided upon arrival, including access to AI models and guidebooks on how to conduct scams online.

Advertisements on social media messaging applications highlight the way that victim-survivors are being re-trafficked from one cyber-scam centre to another across the region. These posts directly advertise the purchase and sale of trafficking victims. These advertisements were described as highly gendered, with men more likely to be advertised as scammers and women more likely to be advertised for sex work or service roles:

> Women who are good looking are easier to sell. There are not a lot of posts selling women as scammers, rather women are advertised by their traffickers as willing or able to work as a customer service officer or, a word translated into English akin to 'daily assistant' and could be interpreted as sex work. (SH1, NGO)

There were reports of an increase over time in the number of willing participants going into cyber-scam centres. There was general agreement that 'a mix of people' worked in cyber-scam centres, with varying levels of willingness and consent to be there. There are 'people who are there and knowingly, willingly do the scamming work, and people who were tricked to come' (SH4, NGO). The increase in people willingly seeking scamming work was related to increased awareness about cyber-scam centres in recent years, with stories about people's experiences getting back to communities. Stakeholders reported that diverse experiences of cyber-scam centres are being reported back to communities:

> There is a definite increase in willing participants. People leaving knowing what it is, and quite frankly, thinking that they can do a good job of it … If I'm a young person who's good at sales, I'm good talker, all I know is online platforms and right now I'm making $50 a month, and there you're telling me that I can make $2000 a month … You're telling me that they give you a place to stay, they feed you, and they're going to pay you all this money? That doesn't sound so bad. (SH10, Gov)

Stakeholders commented that variation in the nature of the work advertised revealed efforts to recruit willing participants. These advertisements often describe desired criteria including typing, communication skills and the ability to conduct 'calculated conversations' (SH1, NGO). Several stakeholders also noted gendered differences in the pathways of men and women into cyber-scam centres through online job advertisements. While constituting a minority of posts, some experienced scammers, predominantly men, are advertising their services online. In contrast, the online recruitment of women appears to be more consistently deceptive.

Transition from voluntary to coerced work

Not all cyber-scam centre workers are deceived about the nature, conditions and location of the work. Stakeholders spoke about a subset of women and men who voluntarily participated in the scam industry for financial gain, because they considered it to be a more lucrative alternative to similar work elsewhere:

> I think it's the economic motivation. I mean this is a very rapid way to climb the socio-economic ladder. I think you find that there are a lot of women that would be drawn in, just as there are men drawn in, in that regard. (SH13, Gov)

However, some stakeholders also believed that a significant proportion of those who entered willingly were subsequently coerced and exploited. This could occur when the nature and conditions of agreed work changed (such as from scamming to sex work) or when they were trafficked to another cyber-scam centre:

> They know it's scamming when they have the job interview … they sign a contract knowing they will do scamming but they don't know that they will be locked up for six months or a year in a room and that they will have their ID and passport taken away and that they will get paid or not. So they know the nature of the job but they don't know the condition. (SH5, Journalist)

Regardless of the circumstances under which a person entered a cyber-scam centre and their initial level of willingness or knowledge about the true nature of their role, many stakeholders described workers as trapped upon entry and prevented from leaving unless they paid an inordinate sum of money to their employer. Multiple stakeholders reported that victim-survivors were at risk of re-trafficking if they could not pay the amount required to secure their freedom. One stakeholder spoke about women being at risk of re-trafficking into sexual exploitation and men being at risk of re-trafficking into forced labour in the fisheries sector:

> After they go to Myanmar, they have to pay the money [but] it's too much money still and most people can't afford to pay the money for their release, so they are trafficked again into prostitution, [or] into the fish[ing] boat. (SH6, NGO)

Importantly, stakeholders challenged the concept of a 'willing participant' in circumstances where work contracts were undermined by deceptive conditions, financial vulnerability, the abuse of power and trust and the denial of liberty. People may be aware of some aspects of the work, such as the requirement to scam people, but then are deceived about the pay, conditions, length of contract and work location—and, critically, are kept from leaving once this deception is uncovered. Traffickers take advantage of vulnerable individuals who face economic disadvantage and desperation and are seeking to change their circumstances.

Illustrative case studies

The individual case studies below illustrate the predominant role of personal connections or networks and online job advertisements in deceptive recruitment. In the first case, recruitment occurred purely through referral by a friend, and in the third case recruitment was through a deceptive online job advertisement. The second case illustrates an interesting example of these two avenues interacting, with a friend referring the victim-survivor to the online job advertisement that they eventually responded to. However, all three responded under the impression that they were applying for legitimate jobs in customer service, marketing or data entry, and only became aware of having been deceived on arrival at the cyber-scam centre.

Case study—Eva

Eva is a young Ugandan woman who travelled to Dubai on a visitor visa looking for work. She had been having trouble finding work when a female friend told her about a marketing job available in Laos. She was hesitant to travel to South-East Asia, having never been there before, but her friend convinced her that it would be fine and many people travel there for work. Her friend gave her the contact details of Jade, a friend of hers who was a recruiter.

Eva got in touch with Jade and Jade subsequently offered Eva the job in Laos. Jade advised Eva that the job involved selling beauty products online and that she would be given training for the role. They met in Dubai, where Jade took Eva's passport and arranged for her visa to travel to Laos. Jade covered the cost of Eva's travel from Dubai to Laos, which she said would be deducted from her salary later.

Eva travelled from Dubai to Laos through Bangladesh with Jade and two others (a woman and a man) who were also going for a job with the same organisation. When they arrived at their destination in Laos, they were told that they would actually be scamming people, and were given a phone and a computer. When Eva and the other two victim-survivors said they wanted to leave, they were told they would not be able to leave unless they paid a large sum of money (US$10,000).

Case study—Zanele

Zanele is a young woman from South Africa who has a degree in education. Zanele was told about a customer service role based in Bangkok by a friend who shared a post about the job on social media. Zanele was looking for work abroad and was familiar with the region as she had travelled to Cambodia before. Zanele was wary about the potential risks of answering a false job advertisement online and took steps to verify the job, which appeared legitimate and had a recruitment process similar to other jobs she had applied for.

After arriving in Thailand, Zanele was driven across the border into Myanmar to a cyber-scam centre in an isolated area. After three days she was told that she had been brought there to work as a scammer and that she would be given a script and training to do the job. Zanele said she wanted to leave and was told she could not unless she paid a large sum of money (US$300,000), leaving her trapped.

Case study—Nimal

Nimal is a man from Sri Lanka who started looking for work online after he lost his job as an electrician. After seeing an advertisement on Facebook for a data entry job, he followed the instructions for how to apply and sent his resume to a WhatsApp number from Thailand. A man responded with more information about the role and responsibilities of the job, advising the position included accommodation, food and medical care. Nimal then participated in a telephone interview and was offered an initial contract for six months to do data entry in Bangkok, after which time he could extend his contract or move to a new role in a different location. He was required to obtain a visa to work in Thailand, for which the company would deduct US$1,000 from his salary.

When Nimal arrived in Bangkok, a driver was waiting to pick him up at the airport. The driver took him to a hotel, but later in the evening the contact person called to say that another driver would pick him up at midnight so they could get a head start on travelling to the company's office. Nimal recalls driving in the vehicle for many hours before they stopped at a river. Nimal became nervous and suspicious as there were men with guns at the river who signalled that he should get on a boat. Nimal tried to ask where he was and what was happening, but no-one spoke English. He called the company contact person, who assured him the armed men were there to ensure his safety and directed him to cross the river.

Once across the river, Nimal was taken to a compound where his belongings were searched and his mobile phone was confiscated. He was led to a room with seven other men from Sri Lanka, Bangladesh and India. An interpreter entered the room and explained that it was time to start work, and the men were led to a large room with more than 50 employees stationed at computers. A Chinese team leader forced the men to sign contracts stating they must work for a period of 12 months with a monthly salary of 20,000 Thai baht. Nimal was told if he wanted to resign, he would be required to pay a contract severance fee of 1,000,000 baht.

Women's experiences in cyber-scam centres

Forced criminality involving scamming

The primary role of women trafficked into cyber-scam centres is to carry out forced scamming, predominantly involving romance-investment scams or 'pig butchering', in which fraud victims are tricked into forming an online romantic relationship that is then leveraged to secure their investment in a fraudulent cryptocurrency scheme. Scams are tailored to the fraud victims, their circumstances and potential investment amount, with romance scams most commonly targeted at people perceived as wealthy based on their country location. Fraud victims are targeted on dating apps and social media platforms including Facebook, Instagram, WeChat, LinkedIn, Jobstreet, Viber and WhatsApp.

Roles, and specifically the roles of women, are differentiated by the stages of the scamming process. Women often have the task of making initial contact with men over dating apps and social media websites, and being the face and/or voice of phone and video calls with fraud victims. If the woman scammer is able to obtain a phone number or WhatsApp details of a fraud victim, then they will pass them on to another area in the cyber-scam centre where typically men will continue the relationship and invite the target to invest in cryptocurrencies. If fraud victims become suspicious, a video call with a 'model' is scheduled to reassure the fraud victim that their relationship (and investment) is real.

The findings show the approaches scammers use to defraud victims online are tailored towards exploiting gendered vulnerabilities, power dynamics and roles. Men appear to be the primary focus of romance scams, but people of all genders and sexual identities are being targeted:

> "They're not just targeting men [but also] women or people of any gender group or gender identity. You see that there are scams that target LGBT [lesbian, gay, bisexual and transgender] groups just as much as they target other gender groups. (SH13, Gov)

This is facilitated by women scammers adopting the identity of other women, rarely adopting the identity of a man. In contrast, men frequently impersonate women while undertaking scamming activities. This is potentially related to women comprising a minority of scammers and men being the primary target of romance scams.

Stakeholders agreed that most women are recruited to be scammers, and those who demonstrate that they are good at scamming are kept in this role. Stakeholders expressed surprise that the percentage of women in cyber-scam centres is as low as it is, given that 'both men and women could do those tasks' (SH4, NGO) and that the typical romance scam is a woman targeting a man online:

> I think that the intuition or logic behind that is that there is no reason why women would be any worse. In fact, reasonably they might be better because most of the scammers are pretending to be young women. (SH2, NGO)

Both women and men are provided with the tools to assume identities, which can be male or female. Workers are given guidebooks on how to approach conversations with fraud victims online including what to say if the scammer is pretending to be a woman or a man. Approaches to targeting women as fraud victims online were described by one stakeholder as 'a little different to the male side' (SH1, NGO) and scams are tailored to the target's circumstances:

> They will give them a book, like a guidebook on different ways to scam victims. And they will have very specific steps, you know, you will copy this paragraph, you will do this, you will pretend to be a male or a female, for example. They will have, like, a very, very specific training for the [trafficking] victim. (SH11, NGO)

Some stakeholders provided evidence of generative AI being used in real time to support scammers in problem solving and framing conversations with fraud victims. Workers can consult AI models to determine appropriate responses depending on the character they are impersonating and the characteristics of the person being targeted. This helps scammers to frame conversations and transcend gender barriers in communication, such as by allowing a man to believably portray a woman in conversations with fraud victims who are men.

Traffickers in cyber-scam centres use a range of strategies to control the behaviour of scammers, including the use of threats, physical violence, sexual violence and exploitation, and rewards. Some of these abuses are disproportionately experienced by women and girls, specifically experiences of sexual violence and multiple and concurrent forms of exploitation, as discussed further in the following sections of the report.

A key theme from the stakeholder interviews was leaders in cyber-scam centres using threats of violence to coerce victim-survivors to engage in scamming and to ensure compliance. Threats are exercised directly and indirectly, through public demonstrations of violence, punishment, humiliation and degradation. Stakeholders provided evidence of victim-survivors being openly assaulted, stripped naked and forced to remain in communal areas to warn others against disobedience. The intent behind these acts of humiliation and demonstrations of violence are to make others afraid for their own safety if they do not comply:

> People who resist, people who don't meet their quotas, people who try to escape. They end up in the river … people are aware of what's happening so most of them choose the [approach] 'I shut my mouth, I go through it and I try to get out after one year,' but they see a lot of things … a lot of torture of their own friends and then they come back in the room and they have to take care of them. (SH5, Journalist)

Stakeholders commonly reported that traffickers used threats of sexual violence to control women in cyber-scam centres in particular. Several stakeholders described how sexual exploitation is often used as punishment when women trafficked for forced scamming underperform in their role or if they lack the required language or computer skills. This included being sexually assaulted as punishment, as well as threats of being re-trafficked into another cyber-scam centre for the purpose of sexual exploitation:

> Most of the women are brought in as scammers, it's just the women who are not excellent at scamming, it's like 'Let's make use of you this way'. (SH2, NGO)
>
> Forced prostitution is actually taking a big role, whether in the victims that were originally lured for this purpose or when they weren't more effective in other roles. (SH16, Law enforcement)

Consequently, women victim-survivors may experience multiple forms of trafficking prior to escaping:

> … for women who are in these compounds, if you don't do the work, [they will] sell you to another compound where they will force you to do prostitution or you will be sexually assaulted as punishments. A lot of threats being used as a sort of method of control. (SH4, NGO)
>
> When we rescued them, they were already in a brothel, but before that they were trafficked from a scam centre to a brothel … they are threatened if they cannot meet the target, they will be trafficked into another brothel, so the next destination will be a brothel, not another scam centre. Or they will be trafficked into online sex trafficking, so they have to kind of live stream [sexual services] … (SH11, NGO)

The impact of threats of violence on victim-survivors is persistent, extending beyond their physical proximity to their abusers. For many victim-survivors 'these threats are very real to them' (SH10, Gov) and they continue to fear speaking about their experience even after they have escaped or been rescued:

> She said you can tell my story but you can never put my face or name because the people who sold me they are here … they are still there so they make sure people don't speak. (SH5, Journalist)

Women are also subjected to physical violence and torture as a method of control, including solitary confinement, sleep deprivation, starvation and electrocution. Unconventional punishments, such as forcing people to engage in extreme physical activity in the heat, were also described. Some stakeholders spoke about people being left handcuffed standing up or electric shocked at their desks if they fell asleep while they were supposed to be working:

> I have a 19-year-old female victim, she felt sleepy when she was working in the office in the scamming compound. The boss there just electric shocked her to keep her awake and to punish her for feeling sleepy during working. (SH9, NGO)

Generally, across the region, available secondary data suggest that men are more likely to be subjected to physical violence and women are more likely to be subjected to sexual violence, although the magnitude of this difference may partially reflect reporting biases (ie men being less likely to report sexual abuse due to shame). However, some stakeholders highlighted variability in violent practices across the region. In some countries, men and women were equally likely to experience extreme forms of violence. However, diverse levels of brutality can occur in different cyber-scam operations within the same country.

The illustrative case studies below all describe victim-survivors being forced to participate in romance scams (in the first case, by pretending to be a woman). The role of all three was to make contact with Western men through online dating and social media platforms and initiate a romantic or sexual relationship with them online, which would be used by others in the cyber-scam centres to lure them to invest in cryptocurrency scams. The case studies also describe long working hours with few breaks or privileges, as well as the punishments suffered for under-performance, including re-trafficking to other cyber-scam centres and sexual violence.

Case study—Nimal

While working at the compound, Nimal was forced to create a fake Instagram account with the profile of a woman. He was told to gain followers and contact American men aged over 40 years while pretending to be a woman. The purpose was to entice them to invest in cryptocurrency scams. If the target of the scam wanted to have a phone or video call with the woman in the fake profile, Nimal would provide enough information about the target and their relationship to women in the compound so that they could make these calls.

Nimal was made to work long hours without breaks and, on several occasions, he was fined 2,000 Thai baht when he fell asleep or refused to work because he needed to rest. When Nimal failed to meet performance targets he was punished by the team leader, who stopped paying his salary, withheld food and drink, cut off electricity and locked him in his room.

Case study—Eva

Eva and other victim-survivors refused to work at the first cyber-scam centre and, as a result, they were sold to another cyber-scam centre. There they were tasked with running romance scams, trying to obtain the phone numbers of potential fraud victims online. Eva did not know how to scam people and did not understand cryptocurrency, so she was unable to do the job. She refused to work in the hope that they would let her leave. Instead, the organisation locked her in her accommodation with two men. To punish them for refusing to work, the managers directed the two men to rape Eva. As a result of the assault, Eva became pregnant.

After this, Eva was then trafficked into a third cyber-scam centre, in the Golden Triangle Special Economic Zone in Laos. She started working, as she saw that it was the only way to make money to find her way home. Her boss, a woman, tasked Eva with getting 'clients', which meant finding people on social media who have money and obtaining their contact details. She stayed there almost six months, and she was paid inconsistently.

Case study—Zanele

Zanele described the cyber-scam centre she was taken to as similar to a prison. She resisted the work, and was then threatened with serious violence if she did not comply. She slept on an iron bunk bed without a mattress in overcrowded living, with eight other women in one room. The other women told her the people running the operation were dangerous and she should do what they say.

Zanele worked seven days a week, between 14 and 21 hours a day. Her role involved pretending to be five different characters online and she had to remember each character's story. Her conversations would be supervised and she was punished for any mistakes. Punishments included adding money to her debt, being beaten or being forced to run in the sun. Zanele said they did not treat men and women differently; everyone was treated the same. However, women who did not perform as scammers (including girls as young as 12) were trafficked into sexual slavery, which did not happen to men.

Exploitation as models

Another way that women are exploited in cyber-scam centres is through the role of the model. If a fraud victim wants a phone call or video call, the model is there to be the voice and face of the romance scam. The model will be briefed on the relationship and advised by the scammers who have been impersonating the love interest online about what they need to say or do during the call to persuade the fraud victim that the relationship is real and encourage them to transfer money:

> The Russian girl, she is the model for hundreds of men, one girl in a room does all the video calls. Basically, they go and brief her on the background of the person, they said 'Ok it's this guy, we have been talking to him for six months, he is in Germany, he has this money, in 15 days he's supposed to do a transfer, this is the situation, convince him, lure him into that.' (SH5, Journalist)

Many of the romance scam targets are wealthy Australian, East Asian, North American and European men who are looking for physically attractive women from East Asian, South-East Asian, Central Asian, Eastern European and Middle Eastern countries. Women from these backgrounds are 'prized as models' (SH2, NGO). Stakeholders primarily referred to models in the context of scams involving heterosexual relationships, and no evidence was provided about models targeting LGBT+ groups. Stakeholders reported that most models are women, but there was some evidence of male models who were employed to support scams targeting rich and older women:

> We see more female models than male models, for romance scam it's easier to target men. (SH1, NGO)

Several stakeholders described how AI is used to help scammers to assume the role of models. Deep-fake technology—the use of AI to digitally alter voices, images and videos—is a mechanism through which scammers can pretend to be someone else when communicating with fraud victims. Stakeholders believed the quality and sophistication of voice and image altering technology was improving at a rapid pace, and had the potential to become more widely used in scamming operations:

> It's good enough right now to fool people with low media literacy levels … I think in some ways an even more pressing question is at what rate is it getting better, and the answer to that is extremely fast. If you just look at where it was two years ago with where it is today, the short answer is, even if it's not that good now, it's going to get there … (SH2, NGO)

Taking audio and video calls was described as easier than other roles held by women in cyber-scam centres, such as scamming and sex work. Some stakeholders reported that models were paid more than other workers and less likely to associate or interact with other people in cyber-scam centres:

> It seems like they're treated different … it sounds like they have a little more privilege than those who are doing the recruitments, the creating social media profiles, et cetera … they're not as forced. They have more stake in the game. There's more willingness, based on what the survivors are telling us. (SH4, NGO)
>
> … she was the only one to have access to make-up and be allowed to go out of the compound. She had some privileges, go for massage, go to beauty shop, shopping, to buy food. Everybody else is trapped. It's interesting in terms of [the] hierarchy of women. (SH5, Journalist)

Overall, stakeholders agreed that models tended to be allowed more privileges and freedom than other women and men in the centres. They were described as less likely to be subjected to violence and 'untouchable within the cyber-scam centres' (SH2, NGO) largely because they need to maintain an attractive physical appearance.

The case study below illustrates the role that models play in romance scams and the different treatment that models receive.

Case study—Eva

During her time in cyber-scam centres in Laos, Eva worked with several women who had the role of the model. One of the women was from South America, and two women were from the Philippines. They were young, aged in their early 20s. They spent their time talking to fraud victims, mostly on the phone but also on video calls. These women were treated differently from other workers in the cyber-scam centre: they were allowed freedom to go outside, buy new clothes and take pictures for their social media profiles. They were also paid more than other workers.

Sexual exploitation

Women's experiences of sexual exploitation in cyber-scam centres are complex and shaped by the nature of this coercive environment. Stakeholders outlined that many women and girls are subjected to overt and extreme forms of sexual exploitation and violence. Some women engage in sex work under conditions characterised by structural inequality and where the lines between consent, survival and coercion are blurred.

Sex work exists as a side industry to scamming in many cyber-scam centres, with brothels and massage parlours operating within them. Sexual services are available to men in management and leadership roles, but male scammers can also be incentivised to meet scamming targets and comply with work demands with rewards of sexual services. Some women are incentivised to undertake sex work within cyber-scam centres and are motivated by financial gain, flying in and out of the relevant town or city specifically to do this work. Women who fly in and out work on a rotating schedule where they come to engage in sex work in brothels within or connected to cyber-scam centres, and then return home for a break. However, stakeholders noted that understanding of this aspect of the phenomenon is limited:

> There is a huge number of [women] who are brought in as prostitutes or as brothel workers. Again, that's something that hasn't been looked into or researched enough to understand. Because you've got complicit ones that will fly in and out—our airlines are full of them here … [they] are clearly going in as workers. (SH15, NGO)

One stakeholder shared evidence of women who were sex workers in their country of origin knowingly travelling to Cambodia to work in the sex industry, but then being trafficked into a brothel in a cyber-scam centre. When asked about one woman's experience of this, the stakeholder replied the leader who had played the role of the broker was a woman:

> It's through her 'mommy', like the owner or the manager … saying if she works in Sihanoukville for six months there will be this much salary, and then she's free to work around and then also go to other countries … unfortunately, she got sold into the compound and to provide sex work in a brothel. (SH12, Researcher)

Depending on the nature of the criminal enterprise and its location, some cyber-scam centres (particularly the smaller ones) may rely on relationships with pre-existing local brothels to provide these services. The syndicates were described as resembling corporations in how they see sexual slavery as 'just another function like marketing or HR' (SH2, NGO). Larger scale scam operations can be situated within cities, and managers and workers who perform and behave well are given rewards such as access to sex and alcohol. One stakeholder described how sex is used to reward scammers who collect large amounts of money from fraud victims:

> There was actually a massage facility in the brothel inside the scam centre and based on what we understood, the brothel functioned to incentivise the scammers, so if someone brought in a big haul or was very effective they would get access to that brothel or to that massage facility. (SH13, Gov)

Referring to the cyber-scam centres on the Thai–Myanmar border, multiple stakeholders reported that women and young girls were being trafficked in and out of surrounding communities for the purpose of sexual exploitation and other forms of exploitation, including forced labour. There were reports of some women ('madams') running some of these operations:

> … young girls, we cannot say woman, we are talking 12–13. Heels, miniskirts, they pass them every evening. They didn't understand why, what was happening. Sometimes woman, sometimes girl, pass the river on a small boat. They come back to Mae Sot in the morning, they see them in the morning coming back. (SH5, Journalist)

Stakeholders observed temporal trends in the women's exploitation. While women have traditionally been recruited into cyber-scam centres for sexual exploitation, they are increasingly trafficked for forced criminality as scammers:

> A couple years ago, women were almost solely being trafficked to scam centres and casinos to work in the prostitution behind the scenes of the casinos [and] scam centres … However, as the rise of success in the romance scams, more and more women are being tasked for the romance scams (SH10, Gov).

It is clear from the evidence provided that the leaders of criminal syndicates running cyber-scam operations can extract additional financial gains from women and girls. This is because women and girls who turn out not to be skilled scammers can be easily reassigned to sexual exploitation, whereas men are usually only profitable as scammers. Only one group of stakeholders spoke about transgender women and their experiences in cyber-scam centres. They highlighted one case where a transgender woman was trafficked into a cyber-scam centre and was assigned to be 'a form of entertainment' for the men, implying that she experienced sexual exploitation (SH11, NGO).

Multiple stakeholders commented on women's sexual services being advertised on encrypted social media groups tailored to specific scamming hubs. These advertisements include the woman's ethnic background, the cost and the services offered. One stakeholder clarified that many women advertised on these groups have very high prices, indicating that they are targeting higher-level management and syndicate leaders rather than lower-level scammers.

Stakeholders noted that women in diverse roles within the scam industry commonly experience sexual exploitation. Sexual exploitation can be the primary form of exploitation for some women in cyber-scam centres, but often sexual exploitation is concurrent or subsequent to forced scamming. Stakeholders highlighted the compounding nature of women's exploitation in cyber-scam centres. Women's experiences of abuse are layered, as they are more likely than men to experience sexual violence in addition to other forms of violence like psychological and physical abuse. Women and girls in cyber-scam centres are at risk of experiencing sexual abuse from men at all levels—male co-workers and victim-survivors, managers and leaders:

> The female will be expected to do more serving job and provide sex for the owner, for the gang, for the supervisors also even for the other male survivors … the owner [is] trying to get as much as they can from them so they have to work in the scam compound but they also have to work in the brothel to get more money for the owner. (SH11, NGO)

Some stakeholders also spoke about intimate relationships being a form of protection against sexual violence for women in cyber-scam centres. These strategic relationships can be with male victim-survivors or someone in a leadership position. Several stakeholders commented on the intersections between class, agency and gender that relate to this. Women's capacity to navigate their experience in cyber-scam centres is constrained by their relative disadvantage and social marginalisation. It may be a way to avoid worse outcomes, but it is also a vulnerability that is exploited by men to coerce women into relationships with them:

> … in the scam centre she had no choice. One guy come and say that you have to stay with me, if not someone they will attack you in here. If you don't listen to me, if you don't let me have sex with you, nobody will protect you here. (SH17, NGO)

As this quote demonstrates, a proportion of these relationships involve coercion and intimidation, consistent with the larger criminal enterprise within which they occur. These relationships, particularly those between trafficked women and men in leadership positions in the criminal organisation, who are effectively their captors, have been described as having a 'Stockholm syndrome' (SH15, NGO) dynamic, where women compartmentalise their experience and do what they need to do to survive:

> I would also say what we are seeing is a trend towards women getting involved in romantic relationships inside the compound … we also see a lot pairing up with a Chinese boss and that gives them a sense of protection for them … I know a lot of people when they go in, they kind of compartmentalise the situation to make it easier to accept. You look at women and you go, they made this relationship with one of the bosses, and in some ways its consensual … it was a relationship, but it was a relationship under duress. (SH15, NGO)

Some stakeholders spoke about victim-survivors' experiences of pregnancy in cyber-scam centres. Management in some cyber-scam centres attempt to prevent pregnancy and sexually transmitted diseases by making barrier contraception available to workers through vending machines. The intention behind this is to reduce the number of pregnancies which 'disrupt the system' (SH15, NGO) by reducing a woman's capacity to work after childbirth. Indeed, pregnancy appears to be a key mechanism through which women exit cyber-scam centres (see *Exit routes* section).

Evidence of reproductive coercion and abuse, including forced abortions and denial of access to reproductive health care, was reported by several stakeholders:

> If the pregnancy occurred through abuse they are doing forced abortions inside the centres and if it's more consensual they are coming out pregnant … (SH15, NGO)

Another stakeholder described the case of a woman who had recently given birth who was deceived into giving her breastmilk to the male leaders, who wanted to consume it for the health benefits. Further, there was evidence of women being denied access to menstrual products as a form of coercion and shaming.

Exploitation in service and support roles

Stakeholders described women in cyber-scam centres as frequently being expected to carry out traditionally gendered, service-oriented work tasks, including catering, cleaning and other caregiving, in addition to their primary roles as scammers. The workers who occupy standalone roles as caterers, cleaners and caregivers are also usually women. This means women experience multiple and concurrent forms of exploitation that men are less likely to experience. The environment of cyber-scam centres reflects real-world and regional gender inequality observed across South-East Asia more broadly, where women disproportionately undertake multiple forms of care work and emotional labour and are expected to prioritise the needs of others.

Women are the primary providers of emotional, sexual and domestic labour in cyber-scam centres, with one stakeholder stating they are 'viewed as a servant of people there' (SH11, NGO). These forms of labour can be standalone roles, or performed alongside other roles, such as scamming. These layered forms of exploitation reflect entrenched gender hierarchies and norms:

> For the survivor that share with me, mostly the main job is scammer. But for the female, they do another thing, for example, they can be a cleaner, they have to cook … when people are sick they can look after them. They do a lot of what we could call 'serving jobs' for the people who stay in the centre. They serve their needs, like physical need, sexual need, anything … (SH11, NGO)

One stakeholder commented on the significant logistical operation involved in feeding the workforce inside the cyber-scam centres, insisting that this was run primarily by women. They noted that each day women arrange for massive amounts of food to be transported over the border into the cyber-scam centres to feed the workers inside:

> You have Chinese restaurants who do every day a huge daily delivery of trucks, and this is women who deal with the business. (SH5, Journalist)

Other support-based roles held by women in cyber-scam centres included those related to training, contract management, paying salaries, ensuring quotas are met, managing resignation payments, as well as negotiating the release of victim-survivors from the cyber-scam centre or their re-trafficking to another centre. There was evidence that women occupy accounting roles, for which they were recruited by personal contacts such as friends and relatives, rather than deceptive online job advertisements.

Women frequently occupy receptionist roles, particularly in smaller cyber-scam centres. Commenting on evidence from a raid of a cyber-scam centre in the Philippines, one stakeholder identified women as holding this role as the first point of contact for any external person entering the business. Further, they outlined how the reception area is strategically located and physically separated (such as by several corridors and walls) from the operational spaces where scamming occurs. This environment is designed intentionally so that, if there is a raid by law enforcement, the receptionist can warn workers and managers to give them sufficient time to shut down their computers and hide evidence:

> … the role of this person at the front of the reception is really to alert the others inside to shut down your computers if a raid happens, or if there's any urgent need to do that. So that was something to notice that two actually young woman were seated at reception, sometimes with men, sometimes alone. (SH16, Law enforcement)

It is notable that these forms of service work are all public- and customer-facing roles. Some stakeholders asserted that women occupying these roles may be absorbing disproportionate risk (by design) and that women may be strategically positioned in these roles to present a more trustworthy or approachable face for criminal operations. This finding also relates to women's roles and responsibilities in recruitment and as leaders in the criminal enterprise, discussed below.

Recruiting others

Most stakeholders reported that women are often tasked with recruiting others (primarily women but also men) into forced criminality and sexual exploitation in cyber-scam centres. This recruitment occurs online, in person and through labour hire and travel agencies. Several stakeholders reported an apparent increase over time in the proportion of women working as recruiters in cyber-scam centres. However, these accounts were largely anecdotal and other forms of data to verify this trend were not available.

Some stakeholders described women's roles in recruitment as facilitators, evidenced by reports of women commonly being involved in transporting victim-survivors, such as driving victim-survivors from the airport to their accommodation and then to the border. Women's duties involve building trust during the recruitment process, reassuring new arrivals, and creating a false sense of safety to ensure cooperation until the new recruit is secured at the destination. Stakeholders explained that the strategic use of women in these roles was driven by stereotypes about women appearing less threatening and more trustworthy than men.

In some cyber-scam centres, recruiting other people is a key performance indicator in addition to scam activity. Victims may be required to recruit someone to take their place if they want to leave (see *Exit routes* section). Recruitment was also positioned as a way for women to move up from the lower-level roles and achieve a higher degree of autonomy. These findings highlight the dual role of these women as victims and perpetrators (the victim–offender overlap) and the difficulty of identifying people as victims within coercive environments such as cyber-scam centres. For some women, achieving a promotion is a survival strategy or a pathway to escape their own exploitation:

> … if you're brought in a scammer [and] you're bad at scamming so you're made into a sex slave, at first you have no rights, but then if you cosy up to the management or if you somehow impress them they might give you the autonomy to go out of the centre and recruit ten more women … (SH2, NGO)

There is also evidence that women are required to recruit men into cyber-scam centres using seduction tactics. This is consistent with observations recorded earlier (see *Personal networks*), about women being recruited using tactics similar to those characterising romance scams aimed at wealthy fraud victims. A stakeholder gave an example of a case where a number of Brazilian men were trafficked into a cyber-scam centre after 'having an affinity for an attractive young woman who it later turned out was one of the individuals who was involved in recruitment' (SH13, Gov).

Leadership roles

Stakeholders indicated that men occupy most management and leadership positions in cyber-scam centres. Outside of recruiters and some high-profile cases of women prosecuted for offences relating to TIP in cyber-scam centres, there was little evidence of women holding positions of authority. Most commonly, when women were described as holding leadership positions, they were a team leader, supervisor or the second in charge:

> The boss or the leader but not the top one, it seems like the second level from the top, she is a woman because some of the victims call her 'madam' but they don't know her real name. (SH14, Law enforcement)
>
> … we see the room of their team leader and it's a woman, and she has more space, she has a bed for herself, she has more items … then the group of team leaders sitting together, they were having a break at the time of the raid and many of them are women. (SH16, Law enforcement)

Law enforcement stakeholders from diverse regions reported that data available in police reports, person of interest lists and witness testimony from victim-survivors show that some women have been identified as leaders in cyber-scam centres at different levels:

> There are female kingpins that can be identified. Some of them are quite publicly known … [they] were both the daughters of key patriarchs of powerful militia groups, and you see similar things in other areas as well. (SH13, Gov)

In one of the focus groups, stakeholders suggested that women's likelihood of having a higher-level role in the criminal network was related to women's role in society more broadly (ie more likely in areas with more gender equality). Relatedly, women's presence within the upper ranks is often linked to their familial or romantic relationship with a male co-offender. In this regard, women's offending and leadership was at times interpreted as lacking agency, assuming criminal responsibility in a supportive capacity rather than through having real authority and power.

Exit routes

Stakeholders spoke of a range of avenues through which people exit cyber-scam centres, including diplomatic intervention, ransom payments, paying off 'debts' owed to the criminal syndicate, persistent refusal to work, recruiting someone else to take their place, being allowed to leave and escaping. The findings reveal that the primary gender difference in pathways out of cyber-scam centres relates to women's role as recruiters, their likelihood of seeking help and their experience of pregnancy.

Diplomatic intervention can help victim-survivors exit from cyber-scam centres, although according to stakeholders this occurs inconsistently and is influenced by a victim-survivor's country of origin and the location of the cyber-scam centre in which they are trapped. This pathway is initiated when a victim-survivor manages to contact an NGO, law enforcement or their embassy asking to be rescued. When seeking assistance from an NGO, they must provide sufficient information that the NGO can then relay this request for rescue to the victim-survivor's embassy or relevant law enforcement. In many cases, victim-survivors cannot be rescued because there are no diplomatic links with the area in which they are being held or the embassy is not responsive.

When a person is rescued from a cyber-scam centre, what happens next depends on the country they are assessed in and the agencies involved. Generally speaking, they will undergo a screening process to determine whether they are a victim or if they were, at any point, a willing participant. In some countries, most notably Thailand, standard initial screening is conducted by first responders and if indicators of trafficking are present, a multidisciplinary team including relevant government departments, law enforcement and NGOs may be formed. The person may then be transferred to a shelter or another safe location, where they may be interviewed by a member or members of the multidisciplinary team, an NGO or law enforcement, depending on the location. This interview will further inform the victim identification process and establish whether the case meets the definition of human trafficking in that particular country. Whether the person receives victim status influences their access to further support and repatriation services.

NGO stakeholders reported their role in the rescue process varied. Some had an active role in the rescue process, whereas others described a primarily supportive role that is initiated post-rescue. Once rescued, victim-survivors may also be contacted by others from the cyber-scam centre who want to be rescued and they may pass on their details to the NGO.

One stakeholder reported that it was more common for men to reach out to the NGO for support with rescue than women. They reported that they thought this was because men were more likely to risk having an illegal phone and communicating on behalf of their group:

> I actually feel like the men seek help more than the women do. Not everybody has a phone but one person in the group kind of has this secret phone, so men are more likely to be the ones that reach out … you'll have a group of seven to eight people and there are two women in it, and there is one nominated person who is doing the communication, [it] generally tends to be men. (SH15, NGO)

Another way that victim-survivors escape is through having their ransom paid, often by family members, friends or the relevant diplomatic missions, who the syndicate leaders allow them to contact for this reason. Cyber-scam syndicates often make an initial investment in victim-survivors which they expect victim-survivors to repay before they can leave. This is usually the cost of their travel to the cyber-scam centre (eg plane ticket, accommodation) or the amount they were purchased for if they were re-trafficked. In some cases, NGOs will pay the ransom for a victim-survivor to be released, or an embassy may pay the ransom for their citizens. However, in most cases described by stakeholders, victim-survivors request money from their families to pay their ransom, or they pay it themselves.

Stakeholders reported cases involving both men and women who eventually exited the cyber-scam centre by simply 'refusing to work' (SH8, NGO). However, it is common for people who refuse to work to be tortured by traffickers in an effort to force them to return to work. If the victim-survivor endures the abuse for long enough without giving in, then they may eventually be let go. In other cases, they may be killed, or they may be re-trafficked multiple times to other cyber-scam centres before being released:

> I have an example of a girl being re-trafficked four times within half a year and the reason she was trafficked so many times is because she was crying every day and she refused to work. (SH1, NGO)

As described in the section on recruiting others, stakeholders reported that women are often tasked with recruiting others into cyber-scam centres due to stereotypes around women being perceived as more trustworthy and approachable. Multiple stakeholders reported that recruiting another person to take their place is one way that victim-survivors are exiting cyber-scam centres, but it is unclear how common this is. Aside from being forced to carry out scams themselves, this is another example of how victim-survivors are coerced to engage in criminal behaviour in the cyber-scam centres, and how victim-survivors become traffickers themselves. The act of recruiting others can be a survival strategy where victim-survivors transition into traffickers as a means to escape their own exploitation. This applies to both men and women who wish to escape:

> We're also hearing that some people will be tasked with recruiting other victims who are coming to work in these compounds … That seems to be the way to get out of these compounds. If you want to get out, you have to recruit someone else to replace them or a number of other victims who will have to come work at the compound. (SH4, NGO)

There were several examples provided of women being released after they became pregnant. One stakeholder reported that women who become pregnant in cyber-scam centres in Myanmar can have their babies taken from them after birth, and the infants are then killed and the mothers forced back to work. However, this was an isolated report. Certainly, pregnancy was described as interfering with productivity in the workplace, where pregnant women become less valuable as workers to the criminal syndicates. Stakeholders described cases where women were released towards the end of their pregnancy as the criminal syndicates did not want to pay their hospital bills or take care of them. Another stakeholder described their experience supporting a victim-survivor who became pregnant to her boyfriend while in the cyber-scam centre:

> At the time that I have interviewed her she's seven months pregnant with twins. She didn't pay any ransom If I remember correctly, the company just let her go because it would be a bit of challenge for the company to have her giving birth inside the compound and have to raise a baby … (SH9, NGO)

This is related to similar reports from stakeholders about victim-survivors being released after becoming sick. Broadly, they reported that those running scam operations do not want to take care of and feed people who are not productive workers.

A number of exit routes are evident in the cases below. In the first, the victim-survivor strategically built relationships of trust with managers in the cyber-scam centre. Because of this, she eventually convinced them to allow her to leave temporarily and used this opportunity to escape. The second and third cases include examples of victim-survivors being allowed to leave after cyber-scam centre managers came to see them as a liability due to health-related events, including pregnancy. However, in one case, the victim-survivor was still forced to pay a ransom. Interestingly, all three of these victim-survivors persistently refused to work, and were punished in a variety of ways for doing so. This does not appear to have had a direct impact on the decision of cyber-scam centre managers to allow them to leave. It is unclear whether the health-related events which eventually prompted managers to allow victim-survivors in the latter two cases to leave compounded their pre-existing perceptions of these victim-survivors as liabilities, or whether these events were the catalyst for such perceptions.

Case study—Zanele

Zanele is sociable and outgoing by nature and she used these skills to get by while she was inside the cyber-scam centre. She taught some of the managers how to dance and sing, which increased their trust in her over time. After nine months in the cyber-scam centre, Zanele convinced the organisation to let her leave temporarily to visit her mother, who was unwell. They reduced her debt to one-third of the original amount, and while it remained a substantial figure, she was able to pay it after borrowing money from people she knew at home. She left and did not return.

Upon returning home to South Africa, Zanele was very depressed and experienced severe post-traumatic stress disorder for a year. She still has nightmares but cannot afford to go to a psychologist. She received support from her church and pastor, who encouraged her to seek work again so that she could repay her debts to her friends and family. She ended up returning to Thailand to find work and is now working as a teacher.

Case study—Nimal

Nimal required daily medication for a chronic health issue, but he was not allowed to obtain the medication when his supply ran out and was also refused access to a doctor. Nimal became so unwell that he thought he might die. It was only at this point that he was allowed to leave the compound if he paid a ransom equal to the small amount of money he had earned while working in the scam compound for six months. After exiting the compound, Nimal sought medical treatment at a hospital and, with the help of an NGO, travelled back to Bangkok before flying home to Sri Lanka.

Case study—Eva

Eva became pregnant after being raped as punishment for not working at the second cyber-scam centre she was trafficked to. She was then trafficked to a third cyber-scam centre, where she kept her pregnancy a secret until she went into labour and took herself to a hospital within the Special Economic Zone. She used the money she had made from scamming to pay the hospital bill. One of the managers from the cyber-scam centre brought her things to the hospital and said she was free to go. Eva was able to contact a woman she had previously worked with at the cyber-scam centre who had left and lived nearby. The woman acted as translator between Eva and police, and the police then took her to a shelter in Thailand, where an NGO helped her get home.

Intervention and response

Prevention, education and awareness

Stakeholders highlighted the importance of delivering engaging, tailored and grassroots prevention and awareness campaigns to prevent trafficking into cyber-scam centres for forced criminality. These awareness raising efforts should include community outreach to at-risk groups and communities, with a focus on local trends and the gendered nature of recruitment practices.

Stakeholders emphasised the importance of delivering education and awareness initiatives that focus on high-risk cohorts such as recent school leavers, university students and job-seekers in source, transit and destination countries. They noted that a key aim of these campaigns should be to reduce the number of people who are answering deceptive job ads and travelling abroad for this purpose. For young people and school leavers, it is important that awareness campaigns are engaging, delivered on relevant platforms and co-designed with persons with lived experience of trafficking. People seeking work are at highest risk of this type of exploitation, so it is important that this group is taught to identify common strategies traffickers use in fraudulent recruitment advertisements:

> I think there needs to be more of a comprehensive response to intercepting, to stopping the victims from really responding to the ad and taking the flight and going to the transit destination, I think this is where we can have a bigger impact, intercepting and stopping the victim before they reach the scam centre. (SH16, Law enforcement)

Several stakeholders argued that improving critical thinking skills among children and adults is an important way to reduce their risk of answering a false job ad online. However, the findings from this work also show that this can only take people so far, especially in the absence of an authority through which people can validate legitimate versus predatory ads online. As the evidence here shows, many false job advertisements are designed to mimic real job positions and it can be extremely difficult to distinguish which ones are false, including for people with advanced university education. While an important avenue, this approach will not prevent all cases.

We note efforts are being made to strengthen the capability of local authorities to prevent trafficking for forced criminality. For example, partnerships between NGOs and the tech sector are creating generative AI tools and chatbots that help alert potential victims to these scams and point out warning signs about suspicious job postings. Our findings suggest it is also important that campaigns recognise the differences between how men and women are being recruited. As discussed in the *Recruitment of women into cyber-scam centres* section, the evidence shows that women and girls are primarily targeted through people they know such as acquaintances, partners, friends and even family:

> Women are being targeted more through offline networks, through friends and family … The awareness with women has got to be, it's a sad realisation but just because you know someone you can't really trust them when it comes to this stuff. (SH2, NGO)

Relatedly, one stakeholder spoke about the need to raise awareness about how perpetrators, recruiters and traffickers use social engineering (ie psychological manipulation tactics) to gain trust and control over their victim-survivors. This includes educating people about what in-person recruitment often looks like. For example, if a stranger tries to build rapport and then suggests a job opportunity, maybe one that is abroad, additional validation processes should be investigated.

Social media platforms provide the landscape in which malicious actors access fraud and trafficking targets, and these companies therefore have a shared responsibility for preventing fraud and reducing the prevalence of predatory advertisements online. Research that has tested machine learning approaches has found that these techniques can accurately predict and identify scams and protect jobseekers from fraudulent job advertisements online (Hanif et al. 2024). However, challenges such as the evolving nature of scams, attempts by those responsible to avoid detection and limitations in research reproducibility mean that, at the time of writing, the effectiveness and application of these tools in practice remains limited (Papasavva et al. 2025).

Awareness campaigns in Hong Kong have been effective in raising awareness about trafficking into cyber-scam centres among the general population, which was associated with reductions in the number of people being trafficked from this region for a period of time. However, recently the number of women being trafficked from this region has again increased. This was related to the increasing sophistication of recruitment schemes and a rise in deceptive recruitment of a romantic or relational nature, suggesting syndicates are adapting the ways they target victim-survivors in this region:

> The awareness [raising campaigns] in Hong Kong are generally quite good, we go to shops and talk to normal people and they all aware of it. So why nowadays there are more female cases coming from Hong Kong? Maybe it's they are targeted, the transcript, the way of luring is more advanced than before. (SH12, Researcher)

Stakeholders in the focus groups and interviews agreed about the importance of delivering targeted prevention interventions for women living in regional and remote areas with limited education and opportunities for employment. Programs that upskill women and provide opportunities for work and independence can build women's skills and confidence. This may include supporting women to establish small businesses such as street food carts, providing training in traditional weaving of clothing or sarongs and helping them to sell their products in international markets such as in Europe and the United States. Programs that focus on empowering women in a range of ways, including skill development, business and employment workshops as well as therapeutic support, can have intergenerational impacts.

For small communities at risk, the campaigns should be locally driven and run. There are opportunities for sharing information and resources aimed at prevention along the Thailand–Myanmar border, such as through local women's organisations:

> It has to be extremely direct, in their language, by their own people, with people they trust, with a teacher they have for ten years. It's providing these people on the front line with the necessary material to educate their people. (SH5, Journalist)

This localised approach to prevention was described as effective in reducing trafficking of girls into China for forced marriage in pre-coup Myanmar. Prior to this, traffickers were coming into Burmese communities and promising parents to put their children through school if they allowed them to take their children away. In response, a campaign was run in which local people from Myanmar's Shan State went to schools in the region to speak with children and parents about the issue and to educate them to recognise the risk indicators. This intervention was well received and seen as successful until it was no longer possible to deliver due to instability increasing in the region.

Lastly, while it is clear that providing women and girls with opportunities for employment and skill development is important, our findings show that progress can inadvertently increase the risk of this form of trafficking. Trafficking for forced criminality exploits individuals at the intersections of poverty, education and access to the internet, and targets individuals who are desperate to change their lives and create a better future for their children and families. This vulnerability must be effectively managed during intervention, particularly with vulnerable women in marginalised settings and communities, such as refugee camps and shelters in border areas.

Victim identification processes

All stakeholders recognised the complexities of assessing and identifying victim-survivors of trafficking for forced criminality. The nature of this form of exploitation, in which people are coerced into perpetrating criminal acts, is such that individuals tend to sit somewhere on a spectrum between victimisation and perpetration rather than falling neatly into one category or another. Many are trafficked into cyber-scam centres unknowingly, while some enter knowingly and then are victimised through subjugation, exploitation and abuse. Victims of trafficking into cyber-scam centres even tend to be seen differently from victims trafficked into other forms of forced criminality (eg forced manual labour or drug trafficking), given the common perception of them as too smart and educated to have been deceived in such a manner. The proportion of willing participants in the industry also makes it challenging for authorities to identify victim-survivors.

Stakeholders also outlined that many victim-survivors do not see themselves as victims because they engaged in offending behaviour, even if they committed these crimes under duress and coercion. Many victim-survivors report mental health problems, trauma and shame associated with the crimes they committed, including scamming other victims as well as recruiting others into their same situation:

> They have some kind of mental health issue related to the way that they always constantly had to deceive other people to get involved in the scam. They say that it's just in the situation that death or life so that's why they don't have any other choice but to recruit the others …
>
> We want to inform the victims on how they can reach out for help, or how to identify that they are the victim of trafficking because some victims they don't know that they are the victim. (SH11, NGO)

Some stakeholders commented that increasing media attention to the issue has resulted in an uptick in willing participants seeking out the work. Among a subgroup of people, scamming is perceived as legitimate work that contributes to local economies. A common challenge is determining victim status when there is evidence that people willingly sought a scamming role but then were exploited, abused and unable to leave. One stakeholder reported it is important to look at the travel pattern of the person:

> It's when you have somebody who is very vague about the travel to get there, then you have to ask yourself some more questions, because they're trying to remember what they're supposed to say to make it sound like they're a victim. Somebody who's a victim can tell you exactly what happened. (SH10, Gov)

However, stakeholders agreed that the vast majority of the individuals exiting cyber-scam centres who they had supported were victim-survivors, if not all. Despite this, one stakeholder estimated only half of the people they supported would be clearly identified as victims in official screening processes. Some stakeholders reported that victim identification processes are often inadequate or absent, with many victim-survivors undergoing only basic screening processes rather than trauma-informed assessment post-exit. There was a notable lack of trauma-informed practices (such as having a safe space to ask about sexual violence) which may discourage disclosures from victim-survivors who fear criminalisation.

Some stakeholders cautioned against the use of broad questioning during screening, as the nature of this form of trafficking often requires more nuanced investigative tactics to identify. For example, many victim-survivors answer a job ad they initially perceived to be legitimate and later become trapped, or the job they accepted was not the job they were given when they arrived:

> They would ask, 'So you did agree to come to work in this job?' and they did consent to come to work but they also have to tell them they consented to come to work for a job in Thailand, not in Myanmar. (SH9, NGO)

Fear of further harm prevents many victim-survivors from speaking to authorities about their experience in cyber-scam centres after being rescued, impeding the victim identification process. Victim-survivors may not want to give evidence against a friend or family member if that is how they were recruited. In many cases, when victim-survivors are rescued they must rely on self-report as evidence, because there is rarely photographic or other physical proof of their coercion. In cases where physical evidence is available, the long wait times associated with victim identification can degrade the availability or integrity of evidence.

Regional variability in victim identification processes also means that, if someone is identified as a victim in one country, this may not translate to other countries. The victim identification process differs depending on the country the person is processed in, their nationality and the presence and resources of their embassy in that region. In some countries, victim-survivors who do not or cannot participate in the victim identification process are typically required to pay a fine for overstaying their visa and buy their own ticket to return home. While NGOs are generally restricted to supporting victim-survivors who participate in the victim identification process and are formally identified as victims, some stakeholders reported that NGOs may also offer informal support to individuals they believe to be victims, especially where formal screening mechanisms are limited.

Having a more consistent or shared definition of trafficking for forced criminality across the region was also seen as a potential strategy to minimise some of the challenges with the victim identification process (see *Institutional and legal responses* below for more on this).

Some countries have more structured approaches to victim identification, such as in Thailand through the National Referral Mechanism, while others have less structured processes. Across the region, stakeholders agreed it is important to increase the availability and consistency of national, coordinated systems for identifying and supporting trafficking victims that can connect government agencies, NGOs and service providers.

A best practice approach to victim identification was described as delivered by a multidisciplinary response team that includes a gender-based violence specialist, as this impacts on the experience of female victim-survivors and their likelihood of cooperating and reporting sexual violence in particular. First responders should be equipped to adopt a trauma-informed and gender-sensitive approach when responding to victim-survivors exiting cyber-scam centres who may have experienced gender-based violence.

Several stakeholders reported there is significant variability in the extent to which trauma-informed interview practices are embedded in police responses to this issue across the region. There was recognition that NGOs have been delivering training in trauma-informed interview practices to police in some regions for some time now, and that the training itself was not the issue. Instead, there were reports this training was not consistently implemented by responding officers on the ground. For example, evidence was provided about interviews that were conducted by male officers who repeatedly asked women if they had been raped and for details about their experience in this regard. Some NGO staff reported travelling long distances to interview survivors about their experience, using Google Translate, so they could report their sexual assault, but this often occurred with male officers nearby, watching and listening. One stakeholder provided examples of young girls who had disclosed sexual abuse and then were interviewed by male police officers, linking this experience to the under-reporting of sexual violence in this context:

> “I got one minor who disclosed she got some sexual abuse, but then when she went to the police, there are three male police officer interview her and then they keep asking her, are you getting raped? And then she gets so scared and then she says no, no. (SH12, Researcher)

Individuals exiting cyber-scam centres who are minors (under the age of 18) have been described as easy to identify as victims because they are underage. One NGO described having dedicated spaces for multidisciplinary teams to collaborate and interview child victim-survivors. These facilities allow for forensic child interviews and capacity building activities such as training for other professionals to conduct forensic interviews with children.

Support needs of women and girls

Stakeholders described mental health support post-rescue as critical, because many women exiting cyber-scam centres are experiencing significant mental health concerns. This includes post-traumatic stress disorder, psychosis and suicidal ideation and attempts. There was recognition of gendered and cultural dynamics relevant to mental health assessment of individuals across the region. Financial stress and poverty contribute to victim-survivors' risk of exploitation and their experience of poor mental health. Many women who become involved in cyber-scam centres have complex histories of disadvantage and multiple needs to address in the post-rescue period. In many cases, particularly cases involving young girls, it may not be safe to repatriate them if they came from an abusive family or relationship prior to their trafficking:

> … most of them are underage. It makes it easy to identify them to be a victim but it makes it difficult to work with them in aftercare [because] most of them have family problems. (SH14, Law enforcement)

After victim-survivors exit cyber-scam centres, shelters function as a triage point for coordinating the response. They are typically run by the military, police or NGOs, with variation across countries. Shelters have an important function in providing a safe place for victim-survivors to stay after exiting cyber-scam centres and where they can access relevant support, which is primarily provided by NGOs. This is also where the victim identification assessment often occurs. Initially, NGOs can provide basic support to victim-survivors including food, first aid and clothing. However, in government-run shelters in particular, it is usually only when a person has been identified as a victim of trafficking that they can access the full spectrum of coordinated support that is available through these shelters, including mental health, legal, repatriation and reintegration resources. The gap in service provision between rescue and victim identification, when combined with long wait times in between, was described by these organisations as a challenging space to work in. This is particularly problematic when minors are required to stay in shelters with adult men and women for long periods without knowing what will happen to them:

> While the victims are waiting for the MDT [multidisciplinary team, in Thailand] to come interview them, there's a gap of time where they're kind of in the grey area because they're not confirmed as someone who violated immigration laws and they're not confirmed as a victim yet. (SH4, NGO)
>
> For the victims, they just want to go back to their home and among them there's one minor, female minor, 16 years old. It's not beneficial for any children to drop out the school and stay in a shelter with male and female victims at the same time as them without knowing her fate. (SH12, Researcher)

Some stakeholders commented on the lack of psychosocial support available to women in shelters, including specialised mental health support for women and girls who have experienced sexual abuse and other forms of gender-based violence. One stakeholder reported they had observed a reduction in the number of victim-survivors reporting sexual violence in the cyber-scam centres between 2022 and 2024. They associated this with a lack of prosecutions initiated by police when people did report, and a growing awareness of the lack of support available, which deterred victim-survivors from reporting to police upon their release.

Relatedly, there is a need to increase the number of qualified social workers and other relevant professionals who can provide support to victim-survivors in shelters. There is a particular need for more female specialist staff to provide trauma-informed support for victim-survivors of gender-based violence. Stakeholders described the lack of female police officers as important to address to improve responses to women and girls exiting cyber-scam centres. This was noted as a challenge for the South-East Asian region broadly rather than characteristic of any particular country:

> … you've got kind of a problem in that most law enforcement across South-East Asia is predominantly men. And so, when dealing with these types of issues, how to manage that and that's not something perhaps specific to this, but I think it is an important thing potentially to look at around this research project is how to address kind of the systematic failure to include women in law enforcement. (SH13, Gov)

Many women and girls generally do not feel comfortable asking for certain forms of support from staff members or officers who are men, and men may be less likely to approach women to inquire whether they require female-specific items such as menstruation packs and appropriate underwear:

> There is not a female presence at the shelters and I think that is something that definitely should be corrected. I understand that they stay at shelters where either military or police are looking after them, but there are female military and there are female police… They should be stationed at a shelter where females are being housed, that just should be a blanket thing and it's not. (SH15, NGO)

In many cases, women will exit a cyber-scam centre in a group with others, including men, who may share the same country of origin, but then the women and men maybe separated and transported to gender-specific shelters. Some stakeholders argued that splitting the group is not always in the interests of those individuals, and can be very frightening for someone who has relied on that group throughout their experience. Isolating women from their friends and partners against their wishes can be further traumatising and discriminative.

Some stakeholders indicated that women continue to be at risk of sexual violence in the shelters after they are rescued, although conclusions cannot be drawn on whether this happens more in shelters in some countries than others. Stakeholders described cases where sexual violence was perpetrated against female victim-survivors by another male victim, and the women were relocated to another shelter that was more geographically remote from the psychosocial support they required. Relatedly, stakeholders emphasised that mental health services available in shelters in the post-rescue period need to be gender-responsive, as symptoms of poor mental health can present differently for men and women. Stakeholders also spoke about the importance of improving mental health and wellbeing systems for prevention, and about the need to challenge cultural attitudes stigmatising poor mental health and help-seeking behaviours. One approach to doing this is to provide space for people to be vulnerable and share their experiences and to offer practical guidance and support, as well as information about self-care and wellbeing.

For women with experience of trafficking for forced criminality, it is important to provide extended support to their families, who these women support (and who they may in turn be supported by). Building this capacity is related to their recovery, future health and risk of being re-trafficked. Women face unique challenges in cyber-scam centres, including the high risk of experiencing sexual violence and coercive relationships. It is not uncommon for women to exit a cyber-scam centre with a newborn child resulting from pregnancy in captivity. For women exiting cyber-scam centres with a newborn, this significant change to their circumstances necessitates comprehensive reintegration planning and access to specialised, family-oriented support. Some stakeholders argued that current support pathways within South-East Asian countries, broadly, cannot adequately address women's reintegration needs such as mental health support, paediatric care, safe housing and sustainable work:

> "For the survivor well-being, if the resources focus only on the survivor it's not really sustainable. The resources also should provide support for the people who live close to the survivor … how can we lift up the whole family? (SH11, NGO)

Several stakeholders spoke about the lack of support for victim-survivors to reintegrate into their communities of origin or elsewhere after rescue and repatriation. The lack of aftercare available to victim-survivors when they return home was described as 'a gaping hole' (SH15, NGO). Stakeholders highlighted the unique nature of the experience and the complexity of the trauma associated with it, as well as the challenge in coordinating aftercare planning when victim-survivors return home. Increasing awareness about this form of exploitation and the associated trauma people experience is important for improving access to resources that can aid victim-survivors in their long-term recovery.

Lastly, stakeholders highlighted the significant gains being made by civil society organisations who have primarily taken up the task of responding to trafficking for forced criminality in cyber-scam centres. Unfortunately, these organisations and the systems they work within were never designed to support such a significant number of victim-survivors. Recent funding cuts to civil society entities supporting victim-survivors are expected to have a devastating impact on the regional and international response to this issue. Many shelters are no longer operating, and without functioning support systems, many victim-survivors are transferred to immigration detention after exiting cyber-scam centres.

Institutional and legal responses

The primary institutional and legal responses to reduce the risk of trafficking for the purpose of forced criminality are similar for men and women. These include improving border screening processes, monitoring and regulating recruitment agencies, developing a shared definition of trafficking for forced criminality across the region, and continuing to improve information sharing between NGOs, government and police. Similar to prevention and awareness campaigns, stakeholders' recommendations mostly applied generally to men and women alike. However, there were some suggestions for responses that can be tailored to be gender-sensitive.

Airports were identified by several stakeholders as important sites for prevention. Improved screening processes in key transit hubs could identify people at risk before they leave their country of origin. Travel risk indicators included tickets being bought with cash or shortly before the trip, and travellers not having a clear travel plan and not enough spending money. Individual behaviours that indicate risk include the traveller being constantly on their phone and speaking as if they have memorised a script, making it clear they have received coaching on what to say to immigration officers. Women at risk are unlikely to be travelling with children, and while men often travel alone or with a group, young women are more likely to be in a group.

Importantly, measures such as these should be balanced against the need to preserve freedom of movement. The aim of identifying victim-survivors and at-risk individuals at transit points is to prevent victimisation, educate individuals about safer migration and employment pathways, and refer individuals to services that can provide support. Improved identification of victim-survivors and at-risk individuals at borders is not intended to justify the securitisation of migration.

A lack of recognition about the concept of forced criminality among police and border officials in some regions was reported to be a challenge to effective responses. As discussed, victim identification is hindered by a lack of understanding about the nature of forced criminality. Again, a person may receive a victim status in one region but this may not be recognised in another region. In some countries there is an assumption that a person exiting a cyber-scam centre is a potential victim, whereas in other countries people are routinely prosecuted for crimes they were coerced to commit. These regional differences in the extent to which forced criminality is recognised under law complicates the repatriation process. This could be addressed by having an agreed upon definition of trafficking in the context of forced criminality, including agreements about indicators of trafficking, how cross-border referrals should be facilitated, and processes for victim transfer and protection.

Given the global reach of this challenge, stakeholders agreed that improving cross-border and international collaboration is essential to disrupting the activities of these networks and bringing about lasting change. There are clear challenges in engaging with governing bodies in some affected and implicated countries, and additional complexity in rescuing victim-survivors from regions where there is conflict. Multiple stakeholders spoke about corruption in border areas as a facilitator of trafficking and a barrier to intervention.

> "One of the challenges of I've seen in the past couple years is cross-border collaboration and that's due to the definition of trafficking. Some countries don't recognise forced criminality. Some countries have very strict policy and even if it's forced criminality, they're going to be punished otherwise anyway. And with the nature of ... this type of trafficking, it does require cross-border collaboration. (SH4, NGO)

It is important to continue to improve collaboration and information sharing between local and national governments and the NGOs responding to TIP for forced criminality in cyber-scam centres and supporting victim-survivors. NGOs play a key role in rescuing victim-survivors and must coordinate with local law enforcement, government and other organisations to do so. While cooperation between governments, particularly in neighbouring countries, may exist at a high level, these arrangements do not necessarily translate to cooperation between officers in various departments (ie police, immigration) at the city or county level. One stakeholder described a case where the authorities from one government were attempting to rescue some of their nationals but were experiencing difficulty communicating with authorities from the government where the cyber-scam centre was based. They sought the help of a local NGO to facilitate communication and cooperation to get their citizens out of the cyber-scam centre. The NGO was able to organise the rescue through its networks and by navigating the challenges of corruption within the immigration system.

Several law enforcement stakeholders commented that their inability to publicise operational intelligence or the details of specific cases can lead the public to conclude that this sector is doing little to respond. They highlighted that publicising these operations could jeopardise the effectiveness of future efforts and threaten the safety of the individuals involved. In fact, several stakeholders reported that information sharing between affected nations and international organisations has improved over time, which has resulted in more effective responses. This includes the intelligence sharing between local and international governments and law enforcement, including Interpol, with technology companies and civil society. These partnerships have been extremely important in combatting this form of trafficking, with significant progress reported to have been made in recent years.

Notwithstanding this, stakeholders also described current efforts to shut down cyber-scam operations as primarily resulting in displacement and adaptation by the criminal syndicates involved. Enforcement and legal responses across many countries in South-East Asia have been sporadic, inconsistent and targeted at specific centres or groups, lacking the persistence, scale and comprehensiveness to permanently stamp out cyber-scam centres. Stakeholders argued that this is at least partially due to a lack of political will and, in some cases, the complicity of government authorities in this phenomenon, as well as a lack of cross-national coordination. A recent example of where persistent and comprehensive effort has had demonstrated success is in the Philippines, as discussed earlier. In order to effectively respond, stakeholders agreed that international and intersectional collaboration is required to move beyond targeted enforcement actions and case-by-case rescues, which, while important, have little disruptive impact overall:

> “Unfortunately [case by case rescues] is how it’s happening in many cases. Considering the situation, the ideal would be the takedown of this network, there needs to be a more comprehensive regional, even more so global response, if we are really going to get to that point. (SH16, Law enforcement)

In summary, stakeholders’ views on intervention were focused primarily on prevention and awareness raising. Stakeholders made several suggestions for improving victim identification processes and tailoring programs to respond to the specific support needs of women and girls. Recommendations for improvements to institutional responses related to both men and women alike, and include increasing consistency across the region in how forced criminality is defined and understood within legislation. Continuing to enhance coordination and information sharing between sectors, including local and international NGOs, government and law enforcement, was described as beneficial for improving responses to this form of trafficking.

Recommendations

Prevention campaigns

The current findings point to the importance of geographically broad awareness campaigns that are suitably targeted at and tailored to specific at-risk groups and relevant stakeholders which aim to reduce recruitment into forced criminality in cyber-scam centres, and address the conditions enabling these centres to operate. These campaigns should provide general education relating to gender dynamics and local trends in how people are being recruited into cyber-scam centres. They should focus on building critical thinking skills, particularly among young people, to equip them to better assess opportunities that seem too good to be true. Critically, these campaigns need to reach potential victims in the most common countries of origin for victim-survivors of TIP for forced criminality in cyber-scam centres, while also raising awareness and motivating responses or changed behaviours among stakeholders who are best placed to disrupt the operation of these centres. The latter include not just border officials, law enforcement and embassy staff, but also the government and private sector enablers of cyber-scam centres.

Women are primarily recruited into cyber-scam centres by someone they know, and secondarily by answering a deceptive online job ad. Further, traffickers are exploiting social trust and gendered motivations and vulnerabilities such as women's prioritisation of relationships. It is important that initiatives aimed at reducing deceptive recruitment of women reflect this evidence and highlight that recruitment often occurs through trusted individuals within their own communities, such as family members, friends, acquaintances or romantic partners. Awareness campaigns targeting young women and girls should describe how online relationships are a common way that recruiters target people. These relationships may begin with trust and affection but can be used to manipulate women and girls into exploitation. Awareness-raising materials targeted at border officials should also encourage them to probe people's reasons for crossing borders more closely and, in particular, to look beyond suspicious employment arrangements to other dubious reasons, such as meeting a partner they have never met in person before.

Lastly, prevention campaigns need to challenge misconceptions of scamming as legitimate or harmless, and provide clear information about the working conditions in cyber-scam centres, including the risks of sexual exploitation, so that people understand it is not a legitimate or easy way to make money. As our findings show, being inside a cyber-scam centre is dangerous and victim-survivors commonly leave with significant trauma and without any money, having been required to use their earnings to pay their ransom in order to leave.

Victim identification

Identifying victims of forced criminality is challenging due to variability in the nature and extent of coercion across individuals and organisational contexts. Further complicating an assessment is the fact that many people occupy a dual victim–offender status, such as people who entered voluntarily (including some who knew they would be scamming people) and were later exploited, coerced and kept from leaving. In line with recent research, our findings demonstrate the importance of tailoring victim identification processes that can account for gendered experiences, such as relational recruitment and the victim–offender overlap (Li, Liu & Franceschini 2026).

Many women experience compounded exploitation in cyber-scam centres, including both forced criminality and sexual assault. These women face similar barriers to other sexual assault survivors navigating criminal justice systems more broadly. This evidence highlights that victim identification and screening systems need to be more trauma-informed and gender-responsive to reduce the risk of secondary victimisation and further injustice. Importantly, while women and men generally face similar challenges in the victim identification process and access to services, the findings suggest that an additional potential challenge for some women is that, having entered into sexual relationships with cyber-scam centre managers, or even other scammers, they may be seen as complicit. This can create further barriers to being recognised as a victim and receiving assistance.

Action must be taken to strengthen basic screening and move towards regional consistency in official victim identification procedures. This involves broadscale implementation of coordinated national systems across the region that operate to connect government agencies, NGOs and other organisations providing support to victim-survivors exiting cyber-scam centres. Training in the delivery of trauma-informed practices should (continue to) be made available, with adaptations made depending on the cultural context.

We recommend the development of regional best-practice guidelines and concurrent investments in human resources and their adequate training to support the strengthening of victim identification processes across affected countries. Best practice guidelines should include information relevant to consistent screening protocols, trauma-informed interviewing practices, and culturally sensitive and gender-responsive approaches to ensuring people exiting cyber-scam centres undergo a fair and sensitive assessment process. The evidence collected in this study shows that the primary response should involve a multi-disciplinary team with a gender-based violence specialist.

The presence of law enforcement officers who are women is particularly important for providing gender-sensitive responses to TIP in cyber-scam centres, especially in cases where sexual assault and exploitation may have occurred. It is essential that safe, confidential spaces are available for both men and women to make disclosures, recognising that women may be less likely to disclose experiences of sexual violence to men, and that men may be less likely to disclose at all due to stigma and societal pressures.

Victim-survivor support and aftercare

As stated above, women are subjected to multiple and often overlapping forms of exploitation in cyber-scam centres, which leads to complex needs that must be addressed when they exit. Trauma-informed practices should extend beyond initial screening to the provision of tailored support. This support is critical to helping women recover from the harms they suffered and to preventing their re-trafficking back into cyber-scam centres or other forms of forced criminality.

Stakeholders described psychosocial support post-rescue, and mental health support in particular, as critical, with many women exiting cyber-scam centres experiencing significant mental health concerns. Across the region, there is a need to challenge cultural attitudes that stigmatise poor mental health and discourage help-seeking.

Our findings highlight the importance of developing comprehensive reintegration plans for women exiting cyber-scam centres who became pregnant while inside, ensuring ongoing support that includes access to mental health and paediatric care, stable housing and sustainable work opportunities, so that they can meet their own needs and those of their children. In the longer term, effective reintegration of women back into community requires the presence of strong and trusted support networks that can facilitate recovery and act as safeguards against re-trafficking (Li, Liu & Franceschini 2026).

Shelters play a critical role in providing immediate aftercare and developing longer term recovery plans with victim-survivors. To ensure these systems are gender-sensitive and responsive to the needs of women and men, boys and girls exiting cyber-scam centres, adequate funding must be provided to allow consistency in service delivery and comprehensive psychological support, acknowledging that most existing trafficking support services are already tailored towards women and children. Where possible, shelters should have women and men in support and managerial roles, including female officers who are trained in trauma-informed interviewing.

Aftercare services and shelters for survivors should be designed and implemented following UN Women's (2022a) gender mainstreaming guide, ensuring that programs are gender-responsive, culturally sensitive and inclusive. This supports the provision of services that address gender inequalities and consider the specific needs of all genders while promoting empowerment, safety and access to holistic support.

Policy

Areas for policy development related to the findings from this work include developing a regional shared definition of trafficking for forced criminality, and enhancing regulatory frameworks and oversight mechanisms for sectors implicated in scamming and organised crime, notably technology companies and recruitment agencies.

The potential benefit of having a shared regional definition of trafficking for forced criminality was a consistent theme in the research. It was argued that a consistent definition would strengthen and streamline victim identification processes, and facilitate cross-border collaboration and coordinated responses across the region. As discussed, there was consensus among stakeholders regarding the inadequacy of aftercare for victim-survivors, which was partly related to inconsistencies across countries in the extent to which forced criminality is recognised by law. Having an agreed upon definition and recognition of forced criminality is an important step towards ensuring that victim-survivors can access relevant support once they return home.

The non-punishment principle is a fundamental human right that protects victims of trafficking for forced criminality from being prosecuted for the crimes they committed under coercion, duress or as a direct result of their exploitation (Inter-Agency Coordination Group against Trafficking in Persons 2020). The non-punishment principle recognises that victim-survivors do not have a choice about whether they participate in criminal activities after being trafficked into a cyber-scam centre. ASEAN has developed practical guidelines on implementing the non-punishment principle with the aim of assisting ASEAN member states to update their domestic legislation and policy frameworks to ensure that trafficking victims are not punished for forced criminality (ASEAN 2025). Applying this principle is relevant to developing victim-centred legislation and policy across the region that prioritises a human rights approach and that can strengthen capacity to respond to organised crime.

Another key implication of these findings is the need to improve resilience and response to AI-facilitated scamming and trafficking. This requires governments to put regulatory pressure on AI providers and developers to embed safety and ethical use restrictions into online products, and disable high-risk features that are being exploited to perpetrate harm. Incorporating the principles of Safety by Design (eSafety Commissioner 2024) can help ensure large language models are developed and disseminated with built-in safeguards to prevent misuse and scamming. Recent research on the topic has also called for stronger mechanisms to hold technology companies accountable for the abuse of their products on this scale (GI-TOC 2025).

Partnerships

To have a lasting impact on these criminal enterprises, it is critical to strengthen the regional and transnational partnerships that combat cyber-scam networks and their enablers. Women are recruited from countries around the world and exploited in cyber-scam centres operating across South-East Asia, highlighting that country-specific interventions are not sufficient as a standalone response.

Continuing to improve collaboration and information sharing between local and national governments and the NGOs responding to TIP for forced criminality in cyber-scam centres and supporting victim-survivors is important. Joint law enforcement operations and coordinated policy and legislative frameworks can close loopholes exploited by leaders of criminal enterprises, who can otherwise re-traffic and continue to exploit victim-survivors. Building regional partnerships focused on implementing gender-responsive practices to support victim-survivors will improve victim identification and aftercare for women and girls exploited in cyber-scam centres.

There are clear challenges in engaging with governing bodies in some affected and implicated countries, and additional complexity rescuing victim-survivors from regions where there is conflict. Disrupting epicentres of criminal activities that have global impacts and incentivising countries to combat this form of crime where there is little political will to do so is an international responsibility that requires innovative and coordinated global strategic policy. Existing initiatives by organisations like the UNODC, the RSO and ASEAN provide critical frameworks and the spaces for collaboration and information sharing needed to achieve this goal (GI-TOC 2025).

Lastly, tracking and disrupting financial flows, including targeting cryptocurrency wallets and shutting down scam-related accounts, also contributes towards dismantling the organised crime networks behind cyber-scam centres. Developing deeper collaborations and information-sharing agreements between the private sector and NGOs may be useful in this regard. Increasing the security risks for these groups through enhanced financial surveillance and intervention undermines their operations and makes it more difficult to move large amounts of money. Continued collaboration and information sharing between intelligence agencies, the private sector, international organisations and government bodies will help to strengthen investigative efforts.

Conclusion

The operation, expansion and resilience of cyber-scam centres across South-East Asia represents a global challenge characterised by transnational criminal activity and significant human rights abuses. This research endeavoured to build the evidence around women's experiences of trafficking for forced criminality in cyber-scam centres, and explore gender dynamics underpinning victimisation and perpetration of this crime. This report represents a high-level summary of current knowledge on this topic in the context of South-East Asia, and provides a set of recommendations to strengthen current responses to the trafficking of women and girls into cyber-scam centres.

The findings have shown that victim-survivors experiences in cyber-scam centres in the region are shaped by gendered recruitment pathways, role allocation, and patterns of exploitation, with sexual violence representing a significant threat to women and girls in this context. Women and girls are often recruited into cyber-scam centres through pre-existing personal networks, including intimate partners, and are being targeted using strategies that exploit relational trust. Victim-survivors of diverse nationalities and profiles are being recruited to perpetrate romance-investment scams, where men are primarily the targets.

This research highlights that the effectiveness of current responses varies across the region. Intervention efforts are hindered by inconsistent recognition and definition of TIP for forced criminality, despite growing global awareness of, and attention to, the issue. Addressing these gaps requires integrating established frameworks, such as those outlined in the ASEAN Regional Plan of Action on Women, Peace and Security, into anti-trafficking strategies across the region. Cooperation between affected countries will be facilitated by the establishment of shared legislative and policy positions on the problem.

Delivering broadscale awareness and education campaigns that focus on local and gendered trends in recruitment, and increasing regulation of industries implicated in cyber-scam trafficking pathways, are important steps towards prevention and harm reduction. Increasing regional uniformity in victim identification processes, such as by developing best-practice guidelines for official victim identification procedures, is an important step towards providing a victim-centred and trauma-informed response.

The significant trauma associated with the layered experiences of exploitation and sexual violence among women and girls in cyber-scam centres highlights the complex treatment needs that must be addressed to facilitate their long-term recovery. Trauma-informed aftercare—including immediate safety and shelter; access to medical, mental health and paediatric care; case management and comprehensive reintegration planning—is a key area for development to ensure effective rehabilitation once victim-survivors return to their families and communities.

Finally, to achieve lasting impacts and effectively disrupt the criminal enterprise behind the scamming industry, strong partnerships and mechanisms for information sharing between local and international law enforcement, the private sector and intelligence agencies are necessary. Civil society, government and non-government organisations all play a critical role as primary frontline responders supporting victim-survivors escaping exploitation, seeking safety, pursuing legal action and accessing repatriation services. Adequate and sustained funding is essential to ensure that programs and organisations are equipped to provide secure shelter and gender-responsive care for women, men and children who require support.

To effectively combat human trafficking for forced criminality in cyber-scam centres in South-East Asia, prevention, intervention and aftercare responses must be coordinated and appropriately funded. Gender-responsive approaches are imperative to address the compounded exploitation of women in this context and ensure that the specific and long-term needs of victim-survivors are met.

References

URLs correct as at February 2026

ASEAN—see Association of Southeast Asian Nations

Association of Southeast Asian Nations (ASEAN) 2025. *Guideline on the implementation of the non-punishment principle for protection of victims of trafficking in persons*. https://www.aseanact.org/resources/asean-guideline-npp/

Association of Southeast Asian Nations 2016. *Gender sensitive guideline for handing women victims of trafficking in persons*. https://acwc.asean.org/resources/publications/gender-sensitive-guideline-for-handling-women-victims-of-trafficking-in-persons

Baxter ALA & Chazal N 2022. 'It's about survival': Court constructions of socio-economic constraints on women offenders in Australian human trafficking for sexual exploitation cases. *Anti-Trafficking Review* (18): 121–138. https://doi.org/10.14197/atr.201222188

Broadhurst R, Grabosky P, Alazab M, Bouhours B & Chon S 2014. Organizations and cyber crime: An analysis of the nature of groups engaged in cyber crime. *International Journal of Cyber Criminology* 8(1): 1–20. https://ssrn.com/abstract=2461983

Cross C 2024. Romance baiting, cryptorom and 'pig butchering': An evolutionary step in romance fraud. *Current Issues in Criminal Justice* 36(3): 334–346. https://doi.org/10.1080/10345329.2023.2248670

eSafety Commissioner 2024. Safety by Design. https://www.esafety.gov.au/industry/safety-by-design

Fitzgerald M 2024. Protecting forced offenders: Applying the non-punishment principle to victims of trafficking into scam centres. *Thai Legal Studies* 4(2). https://doi.org/10.54157/tls.276200

Franceschini, I, Li L & Bo M 2025. *Scam: Inside Southeast Asia's cybercrime compounds*. London: Verso Books

Franceschini I, Li L & Bo M 2023. Compound capitalism: A political economy of Southeast Asia's online scam operations. *Critical Asian Studies* 55(4): 575–603. https://doi.org/10.1080/14672715.2023.2268104

Franceschini, Li L, Hu Y & Bo M 2024. A new type of victim? Profiling survivors of modern slavery in the online scam industry in Southeast Asia. *Trends in Organized Crime*. https://doi.org/10.1007/s12117-024-09552-2

GI-TOC—see Global Initiative Against Transnational Organized Crime

Global Initiative Against Transnational Organized Crime (GI-TOC) 2025. *Compound crime: Cyber scam operations in Southeast Asia*. Geneva: GI-TOC. https://globalinitiative.net/analysis/compound-crime-cyber-scam-operations-in-southeast-asia/

Hanif A, Maarop N, Kamaruddin N & Samy G 2024. Machine learning approach in predicting fraudulent job advertisement. *International Journal of Academic Research in Business and Social Sciences* 14(1): 1182–1193. https://doi.org/10.6007/ijarbss/v14-i1/20532

Inter-Agency Coordination Group against Trafficking in Persons 2020. *Non-punishment of victims of trafficking*. Issue Brief no. 8. https://icat.un.org/publications

International Organization for Migration (IOM) 2024. *IOM's regional situation report on trafficking in persons into forced criminality in online scamming centres in Southeast Asia.* IOM Regional Office for Asia and the Pacific. https://migrantprotection.iom.int/en/resources/report/ioms-regional-situation-report-trafficking-persons-forced-criminality-online

Jesperson S, Alffram H, Denney L & Domingo P 2023. *Trafficking for forced criminality: The rise of exploitation in scam centres in Southeast Asia*. London: ODI Global. https://odi.org/en/publications/trafficking-for-forced-criminality-the-rise-of-exploitation-in-scam-centres-in-southeast-asia/

Li L 2024. *Lost in salvation: How the current victim identification systems fail survivors of the online scam industry in Southeast Asia. Global China Pulse*, 26 September. https://globalchinapulse.net/lost-in-salvation-how-the-current-victim-identification-systems-fail-survivors-of-the-online-scam-industry-in-southeast-asia/

Li L 2023. *Forced to scam: Pitfalls and challenges of survivor engagement in Southeast Asia's new fraud economy.* UK: Modern Slavery and Human Rights Policy and Evidence Centre. https://policycommons.net/artifacts/11274894/forced-to-scam/12160081/

Li L, Liu C & Franceschini I 2026. The gendered life cycle of forced criminality: Female victims in Southeast Asia's online scam industry. *Critical Asian Studies* 58(1): 41–61. https://doi.org/10.1080/14672715.2025.2588125

Moore N 2023. *Invested: Australia's Southeast Asia Economic Strategy to 2040: A report for the Australian Government*. Canberra: Department of Foreign Affairs and Trade. https://www.dfat.gov.au/southeastasiaeconomicstrategy

National Health and Medical Research Council 2025. *National statement on ethical conduct in human research (2025)*. https://www.nhmrc.gov.au/about-us/publications/national-statement-ethical-conduct-human-research-2025

Ng K & Simonette V 2024. 'Chinese spy mayor' wanted by Philippines arrested. BBC News, 4 September. https://www.bbc.com/news/articles/c0mnyrm8739o

Office of the High Commissioner for Human Rights (OHCHR) 2026. *"A wicked problem": Seeking human rights-based solutions to trafficking into cyber scam operations in South-East Asia.* OHCHR Regional Office for South-East Asia. https://www.ohchr.org/en/documents/thematic-reports/wicked-problem-seeking-human-rights-based-solutions-trafficking-cyber

Office of the High Commissioner for Human Rights 2025. *UN experts urge immediate human rights-based action to tackle forced criminality in Southeast Asia scam centres.* Media release, 21 May. https://www.ohchr.org/en/press-releases/2025/05/un-experts-urge-immediate-human-rights-based-action-tackle-forced

Office of the High Commissioner for Human Rights 2023. *Online scam operations and trafficking into forced criminality in Southeast Asia: Recommendations for a human rights response.* OHCHR Regional Office for South-East Asia. https://bangkok.ohchr.org/news/2022/online-scam-operations-and-trafficking-forced-criminality-southeast-asia

OHCHR—see Office of the High Commissioner for Human Rights

Organization for Security and Co-operation in Europe (OSCE) 2023. *Understanding the role of women in organized crime.* Vienna: OSCE. https://www.osce.org/secretariat/560049

Papasavva A et al. 2025. Applications of AI-based models for online fraud detection and analysis. *Crime Science* 14. https://doi.org/10.1186/s40163-025-00248-8

Raets S & Janssens J 2021. Trafficking and technology: Exploring the role of digital communication technologies in the Belgian human trafficking business. *European Journal on Criminal Policy and Research* 27(2): 215–238. https://doi.org/10.1007/s10610-019-09429-z

Raziur Rahman M 2025. A legal study on combating cyber slavery in Bangladesh through prevention and protection. *International Journal of Judicial Law* 4(3): 7–11. https://doi.org/10.54660/IJJL.2025.4.3.07-11

Rodríguez-López S 2022. Getting to know women convicted of human trafficking in Spain: Personal profiles and involvement in crime. *Women & Criminal Justice* 32(3): 242–256. https://doi.org/10.1080/08974454.2020.1835791

Royal Thai Government 2023. *Royal Thai Government's country report on anti-human trafficking efforts: 1 January – 31 December 2023.* https://www.thaianti-humantraffickingaction.org/Home/country-reports/

Saldaña J 2011. *Fundamentals of qualitative research: Understanding qualitative research*, 1st ed. New York: Oxford University Press

Sarkar G & Shukla SK 2024. Bi-directional exploitation of human trafficking victims: Both targets and perpetrators in cybercrime. *Journal of Human Trafficking*. Advance online publication. https://doi.org/10.1080/23322705.2024.2353015

Thai Ministry of Foreign Affairs 2025. Thailand-Myanmar-China Coordination Meeting on Combatting Telecommunications Fraud. https://mfa.go.th/en/content/trilat-on-telecommunications-fraud-en

Thepgumpanat P & Wongcha-um P 2025. Thailand and China to set up coordination centre to combat scam call networks. *Reuters*, 24 January. https://www.reuters.com/world/asia-pacific/thailand-china-set-up-coordination-centre-combat-scam-call-networks-2025-01-24/

UN Development Programme 2023. *Learning from provincial and district responses to trafficking in persons for forced criminality*. https://www.undp.org/publications/learning-provincial-and-district-responses-trafficking-persons-forced-criminality

UN General Assembly 2000. *Protocol to Prevent, Suppress and Punish Trafficking in Persons Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime*. Resolution 55/25. https://www.ohchr.org/en/instruments-mechanisms/instruments/protocol-prevent-suppress-and-punish-trafficking-persons

UN Office on Drugs and Crime (UNODC) 2025. *Inflection point: Global implications of scam centres, underground banking and illicit online marketplaces in Southeast Asia.* Technical Policy Brief. https://doi.org/10.18356/9789211542622

UN Office on Drugs and Crime 2024a. *Global report on trafficking in persons 2024*. Vienna: UNODC. https://www.unodc.org/unodc/data-and-analysis/glotip.html

UN Office on Drugs and Crime 2024b. *Transnational organized crime and the convergence of cyber-enabled fraud, underground banking and technological innovation in Southeast Asia: A shifting threat landscape*. https://www.unodc.org/roseap/en/resources/publications.html

UN Office on Drugs and Crime 2023a. *Casinos, cyber fraud, and trafficking in persons for forced criminality in Southeast Asia.* Bangkok: UNODC. https://www.unodc.org/roseap/en/resources/publications.html

UN Office on Drugs and Crime 2023b. *Global report on trafficking in persons 2022*. Vienna: UNODC. https://digitallibrary.un.org/record/4000879

UN Office on Drugs and Crime 2018. *Global report on trafficking in persons 2018.* Vienna: UNODC. https://digitallibrary.un.org/record/4048056

UN Women 2025. *In focus: 25 years of the Women, Peace and Security Agenda in Asia and the Pacific in 2025*. https://asiapacific.unwomen.org/en/stories/in-focus/2024/10/in-focus-25-years-of-the-women-peace-and-security-agenda

UN Women 2023. *Overview of the Regional Framework Towards Peaceful, Inclusive Societies: Advancing the Women, Peace and Security Agenda and Inclusive Governance in the Asia-Pacific Region (2023–2027).* https://asiapacific.unwomen.org/en/digital-library/publications/2023/05/advancing-the-women-peace-and-security-agenda-and-inclusive-governance

UN Women 2022a. *Handbook on gender mainstreaming for gender equality results.* https://www.unwomen.org/en/digital-library/publications/2022/02/handbook-on-gender-mainstreaming-for-gender-equality-results

UN Women 2022b. *Safe consultations with survivors of violence against women and girls*. https://www.unwomen.org/en/digital-library/publications/2022/12/safe-consultations-with-survivors-of-violence-against-women-and-girls

UN Women 2019. *ASEAN launches gender-sensitive guidelines for handling women victims of trafficking*. https://asiapacific.unwomen.org/en/news-and-events/stories/2019/01/asean-launches-gender-sensitive-guidelines

UN Women & ODI 2020. *The gendered dynamics of trafficking in persons across Cambodia, Myanmar and Thailand.* https://asiapacific.unwomen.org/en/digital-library/publications/2020/02/the-gendered-dynamics-of-trafficking-in-persons

UNODC—see UN Office on Drugs and Crime

Veldhuizen-Ochodničanová E & Jeglic EL 2021. Of madams, mentors and mistresses: Conceptualising the female sex trafficker in the United States. *International Journal of Law, Crime and Justice* 64: 100455. https://doi.org/10.1016/j.ijlcj.2020.100455

World Health Organization 2026. Gender and health. https://www.who.int/health-topics/gender

AIC reports

Consultancy report

Dr Siobhan Lawler is a Principal Research Analyst at the Australian Institute of Criminology (AIC).

Samantha Lyneham is a Principal Research Analyst at the AIC.

Dr Christopher Dowling is Research Manager of the Family, Domestic and Sexual Violence and Human Trafficking and Modern Slavery Research Programs at the AIC.

Australia's national research and knowledge centre on crime and justice

www.aic.gov.au