FREEDOM COLLABORATIVE

Deceived, Detained and Overlooked: Trafficking of East Africans into Southeast Asia's Cyber-Scam Industry

OCTOBER 2025

Deceived, Detained and Overlooked: Trafficking of East Africans into Southeast Asia's Cyber-Scam Industry

Written by: Mallika Karunan

Published by: Freedom Collaborative, Inc.

Date: October 2025

Acknowledgements

This report was developed through extensive consultation and collaboration with dedicated civil society organizations addressing trafficking for forced criminality in Southeast Asia and East Africa. We are particularly grateful to members of Freedom Collaborative's Trafficking for Forced Criminality Response Working Group, including Global Advance Projects and Acts of Mercy International, as well as to selected partners from the East and Horn of Africa Anti-Trafficking (EHAAT) Network, including Rahab Uganda, Willow International, and Awareness Against Human Trafficking (HAART) Kenya.

Their expertise, time, and contributions have been invaluable. We also extend our sincere appreciation to Jalil Muyeke for generously sharing his insights and expertise rooted in lived experience.

Introduction

The emergence of trafficking for forced criminality, both in local and inter-regional settings, is a concerning trend with serious global implications, necessitating urgent, ongoing monitoring and a coordinated response by stakeholders at all levels. This form of trafficking involves the exploitation of individuals through deception, coercion, or manipulation to force them into carrying out illicit activities that generate financial or other benefits for the traffickers.[1] Such activities can include fraud, theft, drug trafficking, organ trafficking, forced begging, online scams, and a range of other crimes.

As with other forms of domestic and transnational organized crime, these acts may occur within legally established yet under-regulated industries as well as through underground criminal networks, making detection and response particularly complex.[2] Traffickers typically use social media and instant messaging platforms to lure potential workers with the promise of legitimate employment – once a person is recruited, however, the fraudulent nature of the work is often used as a tool of control, instilling fear of criminal liability and discouraging victims from seeking help from local authorities.

In Southeast Asia, one of the most widespread forms of forced criminality in recent years is the trafficking of individuals into cyber-scam centers. These operations are notorious for entrapping and coercing people to carry out online scams through the use of control, intimidation, and abuse. At the same time, some individuals enter the centers voluntarily, with full awareness of the illicit work at hand, and initially choose to remain without overt coercion. However, the boundary between voluntary participation and exploitation is often tenuous. What begins as consent can quickly shift as workers are subjected to extended hours, withheld wages, threats, or other forms of abuse and control. This blurring of lines complicates victim identification, as individuals may not see themselves or be seen by authorities as victims, even when their conditions amount to labor exploitation or trafficking.

Previous estimates suggested that tens of thousands of individuals were trapped inside cyber-scam centers across Southeast Asia, mostly situated in Myanmar, Cambodia, and Laos.[3] However, recent law enforcement operations and data from civil society organizations (CSOs) indicate that new cyber-scam syndicates are appearing in Northern and Central Thailand, as well as other geographical pockets across Southeast Asia.[4] [5] Furthermore, the cyber-scam model

---

[1] United Nations Office on Drugs and Crime Regional Office for Southeast Asia and the Pacific. (n.d.). Explainer: What is trafficking for forced criminality? https://www.unodc.org/roseap/en/2024/10/trafficking-forced-criminality/story.html

[2] Global Initiative Against Transnational Organized Crime. (2025). Compound crime: Cyber scam operations in Southeast Asia. https://globalinitiative.net/wp-content/uploads/2025/05/GI-TOC-Compound-crime-Cyber-scam-operations-in-Southeast-Asia-May-2025.pdf

[3] Office of the United Nations High Commissioner for Human Rights. (2023). Online scam operations and trafficking into forced criminality in Southeast Asia: Recommendations for a human rights response. https://bangkok.ohchr.org/wp-content/uploads/2023/08/ONLINE-SCAM-OPERATIONS-2582023.pdf

[4] International Organization for Migration Regional Office for Asia and the Pacific. (2024). Situation analysis on trafficking in persons for the purpose of forced criminality in Southeast Asia. https://roasiapacific.iom.int/sites/g/files/tmzbdl671/files/documents/2024-03/iom-southeast-asia-trafficking-for-forced-criminality-update_december-2023-1.pdf

[5] Thai police uncover two Chinese-led online fraud rings in latest blitz against scammers. (2025, July 21). The Star. https://www.thestar.com.my/aseanplus/aseanplus-news/2025/07/21/thai-police-uncover-two-chinese-led-online-fraud-rings-in-latest-blitz-against-scammers

has now expanded beyond Southeast Asia, with new centers emerging in Latin America, West Africa, and the Pacific Islands.

Many of these operations draw heavily on the structures and methods established by the Southeast Asian compounds, replicating and adapting their tactics in new contexts.[6]

Presently, Chinese nationals constitute the largest demographic group working within Southeast Asian cyber-scam compounds. However, a substantial proportion of those affected originate from East Africa, with Ethiopians making up more than half this population.[7] This trend represents an alarming development that warrants heightened attention and coordinated action.

Against this backdrop, this report provides an overview of the current landscape of trafficking for forced criminality, with a particular emphasis on the recruitment and trafficking of East African nationals into Southeast Asian cyber-scam operations. It further examines existing responses, identifies critical gaps and challenges, and underscores the urgent need for strengthened and collaborative efforts among all stakeholders, with particular priority given to the role of civil society organizations.

Methodology

This report draws on interviews with East African nationals who exited cyber-scam centers in Myanmar between February and June 2025, conducted in Mae Sot, Thailand. It also incorporates testimonies from survivors of forced criminality who have since been repatriated and resettled in their home countries following their experiences in Southeast Asia.

Additional insights were gathered through consultations with Freedom Collaborative's Trafficking for Forced Criminality Response Working Group, a multi-stakeholder coalition that coordinates on-the-ground insights and joint actions to address trafficking for forced criminality in Southeast Asia and beyond, as well as with members of the East and Horn of Africa Anti-Trafficking (EHAAT) Network, a large collective of more than 100 anti-trafficking and migrant protection organizations in the East and Horn of Africa.

Given the limited availability of data, some findings in this report are necessarily generalized and may not be representative of every case involving East Africans emerging from Southeast Asian cyber-scam compounds. Nonetheless, the analysis provides important insights into prevailing patterns and trends. In addition, this report prioritizes the lived experiences of all survivors, without differentiating between the conditions of their entry into cyber-scam centers (whether initially voluntary or through fraudulent recruitment) or the varying degrees of coercion they experienced while inside.

---

[6] McPherson, P. (2025, April 22). Billion-dollar cyberscam industry spreading globally, UN says. Reuters. https://www.reuters.com/world/china/cancer-billion-dollar-cyberscam-industry-spreading-globally-un-2025-04-21/
https://www.reuters.com/world/china/cancer-billion-dollar-cyberscam-industry-spreading-globally-un-2025-04-21/

[7] 'I broke completely': How jobseekers from Africa are being tricked into slavery in Asia's cyberscam compounds. (2025, September 9). The Guardian. https://www.theguardian.com/global-development/2025/sep/09/cyberslavery-kenya-uganda-ethiopia-southeast-asia-myanmar-scam-centres

Current Situation

The Proliferation of Cyber-Scam Centers in Southeast Asia

Available data indicates that trafficking for forced criminality from East Africa to Southeast Asia began as early as 2021, coinciding with the rapid proliferation of cyber-scam centers in Myanmar, Cambodia, and Laos.[8] While the specific origins of each syndicate vary by country and location, the COVID-19 pandemic created conditions that enabled these operations to expand. The pandemic deepened economic instability through lockdowns, border closures, and the weakening of key sectors such as tourism, transportation and manufacturing. These disruptions led to widespread job losses and heightened poverty, particularly among young people and low-skilled workers, thereby increasing their vulnerability to deceptive recruitment and exploitation.

More broadly, global trafficking trends during this period reflected a similar pattern: traffickers capitalized on heightened socioeconomic pressures, digital reliance, and weakened protections to recruit and exploit vulnerable populations across multiple sectors. The growth of cyber-scam compounds in Southeast Asia should therefore be understood not in isolation, but as part of this wider global shift in trafficking dynamics and vulnerabilities during and after the pandemic.

Across the region, organized crime groups exploited lack of oversight and economic desperation by setting up scam compounds, often enticing foreign workers with false job promises and then forcing them into online fraud operations. The combination of political turmoil, weak governance, and economic fallout from the pandemic turned these countries into hubs for transnational cybercrime.[9] In Myanmar, the 2021 military coup and civil unrest further destabilized the country, weakening law enforcement and allowing criminal networks to flourish.

Economic Decline and Push Factors in East Africa

Meanwhile, in East Africa, the COVID-19 pandemic was responsible for great economic decline, due to reduced GDP growth, falling revenues, and inflation. Approximately 38 million jobs were depleted across the region, affecting mostly informal workers in the tourism, agriculture, and transportation sectors, pushing those who were already vulnerable into greater debt.[10] This economic precariousness became a considerable push factor, prompting people to try to leave Africa to find better economic opportunities elsewhere, leading them to job advertisements online and in local communities.

East Africans are particularly susceptible to fraudulent job recruitment due to their limited awareness of and engagement with digital safety practices. Many young people entered the job market during the pandemic – a time when education, job searches, and social interaction had

---

[8] Ratcliffe, R. (2025, September 8). Revealed: The huge growth of Myanmar scam centres that may hold 100,000 trafficked people. The Guardian. https://www.theguardian.com/global-development/2025/sep/08/myanmar-military-junta-scam-centres-trafficking-crime-syndicates-kk-park

[9] United Nations Office on Drugs and Crime. (2023, September). Casinos, cyber fraud, and trafficking in persons for forced criminality in Southeast Asia. https://www.unodc.org/roseap/uploads/documents/Publications/2023/TiP_for_FC_Policy_Report.pdf

[10] United Nations Economic Commission for Africa. (2021). Building forward for an inclusive and resilient recovery in Eastern Africa: Post COVID-19 economic outlook. https://www.uneca.org/storys/new-report-reveals-how-covid-19-has-affected-eastern-africa

moved almost entirely to the internet.[11] Yet a 2022 study found that fewer than 37 per cent of Ethiopian, Ugandan, and Kenyan children had ever received information on how to stay safe online, leaving much of the youth population ill-equipped to navigate digital risks.[12] Lacking strong digital literacy and guidance on safe internet use, many became vulnerable to high-risk behaviors, such as responding to unverified job postings or sharing personal information with recruiters.

Traffickers and brokers exploited this gap by targeting individuals through social media and messaging platforms with fraudulent offers that appeared legitimate. For jobseekers facing economic hardship and limited opportunities at home, these schemes were especially persuasive. This intersection of digital vulnerability and economic precarity has contributed to the disproportionate recruitment of East Africans into cyber-scam centers, underscoring the urgent need to embed online safety and digital literacy into prevention and youth empowerment initiatives.

Demographics and Recruitment Dynamics

The demographic makeup of cyber-scam center workers is highly diverse. Beyond Chinese nationals, East Africans comprise the largest group, particularly Ethiopians. Other nationalities represented include Kenyans, Tanzanians, Ugandans, Rwandans, Burundians, and Sierra Leoneans. Most of these nationals are adult males in their early 20s through mid-30s, and were unemployed at the time of their recruitment. Economic hardship was the most commonly cited reason for seeking work in Southeast Asia, regardless of whether they were aware that the job involved online scamming or had been fraudulently recruited.

The recruitment of East Africans into Southeast Asian cyber-scam centers generally follows one of three primary pathways:

1. Systematic online recruitment through platforms such as online job boards and social media channels.

2. Community-based recruitment involving referrals from family members, friends, or other trusted individuals.

3. Workplace-based recruitment or transfer, in which individuals are redirected or moved from previous employment arrangements, often under deceptive circumstances.

East Africans are most commonly hired through systematic online recruitment. Job advertisements that are widely published through online channels such as Facebook and Telegram remain unregulated and unmonitored, allowing deceptive and fraudulent recruitment practices – particularly for work in Thailand and Laos – to occur. Without proper safeguarding mechanisms in place, many individuals are lured by the promise of economic and job abundance in Southeast Asia and quickly move through the recruitment process, overlooking indicators of

---

[11] Krönke, M. (2020). Africa's digital divide and the promise of e-learning. Afrobarometer Policy Paper, 66. https://afrobarometer.org/sites/default/files/publications/Policy%20papers/pp66-africas_digital_divide_and_the_promise_of_e-learning-afrobarometer_policy_paper-14june20.pdf

[12] ECPAT International, Interpol, & United Nations Children's Fund. (2022). Online risks and harm for children in Eastern and Southern Africa. https://safeonline.global/wp-content/uploads/2024/12/Online-Risks-Harm-Children-ESA-2023.pdf

potential exploitation such as vague job descriptions, paid travel expenses, and instructions to travel as a tourist rather than with a legally required work permit. This issue is exacerbated by East Africans' low awareness of the fact that safe and legal employment opportunities in Southeast Asia are both limited and legally restricted for foreigners seeking employment.

When East Africans respond to online job advertisements, their initial step typically involves contacting the listed representative via WhatsApp or Messenger. A recruiter then engages with the individual directly to provide further details about the role, including salary, benefits, and other conditions of employment. Candidates next take part in a seemingly legitimate interview process designed to assess language proficiency, technical competencies such as typing speed, and their ability to interact with potential customers in English and other languages. Most survivors reported applying for positions advertised within the business, entertainment, or hospitality sectors, including roles in administration, human resources, information technology, bartending, restaurant services, acting, music, and DJing.

Recruitment also frequently occurs through community-based referrals, where individuals already working in the centers are offered financial incentives to recruit friends, family, or acquaintances. Many East African survivors reported being recruited by people they personally knew – either friends or community members already inside a center in Southeast Asia, or individuals in their local communities. This system leverages trust within social networks, making potential recruits more susceptible to false promises and subsequent coercion.

East African CSOs further report a subset of cases involving individuals who were initially recruited to work in the United Arab Emirates (UAE). Many entered under tourist visas, believing their employment to be legal. However, as their visas neared expiration and their situations became more precarious, they were targeted with messages and advertisements, often delivered directly to their phones. These communications frequently came from the same employers or brokers who recruited them initially, and offered opportunities to relocate to Thailand for work presented as similar in nature and pay to their previous roles. By this stage, survivors were typically facing financial hardship due to wage reductions or non-payment in the UAE. Desperate to continue earning and repay debts, many agreed to travel onward to Southeast Asia, often unaware that the promised employment was fraudulent and that they were being deceived into conditions of forced criminality.

Many East African survivors reported applying for these jobs with the expectation that they would be working in Thailand rather than Myanmar, Laos, or Cambodia. Thailand is an attractive destination country for workers due to its economic abundance and general receptiveness to tourists and foreigners. Enticed by these prospects, many workers applied for the fraudulent job, unaware that legal employment for foreign workers is only available in specific sectors in Thailand and requires a work permit, which each company or organization is responsible for issuing. A legitimate employer would not ask a prospective worker to travel to Thailand under a tourist visa.[13]

In addition, foreign nationals have historically faced relatively few barriers when traveling into Southeast Asia, as most nationalities are eligible for visa-on-arrival or electronic visas, which

---

[13] Siam Legal International. (n.d.). All about work permits. https://www.thaiembassy.com/thailand/work-permit-requirements

are typically valid for up to 30 days in Laos and Cambodia, and up to 60 days in Thailand.[14] Although travel restrictions were introduced in 2020 and remained in place for much of 2021 due to the COVID-19 pandemic, the subsequent easing of these measures quickly restored a high degree of travel accessibility for most foreigners entering the region, allowing individuals recruited to work inside cyber-scam centers to travel with relative ease.

Travel from East Africa to Southeast Asia

Routes taken from East Africa to Southeast Asia vary considerably depending on the recruitment method and destination country. Many survivors flew directly from their country of origin, often transiting through other major hubs in Africa such as Ethiopia, Kenya, and Ghana, or through Gulf States such as the UAE and Qatar. Less common transit hubs included countries such as Türkiye and India.

In most cases, individuals paid their own airfare, having been assured by recruiters that these costs would be quickly recovered through wages earned in Southeast Asia. Given limited financial resources, some survivors were forced to sell property, including houses, or to borrow substantial sums from relatives, friends, or even informal moneylenders. A smaller proportion of survivors reported that their flights were financed directly by their recruiter or "employer", on the condition that the debt would be repaid through their work. In such cases, traffickers frequently exploited these initial debts, whether legitimate or fabricated, by inflating or adding new charges. Survivors describe being pressured to work under conditions of debt bondage, sometimes without receiving wages for weeks or even months.

East Africans trafficked to Laos, Cambodia, or Vietnam typically transited through Thailand, which functions as a major regional hub due to the greater availability of direct flights from East Africa. Upon arrival at the destination country, most survivors reported first being taken to a "processing center" before being sent to one of various cyber-scam compounds across the region. At this stage, survivors were generally unaware of their final destination. In some cases, survivors who traveled with family members or friends were separated and sold to different centers.

For those trafficked to Myanmar, a distinct travel route emerged. After landing in Bangkok, survivors were collected by car or bus and transported in groups to Mae Sot, a rural town in northwest Thailand bordering Myawaddy, Myanmar. Many reported being unaware that they were leaving Bangkok, believing instead that they were traveling only a short distance outside the city. After a six- to seven-hour journey, they arrived at the Moei River, where they were instructed to cross by boat and on foot, unaware that the river marks the international border between Thailand and Myanmar. Several survivors stated that they did not realize they had entered Myanmar until they began conversing with other workers inside the centers.

In response to growing concerns about this trafficking route, the Kenyan Government recently introduced travel restrictions prohibiting solo holidaymakers under the age of 35 from traveling directly to Thailand. However, the measure has merely prompted traffickers to adapt their methods by rerouting recruits through Malaysia. Frontline CSOs in Thailand have documented

---

[14] MoretaPay. (2024, November 8). Understanding visas & travel regulations in Southeast Asia. https://moretapay.com/blog/understanding-visas-travel-regulations-in-southeast-asia

cases in which Kenyan and Ugandan survivors were instructed to fly into Kuala Lumpur, where they were housed in a hotel reportedly owned by the operator of KK Park, one of Myanmar's most notorious cyber-scam centers. Within days, they were transported across Malaysia's land border into Thailand – evading any official immigration process – and smuggled northward into Myanmar through the mountainous jungle, bypassing Mae Sot to avoid detection. This evolving strategy has already resulted in arrests, with a group of Kenyan nationals apprehended while transiting through Thailand and now facing potential imprisonment for illegal entry. At the time of writing, CSOs know of at least a dozen more East Africans preparing to travel this pathway, raising concerns they may also be treated as illegal migrants rather than trafficking victims, and denied due process and protection.

Upon arrival at the cyber-scam compounds, survivors were subjected to immediate intake procedures – they were photographed, fingerprinted, and blood samples were collected. They also reported the systematic confiscation of passports and personal electronic devices, including laptops and mobile phones. While a minority were able to recover their belongings upon release, many indicated that their possessions, including passports and other personal documents, were permanently withheld, leaving them without essential identification or means of communication.

Living conditions and health issues

Living conditions within cyber-scam compounds vary depending on the size of the facility and the number of individuals housed at a given time. Survivors generally described overcrowded dormitory-style rooms containing three to four bunk beds, accommodating eight to 10 people per room, with only one shared restroom for up to 20 individuals. Meals were provided a few times per day but were described as basic and often failed to meet dietary needs or restrictions. Survivors also reported missing meals altogether due to excessive working hours, which frequently extended around the clock, leaving them unable to access the cafeteria during designated mealtimes. While these accounts reflect the most common experiences reported by survivors, some noted being held in smaller apartment-style locations with fewer workers, where conditions were comparatively less crowded.

Health concerns were widely reported but access to medical care was routinely denied, with survivors forced to continue working despite illness or injury. In severe cases, some were able to negotiate release – either for themselves or for fellow workers – when conditions deteriorated to the point that urgent medical intervention at local hospitals or clinics was required. Survivors also reported physical abuse and torture, which were used as coercive measures. Injuries resulting from this violence often went untreated due to the deliberate withholding of medical supplies or services, leading to permanent disfigurement or scarring in some cases.

East African CSOs report that mental health challenges are widespread among survivors of cyber-scam centers, although these conditions are rarely diagnosed or documented until after individuals return to their home countries. The extensive abuse, coercion, and torture experienced within the centers contribute to serious and often long-lasting psychological and cognitive harm. Survivors commonly report depression, anxiety, and stress-related disorders, including generalized anxiety disorder, post-traumatic stress disorder (PTSD), complex PTSD, and panic disorder. Frequent symptoms include moderate to severe anxiety, nightmares, hallucinations, and severe insomnia, with many survivors stating they were able to sleep only one to two hours per night. In extreme cases, survivors have reported being tortured to the point of sustaining traumatic brain injuries, resulting in severe cognitive impairments; one individual, for example, was unable to recall basic information about themselves, including the names of family members or the location of their home.

These health and mental health issues often persist even after repatriation, underscoring the enduring consequences of exploitation and highlighting the critical need for comprehensive, long-term psychological and rehabilitative support for survivors.

Patterns of Abuse and Victimization inside Cyber-Scam Centers

Trafficking for forced criminality within cyber-scam centers follows patterns consistent with other forms of human trafficking. The process typically involves recruitment, transportation, and receipt of individuals through means such as threats, deception, coercion, or financial inducements, with the goal of exploiting victims for monetary gain. The defining distinction lies in the nature of the exploitation: individuals are compelled to carry out criminal activities – specifically, online scamming – for the benefit of traffickers and brokers. This form of trafficking, therefore, generates two distinct victim categories: 1) those who are trafficked and coerced into perpetrating online scams, and 2) those who are deceived and financially defrauded by the scams themselves.

Within cyber-scam centers, individuals are subjected to varying degrees of physical abuse and torture, employed as punitive measures to enforce compliance and maintain control. Survivors also reported more subtle forms of mistreatment, including verbal threats, deprivation of food and water, restrictions on free time, and limitations on movement within the centers. Notably, even individuals who voluntarily entered cyber-scam operations with prior awareness of the nature of the work were not exempt from these practices. Many described experiencing the same forms of abuse and coercion as those who had been deceived during recruitment, underscoring the pervasive use of violence and control across all groups.

As with other nationalities, East African survivors reported undergoing weeks of training inside cyber-scam centers, during which they were instructed on how to browse social media platforms and identify potential targets – commonly referred to as "customers". Once training was completed, they were moved to active scamming operations, where they were required to meet strict quotas, either in terms of the number of victims engaged or the amount of money extracted from them. Failure to meet these quotas often resulted in punitive measures, including both physical and psychological abuse, as well as the withholding of promised wages. Fear, intimidation, and the inability to leave due to heavy security measures further entrapped individuals, leaving them with no viable means of escape.

In addition to trafficking for forced criminality, survivors reported experiencing other forms of exploitation within cyber-scam centers. Women, and in some cases men, were sexually abused, most often by other workers or managers. Several women stated that they were denied access to contraceptives, resulting in pregnancies from rape or the contraction of untreated sexually transmitted infections, which were only addressed after their return to East Africa. Survivors also noted being compelled to carry out tasks unrelated to online scamming but still serving the interests of traffickers and cyber-scam syndicates. These tasks included cooking, cleaning, and general maintenance duties within the centers.

Challenges for CSOs

The exploitation of East African nationals within Southeast Asian cyber-scam centers presents significant challenges for civil society organizations working to support survivors and counter forced criminality. Survivors face layered impacts, both physical and emotional, stemming from deceptive recruitment practices, coercive training and work environments, restricted freedom of movement, and pervasive physical and psychological abuse. These conditions, combined with the highly organized and transnational nature of the criminal networks behind cyber-scamming, create complex obstacles for CSOs in identifying victims, providing tailored assistance, and advocating for survivor-centered interventions.

Assistance and Victim Identification

Preventing exploitation and assisting victims trapped in cyber-scam compounds presents significant challenges. East Africans confined within these facilities report that seeking help is nearly impossible due to geographic isolation, heavy security, and restricted movement. While some survivors negotiated their escape, many had to repay debts incurred during their travel and employment – often having borrowed from loan sharks or family members – creating additional financial vulnerability. Fear of authorities, language barriers, and cultural factors further discourage individuals from seeking help. Many survivors enter Southeast Asia already in debt, making them reluctant to request additional assistance that might compound their financial burdens.

Victim identification is further complicated by the volume and complexity of cases. When large numbers of survivors are removed from compounds simultaneously, law enforcement agencies often resort to "blanket screening", classifying entire groups either as trafficking victims or immigration offenders without individualized assessment. This approach fails to provide adequate due process, and is particularly problematic when victims are screened alongside perpetrators of the same nationality. The evolving nature of victim profiles in cyber-scam compounds adds to the complexity of victim identification. Current classification systems suggest a spectrum of victimization rather than clear categories, making systematic identification difficult under existing screening protocols.

The conditions under which screening takes place add another layer of difficulty. Limited privacy, simultaneous processing, and the prioritization of speed over thoroughness create environments unsuitable for trauma-informed, victim-centered interviews. Additionally, the limited availability of trained and qualified interpreters of East African languages – including Swahili, Amharic, Somali, and French – into Southeast Asian languages significantly prolongs the identification process and compromises the accuracy of survivors' testimonies. Some survivors, having experienced severe physical torture or sexual assault, suffer cognitive impairment or trauma that makes traditional screening impossible. In such cases, immediate repatriation for services in their country of origin becomes the only viable option.

Repatriation and Funding Challenges

East African nationals face particularly acute repatriation challenges. Most East African governments lack dedicated budgets for repatriation flights, regardless of the type of trafficking involved, creating unnecessary delays and complications. Currently, a small number of frontline

CSOs shoulder the majority of repatriation costs for affected individuals. Present expenditures and estimates suggest millions of US dollars are needed to repatriate all survivors from Southeast Asian cyber-scam centers, far exceeding available NGO and government funding.

A 2025 trilateral standard operating procedure (SOP) agreed between Thailand, Myanmar, and Cambodia has created additional barriers. This SOP requires origin countries to verify nationals and secure repatriation flights before victims can be processed for screening. For East African survivors, whose governments lack repatriation funding, this requirement effectively leaves them dependent on limited CSO support or forced to secure their own funds, resulting in many being stranded and unable to access victim identification services.

Aftercare Services and Restoration

East African survivors face significant gaps in aftercare services upon their return home. Limited inter-regional communication between Southeast Asian and East African government and CSO stakeholders creates substantial delays in service provision. East African CSOs often learn of repatriations only when contacted directly by survivors or through organizational referrals, despite government counterparts typically being aware of their nationals' return and having mechanisms to coordinate with CSOs in advance.

As with labor trafficking survivors, not all individuals returning from cyber-scam centers accept CSO-provided aftercare. Guilt and shame significantly influence this reluctance, particularly among survivors who serve as family breadwinners and feel ashamed about returning without financial resources. Most concerning is that some survivors voluntarily return to Southeast Asia and work in other cyber-scam centers, seeking income despite ongoing harm and creating cycles of re-exploitation that complicate sustainable assistance efforts.

East African CSOs face overwhelming caseloads as repatriations typically involve large groups returning simultaneously. Limited CSO presence across East Africa intensifies pressure on existing organizations already responding to this crisis. Additionally, not all CSOs can provide comprehensive services to survivors due to scope limitations, creating service gaps even where organizations exist.

Cross-Regional Information Sharing and Access to Justice

East African CSOs report significant gaps in cross-regional information sharing. Many organizations do not receive timely updates from government counterparts regarding the potential repatriation of survivors from Southeast Asia, limiting their ability to prepare for an influx of individuals in need of services. CSOs also face frustration over insufficient information on trafficking into cyber-scam centers, including travel routes, the names and affiliations of centers, and the identities of brokers and leaders. Such information is critical for developing targeted prevention campaigns, supporting survivors, and assisting law enforcement in building legal cases.

As a result, CSOs indicate that facilitating survivors' full access to justice is extremely challenging. Limited information sharing, the complexity of international cross-border cases, and survivors' often impaired ability to recall details of their trafficking experience collectively reduce the likelihood of successful legal prosecution.

Recommendations

Recommendations for CSOs responding to forced criminality in Southeast Asian cyber-scam centers can be grouped into three key areas:

1. **Awareness, Education, and Prevention** – Strengthen outreach and educational efforts to inform communities about the risks of unsafe employment and human trafficking. Proactive prevention initiatives can help identify and support at-risk individuals before they are recruited into exploitative operations.

2. **Effective Intervention and Advocacy** – Enhance intervention responses through stronger screening mechanisms at key checkpoints, and advocate for greater government engagement in repatriation and protection efforts for East African survivors. Collaborative efforts between CSOs and authorities can improve timely identification and support for victims.

3. **Aftercare and Survivor Engagement** – Expand and expedite aftercare services for returnees, including physical, psychological, and socio-economic support. Amplify survivors' voices in advocacy, policy discussions, and program design to ensure that responses are informed by lived experience.

While significant gaps and challenges persist in Southeast Asia, these recommendations prioritize actionable steps for grassroots organizations and CSOs working directly with communities and returning survivors. Emphasis is placed on creating awareness, strengthening the frontline response, and providing holistic support to survivors of forced criminality.

Awareness, Education, and Prevention

Community-Based Education and Awareness: Implement community-based initiatives and training programs focused on safe employment practices and online safety, with specific emphasis on identifying and flagging suspicious job recruitment posts. These programs should be culturally appropriate and delivered in local languages to maximize effectiveness.

Private Sector Collaboration: Strengthen collective advocacy efforts for more effective engagement with technology platforms, including Meta, TikTok, and job recruitment websites, to encourage the implementation of robust safeguards against trafficking recruitment. These companies should be urged to monitor suspicious activity, flag fraudulent job postings, and develop reporting mechanisms that enable the public to help identify potential trafficking schemes.

Pre-Departure Support Systems: Expand accessible support channels for Africans traveling abroad for employment purposes. This includes establishing and promoting helplines, providing local police contacts, and connecting travelers with NGOs that offer guidance both before departure and after arrival. Clear information about these resources should be widely distributed through multiple channels.

Intervention and Advocacy

Enhanced Screening: Strengthen screening mechanisms in East African countries of origin, particularly for individuals traveling to Thailand for employment. Given that migrant workers in Thailand are legally permitted only in the construction, fishing, and domestic sectors through registered employers, any use of tourist visas to facilitate travel for work purposes should trigger immediate intervention. Pre-departure screenings and awareness campaigns in origin countries can identify at-risk individuals and reduce trafficking vulnerability.

Transit Point Monitoring: Implement robust screening protocols at transit checkpoints in Thailand, Laos, and Malaysia. Train immigration, airport, and security personnel to detect trafficking indicators and respond appropriately. These frontline officers are crucial for identifying suspicious travel patterns and intercepting trafficking activities before they escalate.

Access to Justice: Promote inter-regional information sharing to enable comprehensive access to justice for repatriated trafficking survivors and accountability measures for perpetrators, including those from survivors' own communities. When survivors witness achievable justice, it promotes healing, restores dignity, and encourages others to seek help. Empowered survivors can become change agents, raising awareness, supporting fellow survivors, and fostering community resilience.

Aftercare and Reintegration

Pre-Repatriation Coordination: Establish systematic coordination and communication between destination countries, origin country governments, and local CSOs to connect survivors with support services before repatriation. This coordination should ensure access to medical care, psychosocial support, legal aid, and reintegration programs, facilitating dignified and secure transitions while preventing isolation, stigma, and re-victimization.

Sustained Government Commitment: Advocate for dedicated, long-term government funding mechanisms that cover repatriation and reintegration across all trafficking scenarios – not only high-profile cases. These commitments must persist beyond media attention cycles and specific operations to ensure consistent support for all survivors.

Survivor-Centered Approaches: Systematically elevate survivors' voices in policy discussions, advocacy efforts, and service design across all platforms. Survivors' firsthand experiences provide invaluable insights for shaping responsive policy, enhancing advocacy effectiveness, and creating more humane systems. Their perspectives offer frontline responders unique knowledge which is unavailable through other sources. Placing survivors at the center of decision-making and public discourse creates more just and survivor-led anti-trafficking responses.

Conclusion

Despite ongoing intervention efforts, estimates suggest tens of thousands of individuals remain detained in Southeast Asian cyber-scam compounds, though independently verified numbers are unavailable. The scale of this crisis becomes clear when comparing victim identification screenings to actual repatriations. The situation grows more complex as recent reports indicate that some survivors voluntarily return to Southeast Asian cyber-scam centers due to economic desperation and limited opportunities in their home countries. This pattern of re-trafficking highlights that the crisis will persist unless stakeholders address both the immediate rescue needs and the underlying push-and-pull factors that drive initial exploitation.

With East Africans disproportionately affected, it is critical that civil society organizations, governments, private sector actors, and other stakeholders mobilize to address gaps in repatriation and aftercare services. Preventative measures must be scaled to effectively deter trafficking, while government-level engagement and funding must be strengthened to complement CSO-led initiatives. By ensuring coordinated, survivor-centered responses and addressing the structural drivers of forced criminality, it is possible to meaningfully reduce the trafficking of East Africans and other nationals into Southeast Asian cyber-scam centers and ensure long-term protection.

FREEDOM
COLLABORATIVE