Hooked by hope

Social media as a Myanmar scam-worker recruitment tool

October 2025

By: Bo Bo

KNOWLEDGE FOR
K4DM
DEMOCRACY MYANMAR

MYANMAR
DIGITAL
RESEARCH
26

Acknowledgment

Bo Bo is a digital rights and governance specialist with over six years of experience in Myanmar. Her work spans translation, digital security training, and research for organizations focused on rights, security, and development. She has trained election observers, survey enumerators, and civic facilitators, and supported civic education research. As a digital rights practitioner, she helps civil society organization strengthen their digital security and continues to advance digital governance in Myanmar.

This paper was produced for the Knowledge for Democracy Myanmar (K4DM) initiative, with the aid of a grant from the International Development Research Centre (IDRC), and with coordinating support from The SecDev Foundation. Views expressed herein do not necessarily represent those of either organization.

K4DM was launched in 2017 by Global Affairs Canada and IDRC. It nurtures a new generation of young actors to promote inclusion, gender equality, respect for diversity, and prosperity for all in Myanmar. Through online courses, fellowships and research on digital spaces, K4DM supports diverse students and researchers primarily in the Myanmar diaspora and research institutions outside the country.

Abstract

This research examines the use of social media platforms by transnational criminal networks to recruit individuals for forced labour in cyber scam operations, with a particular emphasis on the Myanmar-Thailand border region. The study reveals the deceptive recruitment patterns employed across platforms like TikTok, Facebook and WhatsApp, based on comprehensive interviews with investigative journalists and survivors, surveys, and digital content analysis. The findings show that people who are vulnerable, mostly from poor countries in Asia and Africa, are targeted by false job ads and stories that play on their emotions. Once inside a scam compound, many recruits must deal with terrible working conditions, psychological abuse and harsh punishment for not doing their jobs well. The study also shows how collusion between criminal groups and local governments, as well as digital and geopolitical systems, help these operations continue. To stop these recruitment tactics, the authors recommend stronger platform accountability, increased cross-border policy cooperation, and improved prevention and rehabilitation efforts based on survivor experiences.

Contents

Introduction

In the past few years, cyber scams have grown from small-scale digital fraud to highly organized, militarized networks that exploit people all over the world. Southeast Asia, especially the area along the Myanmar and Thailand border, has become an important centre for these activities. Criminal gangs, paramilitary groups, and corrupt state or quasi-state actors often defend scam compounds in this area. These operations often take place in fortified areas of conflict zones where law enforcement is either not present or is working with the criminals. Even though the kidnap of Chinese actor Wang Xing in early 2025 received a lot of worldwide attention, state-led interventions are still restricted and mostly useless.

One thing that sets these networks apart is how well they use social media to find new recruits. Platforms like TikTok, Facebook and WhatsApp are not just places where misleading information can spread, but they are also important tools for finding and enticing people who are weak or vulnerable. Criminal networks hire people who are poor, unemployed, displaced by war, live in areas with weak governments, or have limited computer literacy. These workers are then forced to take part in frauds that involve romance, investment or job offers. Victims come from Myanmar, Vietnam, Bangladesh, Sri Lanka, Cambodia, the Philippines, and many African countries. They typically think they are going abroad to get real jobs.

Once inside these compounds, victims are forced to stay there and are put into internal labour groups based on their tasks. These include: 1) finding high-value targets, 2) talking to potential victims to gain their trust, and 3) 'killing,' which entails using psychological manipulation and threats to induce targets to send money. When people don't reach their quotas, they often face harsh punishments such as physical assault, electric shocks, starvation, or sexual violence. Women are more likely to be victims of gender-based violence.

Weak border government, entrenched corruption and cooperation between local militias and criminal networks are all structural and systemic problems that let these operations continue and grow. This study examines the digital and structural factors that perpetuate these unlawful networks, the human toll on their victims, and the deficiencies in policy and legal enforcement that enable their expansion. This research uses survivor testimonies and insights from frontline investigators to formulate evidence-based recommendations for prevention, intervention and rehabilitation, while enhancing the understanding of the intersection between digital technologies and transnational human trafficking and forced labour.

Methodology

A mixed-methods research design was employed. Semi-structured in-depth interviews were conducted with 4 investigative journalists and 16 individuals who had escaped from scam compounds. A digital content analysis examined more than 100 recruitment posts shared across TikTok and Facebook, evaluating common themes, imagery, language and platform-specific trends. Additionally, the study incorporated desk research, including media reports, government documents and policy statements, to situate findings within broader law enforcement and geopolitical contexts.

Key findings

Recruitment mechanisms via social media

Social media sites like TikTok, Facebook, Telegram, WhatsApp, and personal networks, are the main ways that people get jobs in cyber scam compounds along the Myanmar-Thailand border. There are a lot of job ads online that promise work from home doing things like data entry, online marketing or managing social media channels. The ads are usually written in the native languages of the people they are trying to reach, and they focus on appealing offers like high pay, free housing and easy entry. A lot of the a ds also talk about basic skills like typing or being comfortable with computers, and basic English skills, all of which make it seem like the jobs are easy to get.

Based on the survey interview data of 16 respondents, 10 respondents found the job through social media job postings, and 6 respondents found it through their closest friends and agents who introduced them to the work in scam compounds. These friends and agents often lured them in with tales of easy money and high pay. Online job search groups are where recruitment posts are most common. They can also be sent directly to people’s phones through Viber and Telegram. The messages look good to young people, aged 18 to 30, who are having trouble finding work. A lot of people are just trying to get by in a time when jobs are scarce, and they don't know that these offers are connected to dangerous scams. Because of this mix of economic need and carefully planned recruitment strategies, people are easily pulled into these networks without knowing how dangerous they are.

Job advertisements often list job positions as M1, M2 and M3, and the salary ranges are between 12,000-80,000 Thai baht (300-2,500 USD) , depending on the job. The jobs that are being advertised are for an interpreter, a personal assistant, a model (for women), an accountant, security staff, house cleaners, even cooks. The recruitment ads look professional and legitimate to young people that are financially vulnerable.

On social media like Facebook, Telegram and WhatsApp, community groups and group chats, specifically of fellow countrymen in Myanmar, can act as double-edged swords for recruitment purposes: on one hand, victims can reach out for help, and survivors of cyber scam human trafficking can use virtual communities as a relatively safe platform to speak out, raise awareness about scam recruitment methods, and warn people against traveling to Myanmar for this type of work. On the other hand, scam recruiters also lurk in these online spaces, posting their recruitment advertisements or pretending to be survivors offering rescue support, only to scam money from the victims and/or trick them to be resold to other scam/prostitution businesses (Ying, 2025).

Facebook

Facebook is the most common way that people first come across scam recruitment posts, with 39% of those surveyed saying they became scam workers through Facebook job announcements. Recruiters often use community pages and local job-seeking groups to post job openings that sound very appealing. They usually post jobs for things like online sales, digital marketing or working in a call centre, with salaries set much higher than most people can make at home. The posts are written in local languages and sometimes use the names or logos of well-known companies to make the offers seem more real. The recruiter quickly moves the conversation to Messenger when someone shows interest. Simultaneously, they give more information, which can include fake contracts, pictures of nice offices, or even videos of workers who seem to be living well. This back-and-forth makes the offer seem real, especially for young people or migrant workers who really want better jobs. Once trust is built, recruiters help with travel plans and promise to take care of housing or visas. But when the person gets there, their papers are taken away, and they are locked up in compounds and made to do online scams.

Telegram

Telegram has become the main place for openly hiring scam workers. Telegram groups openly post job openings for positions like “US chatting,” “sexy AI model,” or “high-paying online work.” This is different from other social media, where initial contact may be private or disguised as real job offers. There are often multiple posts in these groups at the same time, which makes it easy for anyone who is looking to see the opportunities. Scammers take advantage of this openness to reach a lot of people who might want to work for them, making it seem like the job is real and in high demand. Telegram has become the primary tool for criminals to advertise, persuade and coordinate workers by centralizing recruitment in these groups. This makes it a key node in the forced labour pipeline (as even those who willingly take scam farm jobs often end up in forced labour conditions if they try to leave).

TikTok

TikTok is very important at the start of the hiring process, especially for younger people. Recruiters put up short, well-made videos that show pictures of how the workers have easy, good working conditions without any qualifications. If someone comments or messages on the posts, recruiters tell them in private chats that they don't need any experience: only basic skills are needed, and they will get training. To make the offer seem more real, other people join the conversation and pretend to be workers who say they have already benefited. TikTok’s visuals get people’s attention. Victims are often offered loans or help with travel, which turn into debts that keep them stuck in the system once they get there.

Viber

Viber is more personal, and recruiters often use it to get in touch with people directly and in a friendly way. They send private messages that look like real offers and sometimes name people that both sides know to build trust. The recruiter then gives the job seeker fake job descriptions, contracts or salary tables that look real. On Viber, grooming is usually done one-on-one, with recruiters spending a lot of time talking to and calming the person down. In some cases, small groups are formed where workers talk about their “positive experiences.” The victim feels like the recruiter is looking out for them because of this personal touch. Once the person is sure, they are told how to get there and who to meet along the way. When they do what they’re told, they are taken to compounds where they lose their freedom.

Even though the platforms are used in different ways, the overall process of hiring people is generally the same. It usually starts with first contact, which can be a public job post on Facebook or TikTok, or a private message on Telegram or Viber. Finally, when they get to their destination, their papers are taken, and they are kept in scam compounds where they have to work under threat of violence, debt, and punishment.

In every case, the process starts with hope and ends with force. Facebook and TikTok are good for getting the word out and reaching a lot of people. Telegram and Viber are better for getting people to do what you want and for planning. They work together to make a recruitment system that takes advantage of people's weaknesses, making the lies stronger and harder to resist.

Target demographics and vulnerability factors

Cyber scam networks go after people who are financially or socially weak on purpose, typically going after demographics who are most likely to be interested in quick ways to make money. Young adults, usually between the ages of 18 and 30, are a primary target because they are adaptable, know how to use technology and often don't have sufficient employment opportunities. These people are particularly prone to respond to offers that promise them financial freedom or quick career advancement.

Internally displaced people and ethnic minorities from Myanmar's conflict-affected areas, such as Shan, Kachin, Kayin are also very vulnerable. Ongoing conflict, loss of farming jobs and weak government in these areas make it easy for exploitation to happen. A lot of scam compounds are in border towns where the government doesn't have much control. Therefore, this makes these communities very vulnerable.

Another important group of people to target are unemployed workers and migrants from countries like Bangladesh, Pakistan, Sri Lanka, African countries, the Philippines and Vietnam. Many of them are already on the move and looking for job opportunities or a new place to live. Recruiters use networks of migrants and people from the overseas community to get people to join scam operations.

Cyber scam networks take advantage of people who are poor, socially isolated, or displaced. These groups are especially vulnerable because of a mix of structural factors that make it easy for people to take advantage of them. People who are having a hard time making ends meet are very interested in well-paying remote jobs because of economic shocks like rural poverty, falling farm incomes, and a lack of jobs in cities. In places where there is a lot of conflict and the governing structure is failing or under the thumb of armed groups, scam compounds can run without much oversight, making them safe havens for criminals. Because so many people use social media, recruiters can use sites like TikTok, Facebook, Telegram, WhatsApp and dating apps to trick people by using fake testimonials, polished ads, and fake identities. Corruption and collusion among local officials make it easier for these operations to keep going without being stopped. Cross-border smuggling networks also make it easy to move vulnerable people into scam hubs. These vulnerability factors make it easier for recruiters to trick people into working for them in ways that are harmful to them, and they don't have many options for getting away or protecting themselves.

Role assignments and operational structure

Upon arrival at scam compounds, scammers confiscate victims' identity cards, passports, and phones. The victims are immediately assigned roles based on their language proficiency, typing speed, appearance and communication skills. The compounds function as industrial-scale fraud operations, with a rigid hierarchy and division of labour, all enforced under coercion and constant surveillance.

Three major teams drive the scam operations:

- **Finding team (M1):** This group is tasked with identifying potential victims through platforms like TikTok. In one room, as many as 50 to 200 people are assigned this work, each operating up to 10 smartphones simultaneously. They are instructed to target by country, focusing on specific regions where people are likely to have money or appear emotionally vulnerable. Each "finder" uses keywords, hashtags and location tags to locate profiles that could be exploited. Once suitable targets are identified, their profiles are forwarded to the chatting team. A technical expert in the room manages the internal servers and devices, ensuring stable internet, secure routing and mass device operations.
- **Chatting team (M2):** These workers take over communication with the selected targets. Using scripted storylines tailored to each target's background—such as romantic interest, investment advice, or business proposals—as they engage in daily conversations. The scripts are regularly updated and adjusted based on responses. Workers type in their native language, which is then automatically translated into the target's language, allowing real-time multilingual communication.
- **Killing team (M3):** The "killer" team is the scamming operation's backbone. They make sure money keeps coming in by enforcing quotas and debts, threatening or punishing anyone who doesn't comply and keeping an eye on where payments are made. They are held responsible to get the targeted amount of money from the fraud victims.

Once contact is established by the finding team, chatting staff are assigned to pursue and manipulate the target continuously until they meet the assigned financial quota. If the chatting person cannot get the targeted money, the case is moved to the killing team, and they continue to threaten victims to force them to transfer money. This may take days or even weeks, and targets are not dropped until a successful extraction of money or data is made. If the chatting staff fail to meet the quota, they face threats, abuse or financial penalties.

Abuse, punishment and gendered violence

Inside the compound, workers are subjected to extreme control. Work shifts can last 18 to 20 hours per day, and personal phones are confiscated. If workers want to use their phones, they must pay 5,000 MMK (1.2 USD) per hour. Surveillance cameras and guards are everywhere. The entire setup is engineered to maximize profits while silencing dissent, limiting outside communication and preventing escape.

Scams along the Thai-Myanmar border are not just violent and manipulative in a random way. Violence is built into the system. People who don't meet their quotas or show any sign of resistance are often punished in very harsh ways, such as electric shocks, beatings, lack of sleep, and being forced to stand for long periods of time. These methods are meant to weaken both your physical and mental strength. People are often beaten or made fun of in public as a warning and to stop them from disobeying again.

People who have been scam workers say that severe physical abuse and torture are common ways of keeping them in line. One survivor said that for months, they were shocked every day with electric probes. Another was tied to a pole, beaten and sold to another compound because they didn't meet performance expectations *(The Guardian, 2025)*. These stories show that violence is a regular and routine method of keeping people in line.

A media story mentioned the case of Abdul Manan, a 20-year-old from Pakistan, who vanished after his journey to Thailand in December 2024. His family subsequently discovered that he was detained in KK Park, a large fraud compound under the jurisdiction of the Border Guard Force (aligned with the military regime). A Chinese trafficker reached out to the family with a ransom demand of USD 15,000, significantly exceeding their financial capacity. In message conversations, Abdul revealed severe penalties, encompassing everyday assaults and torture via electric shocks. He said he lived under perpetual danger in hazardous circumstances. His example illustrates the plight of victims enduring both coerced work and systematic maltreatment, while their family remain unable to effectuate their liberation (Mizimma, 2025).

Women are at even greater risk because they are exploited in two ways. In addition to the usual punishments that all workers face, women are at risk of sexual harassment, coercive sexual relationships, and rape. Gender-based violence is used intentionally to keep women in line. Threatening to traffic women into brothels or forcing them into sexual exploitation roles like sextortion are ways to make sure people follow the rules at work and keep a culture of fear inside the compounds.

A letter from the family of a Philippine victim shared with a journalist shows how bad this abuse was and how it could have killed them:

> *"In November, my sister was recruited to work in Thailand as a call-centre agent but forcibly brought to Myanmar. We hadn't heard from her until this January. We received a message from a dummy account that my sister used to contact us, and she's begging to be rescued. They are not allowed to contact anyone, even family members, and she must do it secretly and carefully because she will receive punishment once caught.*
>
> *They confiscated her phone and passport, and she was not allowed to leave the compound. There are other Filipinos trapped in the compound. They are being forced to work as scammers, 18 hours a day, with limited food. They are also being physically abused, especially if they don't meet their assigned quota. They receive punishment like paddling and electrocution. We have already reported everything to the Philippines embassies in Bangkok and Yangon, but sadly they said that the area is not accessible. They tried to coordinate with the local authorities, but until now, there's no clear update if there will be a rescue.*
>
> *Recently, we found out that she is pregnant, and the Chinese are trying to terminate it. They injected her with medicine that can cause a miscarriage and now she feels dizzy, has blood spotting, constant abdominal pains and swollen breasts and private parts. And they are refusing to provide medical help. I'm very worried about her health and life. She is being yelled at every time she needs to go to the restroom to pee, she is not allowed to use the restroom, and it looks like this is affecting her condition."*

This letter makes it clear how dangerous these operations are for women and men. The system goes beyond economic exploitation to completely control the lives and bodies of victims by denying them medical care, forcing them to take drugs to end their pregnancies, limiting their basic bodily functions, and always threatening sexual violence. Women are not just workers in the scam machine; they are also hostages whose health, dignity, and lives are always in danger.

Internal recruitment among Myanmar nationals

Foreign victims who are trafficked from places like the Philippines, Vietnam, Bangladesh, Pakistan, or Ethiopia often experience extreme violence and torture. Myanmar nationals tend to experience less physical abuse in some of the scam compounds run by the Border Guard Force and the Democratic Karen Buddhist Army. However, according to one of the interviewee investigative journalist's responses, there are some cases of Myanmar nationals also suffering violence and sexual assaults in some of the scam compounds. The difference in experiences may be related to the specific scam group and their relationship with local armed groups, especially the Border Guard Force under the military junta, which informally runs many of these areas. The armed groups can influence how the scammers treat people, because the scammers rely on them for controlling territory and protecting businesses. Their goal is to keep things calm and give the impression that things are in order.

But this somewhat 'softer' treatment has caused a troubling trend. Many people in Myanmar, especially in areas with low incomes and a lot of fighting, think that these jobs are safer for locals and might be a good way to make money. This idea has led to a pattern of voluntary recruitment, thanks to social media posts that talk about high salaries and low risks, as well as word-of-mouth reports in communities. This so-called voluntariness, however, is influenced by profound structural weaknesses, including pervasive unemployment, forced conscription, political oppression, and a deteriorating education system.

One respondent said: ***"We have only two options—struggle in the country which has no future for us, or make more money with this kind of work for our survival. Even if we don't do it, other people will."*** This statement shows a resigned rationalization that comes from desperation, not real agreement. For many, going into scam compounds is less of a choice than a way to stay alive in a world that is increasingly dangerous and there aren't many other options.

But life inside these compounds is still hard. Some workers in Myanmar are not subjected to the most extreme forms of violence, but they still have to work long hours, often up to 20 hours a day, and are constantly watched on digital devices. They are also isolated and under a lot of mental stress. They can't leave the compound and are threatened with fake debts. In this way, Myanmar citizens are also stuck in systems that take advantage of them, but the stories they tell are different from those of foreign victims. Their stories show that coercion in forced labour goes beyond physical violence. It also includes structural and economic pressures that keep people in harmful work even when they seem to agree to it.

Organized crime networks and structural impunity

Scams along the Thai-Myanmar border are not just isolated crimes; they are part of a large, well-organized network that thrives on legal impunity and deep-rooted corruption. These networks are very well-organized, operate like industries with a hierarchy, specialized teams, and cross-border financial channels that make it easy to commit fraud and launder money on a large scale. The compounds are not hidden or in remote areas. They are often large, fortified complexes that employ thousands of people in forced labour. They are clearly visible in border towns, and state authorities don't really interfere with them.

One of the main reasons they are so strong is that organized crime groups work with local leaders. The Border Guard Forces (BGF) under the command of the Myanmar State Administration Council (SAC), along with other armed groups in these areas, are a key part of making scam operations possible. In exchange for bribes or direct profit-sharing deals, they offer territorial control, logistical support, and protection. This protection lets the compounds work openly, and checkpoints and militia-controlled areas are less like walls that keep crime out and more like shields that protect it.

Corruption and bureaucratic inertia make impunity even worse. Thai or Chinese authorities sometimes raid or crack down on compounds, but these actions are usually very selective and symbolic. Arrests are often only made of low-level recruiters, drivers, or forced compound workers, who are then shown in the news as proof that the police are doing something. The financiers, political backers and military-linked masterminds who run these networks, on the other hand, are still free. This imbalance not only fails to break down the core structures, but it also keeps a cycle going where people who are not needed are punished while the leaders benefit from ongoing protection.

Sometimes, state-led interventions make things worse for civilians instead of stopping criminal activities. Blockades at the border, trade restrictions, and embargoes often stop humanitarian aid and basic goods from getting to nearby communities. The scam compounds, on the other hand, adapt by creating their own supply chains. They are still protected from outside shocks because they grow their own food, make their own medical supplies, and have their own smuggling routes. This shows how deeply they are connected to the regional political economy.

These dynamics show that scams aren’t just crimes; they’re also signs of a failure in governance and political involvement. When organized crime, armed groups and corrupt officials come together, it makes it almost impossible to break up these groups without also changing the larger political and economic systems that keep them going. In this situation, victims are stuck not only by physical barriers inside compounds, but also by an international system that has so far been unable or unwilling to deal with the deep-seated complicity that protects these networks.

Escape, resistance and survivor experiences

As soon as victims are brought into scam compounds, the systems that keep them in line start to work. Signing what looks like a real work contract is usually the first step to getting in. These contracts usually last for one or two years. These contracts make people think they are legal, but they are really tools of coercion. As soon as they sign, victims lose their freedom: their phones, passports and national ID cards are taken away, cutting them off from the outside world and taking away their ability to move freely.

It's almost impossible to try to resign. The operators tell the victims they must pay three times what they promised to leave, and the amounts are different for each person and set by the operators. Wages are heavily manipulated, even when they are still in the compound. Deductions often lower or even eliminate salaries, and this is often done by saying that the employee didn't meet their daily or monthly quotas or by charging them too much for food, lodging or made-up disciplinary fines. For a lot of people, this leads to a cycle of debt bondage where they make little to no money, which keeps them stuck. Survivor accounts collected by advocacy groups show that some victims never got paid while they were being held, and others only got small amounts that were much less than promised.

Under these circumstances, getting away is very hard. Armed guards, tall fences and compounds that are hard to get to are all physical barriers. The threat of violent punishment stops most attempts. People who try to escape face harsh punishments like beatings, electric shocks, or public humiliation. These punishments are meant to scare others into following the rules. A few victims have been able to get away by paying off guards, taking advantage of times when guards weren't paying attention, or with the help of humanitarian networks. But life after escaping is still hard for those who do make it.

Survivors frequently report enduring psychological trauma, encompassing anxiety, depression, nightmares, and manifestations of post-traumatic stress. Reintegration into their communities is also difficult because of mistrust or stigma. Some neighbors see them as criminals instead of victims of trafficking. Financial difficulties make this social isolation worse because survivors often have debts that traffickers made up, which makes them more likely to be trafficked again or exploited again. It is almost impossible to get health care, legal help, or even basic social services without a passport or ID. Many survivors are afraid to go to the police because they think they will get in trouble or because they think local officials are corrupt or involved in the trafficking networks.

Survivors and their families' stories make these truths even clearer. In an *Al Jazeera* documentary, a young man said he had to work up to twenty hours a day and that anyone who slowed down was beaten or shocked with electricity. Another survivor said that women were threatened with being sold to brothels if they didn't meet their financial goals. This shows how gender-based violence is used to control operations. Families of the victims have also begged for help. In one case, the family of a pregnant woman said that she had been forcibly injected with drugs meant to cause a miscarriage, denied medical care even though she was in a lot of pain and bleeding, and humiliated for asking to use the bathroom. These testimonies show not only the physical and mental abuse that happens in these compounds, but also the gender-based weaknesses that exist there.

Even though these conditions are terrible, survivor accounts are still very important for learning how scam operations work. They show how work is divided into tasks like recruiting, talking to targets, and collecting debts. They also show how local militias, brokers, and criminal groups work together to keep the trade going. Survivors also stress the importance of finding long-term solutions after being rescued. They always ask for ongoing mental health and psychosocial support, safe housing, help with the law to get back lost documents, and job training that can give them real economic options. To help survivors rebuild their lives and break the cycle of exploitation that keeps scam operations going along the border, it is important to meet all their needs.

Survivor testimony: Mya Mya (alias)

"I'm Mya Mya from Myanmar. Four months ago, I quit my job as a scammer and now work as a maid in Thailand. An agent hired me and promised me a high salary, but they took me to a scam compound. Before I could start working, I had to go through ten days of computer typing training and sign a six-month work contract. I figured out that the job was a scam after four days of talking to customers.” This shows how agents take advantage of people’s financial problems and the promise of high pay to force them to do illegal things, while initial training and contracts make it look like they are doing the right thing.

“We worked 18–20 hours a day. We began by looking for possible victims on TikTok, Telegram, and Facebook. Once we had a connection, we moved the talks to WhatsApp. To hide where we were, we mostly used SIM cards from Thailand, Laos, or Cambodia. We had to be nice, stick to the scripts, and get people to send us money. The main countries to target for our group were Russia, Turkey, Iraq, and the UAE.” This shows that social media sites are often used for cross-border scams that use digital manipulation, building trust, and hiding the location of victims to reach people in other countries.

The scam was pretending to run a business. “We showed victims fake slips to make them think they had gotten money, and then we got them to send money. We blocked the victims after we got the money. It was thought that each victim would lose about $7,000. The transfers and exchanges were made through the **OKX platform**, which used the victims’ country codes and ID numbers. The main way to talk to each other was through WhatsApp.” This shows how cryptocurrency platforms are used in international scams and how scammers use private messaging and digital money laundering to steal from a lot of people at once.

“I felt guilty about scamming people, even though I made more money than I would have at a regular job, which is why I quit.” This personal reflection highlights the psychological and moral burden endured by workers compelled to participate in these operations, as well as the possibility of voluntary departure when ethical boundaries are transgressed.

Gaps in prevention, protection and policy

Even though more people around the world are becoming aware of cyber scams in Southeast Asia, institutions are still not doing enough to stop them. Social media sites, which are very important for recruitment, don’t have strict rules for job postings, especially those that target people in low-income or conflict-affected areas. Content moderation in languages other than English is often poor, which lets false recruitment messages spread quickly and without any checks (Global Initiative, 2025). Platforms have also been slow to respond to reports of coordinated abuse, which has left networks that take advantage of people mostly unchallenged online.

The government responses haven't been good enough either. There isn't much coordination between Southeast Asian countries, and corruption in local police departments makes it harder to enforce laws and investigate crimes. Attempts at rescue by foreign embassies in Myanmar and Thailand are limited, largely symbolic, and far from sufficient given the scale of the problem. Many victims were told to contact their countries' embassies for help, only to be ignored or turned away, or even get exploited in their situations. Support systems for survivors such as shelters, legal aid, or trauma counseling are often underfunded or entirely absent (Ghoshal & Wongcha-um, 2025; Wu, Saksornchai, & Mendoza, 2025). For example, after being relocated to makeshift refugee camps alongside the Thai-Myanmar border, many rescued Vietnamese nationals reached out to the Vietnam embassy in Thailand for emergency repatriation, only to be asked to pay hundreds of dollars in bribes for a flight home (Truong, 2025). Data collection and documentation are also severely lacking, particularly in local dialects and rural areas where most victims come from. These systemic gaps allow exploitation to continue unchecked and make it extremely difficult to hold perpetrators accountable or provide meaningful support to survivors.

Scammers often get help from local elites and security forces. They use global money laundering networks, like cryptocurrencies and high-risk financial services providers (Global Initiative, 2025). These kinds of systemic problems make it harder to intervene effectively and keep the cycle of exploitation going.

Scam operations have shown amazing flexibility, spreading across Southeast Asia and moving to different mobile and online platforms to find new victims. Along with technological advancement, scammers are using increasingly advanced AI tools to improve their strategies. They use AI to automate communication, create fake content, fake financial documents and expand their scams around the world. According to the Democratic Voice of Burma, AI is now widely used in Myanmar scam centres, making it easier for criminals to find victims and run their businesses more efficiently. This makes it harder to regulate and stop scams (The Democratic Voice of Burma, 2025).

Support systems for survivors are still insufficient. There aren't enough shelters, legal aid, or trauma counseling services for victims to get the help they need to start over. There is a lack of effort to collect and record data, especially in local dialects or among people who live in rural areas, where most of the victims come from. This lack of information makes it harder to hold those responsible accountable and give survivors real help (United Nations Office on Drugs and Crime, 2025).

These findings show that there is a deeply rooted and complex system of exploitation that is caused by digital manipulation, instability in certain areas, and failures of institutions. To solve the crisis, we need to take a big-picture approach that includes digital regulation, cooperation between law enforcement agencies in different countries, support for survivors, and campaigns to raise awareness at the community level.

Discussion

This study contextualizes forced labour in scam operations within a framework of digital exploitation, global trafficking, and the dynamics of war economies. Social media channels are essential for recruitment, allowing offenders to access susceptible groups internationally with little to no expense or regulation. The system's efficiency is enhanced by the algorithmic promotion of misleading information, especially on TikTok and Facebook, where employment scams can proliferate rapidly.

These operations are supported by a convergence of facilitating factors: geopolitical instability, the disintegration of official authority in certain regions of Myanmar, and economic desperation among displaced individuals. The differentiation between coerced and voluntary engagement is frequently blurry in this type of situation. The existence of a hierarchy within scam organizations, along with varied treatment based on race and national origin, indicates both systemic prejudice and strategic choices by scam operators aiming to reduce risk and enhance profits.

The results highlight the deficiencies of existing enforcement strategies, which frequently lack cooperation and do not tackle the underlying reasons of exploitation. In the absence of enduring political commitment, intergovernmental collaboration, and platform accountability, any intervention is prone to being inadequate. The lack of survivor-centered measures, including trauma-informed care, legal recourse, and reintegration assistance, intensifies the vulnerability of individuals who have escaped.

Recommendations

A multi-layered and coordinated strategy is needed to deal with the complicated problem of forced labour in cyber scam operations. First, the companies behind TikTok, Facebook and WhatsApp need to be responsible for the content on their digital platforms. These businesses should improve their moderation systems so they can find and delete posts that try to recruit vulnerable people for spurious employment opportunities. When technology companies, civil society groups, and governments work together, they can help create automated systems that flag job postings that seem suspicious, especially those that offer unusually high salaries for vague or unspecified digital roles.

Second, formal government institutions of affected countries should be more proactive and take concrete actions toward preventing scams and human trafficking, alongside cross-border cooperation among Southeast Asian nations, particularly Thailand, Myanmar and China. Past law enforcement efforts have often fallen short due to corruption, lack of transparency, and the entrenched influence of criminal networks, while most rescue, documentation, relocation, and repatriation efforts have so far been initiated by non-state actors like NGOs, humanitarian organizations and voluntary individuals (Kelliher & Mureithi, 2025). Bilateral and regional agreements should be pursued to facilitate transparent investigations, create joint task forces, and ensure the prosecution of both recruiters and compound operators. Special attention should be given to dismantling the financial networks that allow these operations to thrive.

Third, targeted prevention campaigns need to be launched and spread in many languages in high-risk areas. These campaigns should try to make more people aware of how recruiters work, especially for people between the ages of 18 and 30. Digital literacy programs should also be a part of community outreach, schools, and vocational training centers to help young people spot and report job offers that seem too good to be true.

Fourth, protecting and helping survivors should be the most important thing. International donors and humanitarian groups should give money to help victims with shelters, trauma-informed counseling, and legal aid. Survivors must also play a role in shaping policies and programs so that their experiences are taken into account when making decisions. At the same time, police must make it safe for victims to report crimes and protect witnesses to get them to come forward without fear of being hurt.

Fifth, ongoing collaborative research is essential due to the rapidly changing nature of cyber scam operations, which are marked by decentralized structures, digital sophistication, and fluidity across borders. These operations are not fixed; they change quickly, spread widely across platforms and regions, and work a lot like a viral network. Without ongoing examination of their internal workflows, financial systems, and transnational facilitators, initiatives to combat them will persist as reactive and disjointed. Future research ought to concentrate on delineating operational hierarchies within compounds, scrutinizing cryptocurrency flows, and chronicling survivor routes to escape. We need to know more about these highly adaptable networks to come up with better ways to stop, disrupt, and help survivors get better.

Lastly, there is an urgent need for independent oversight and record-keeping of these operations. Local NGOs and investigative journalists are very important for finding out about abuses and speaking up for victims. Instead of getting in the way of these people, governments and international organizations should protect and work with them.

By following these suggestions, stakeholders can start to break down the system of exploitation that keeps cyber scams going along the Myanmar-Thailand border. This transnational human rights crisis can only be effectively addressed through sustained, collaborative, and survivor-centred action.

Conclusion

Social media is fueling modern slavery. People are using platforms like TikTok, Facebook, WhatsApp and Telegram to trick young adults, migrants, and people who have been forced to leave their homes into cyber scams along the Myanmar-Thailand border. What starts out as a job offer online quickly turns into forced labour, abuse, and coercion in heavily guarded scam compounds.

These platforms amplify deception. Fake job ads, fake testimonials, and polished recruitment content make things look real. Once inside, victims must work long hours under surveillance and are abused, particularly women. Even local recruits who think the job is safer are stuck because of structural pressures and digital manipulation.

It is crucial that something be done urgently to stop the exploitation that social media makes possible. Companies that run platforms like TikTok, Facebook, WhatsApp, and Telegram should be held responsible for content that targets vulnerable groups with false recruitment methods. Governments, regional authorities, and local stakeholders must work together to break up criminal networks, uphold the law, and keep people safe. Survivors need a lot of help, such as safe housing, legal protection, trauma-informed care, and long-term job prospects that will help them get their life back on track.

Online recruitment tactics are a serious threat to communities and young job seekers. Job offers that look good on social media can be hiding pressure and forced labor. Public awareness, preventive initiatives, and survivor-centered aid must all be part of effective solutions. Social media will continue to be a powerful tool for forced labour operations, allowing exploitation to continue across Southeast Asia and beyond, unless concerted and long-term actions are taken.

Limiting the operations of cyber scam networks would be greatly enhanced if recruitment through social media could be successfully discouraged and curtailed. By eliminating the recruitment vector that most of these frauds use—social media—we can protect victims from forced labour and financial exploitation. To prevent the exploitation of vulnerable groups, it is possible to disrupt these operations at their source by targeted interventions on digital platforms, awareness campaigns, and regulatory control.

References

Democratic Voice of Burma. (2025, September 16). *Scam centers in Myanmar use AI tools*. https://www.dvb.no/post/724461

Ghoshal, D., & Wongcha-um, P. (2025, February 28). Some foreigners pulled out of Myanmar scam centres face struggle to get home. *Reuters*. https://www.reuters.com/world/asia-pacific/some-foreigners-pulled-out-myanmar-scam-centres-face-struggle-get-home-2025-02-28/

Global Initiative Against Transnational Organized Crime. (2025, May 29). *Cyber scam operations in Southeast Asia are a type of compound crime*. https://globalinitiative.net/analysis/compound-crime-cyber-scam-operations-in-southeast-asia/

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

Mizzima News. (2025, June 6). Chinese mafia demanded ransom from the family of a trafficked Pakistani national. https://bur.mizzima.com/2025/06/09/58220

The Guardian. (2025, February 25). Beatings, torture and electric shocks: Freed scam compound workers allege horrific abuse. *The Guardian*. https://www.theguardian.com/world/2025/feb/25/beatings-torture-and-electric-shocks-freed-scam-compound-workers-allege-horrific-abuse

UN Office on Drugs and Crime. (2025, April). *Inflection point: The global effects of scam centers, cyber-enabled fraud, and human trafficking*. https://www.unodc.org/roseap/uploads/documents/Publications/2025/Inflection_Point_2025.pdf

Wu, H., Saksornchai, J., & Mendoza, M. (2025, March 9). They were forced to scam others worldwide. Now thousands are detained on the Myanmar border. *AP News*. https://apnews.com/article/myanmar-thailand-scam-centers-trapped-humanitarian-c1cab4785e14f07859ed59c821a72bd2

Ying. (2023, August 15). Between survival and betrayal. *Mekong Review*. https://mekongreview.com/between-survival-and-betrayal