Human Trafficking and Cyber Scam Operations

All over the world, we are still unraveling the complex and multifaceted ways in which traffickers—from individual criminals to heavily resourced crime syndicates—adapted to and thrived during the COVID-19 pandemic. We know the sudden interruption of migration dynamics, bans on public gatherings, the closure of entertainment establishments, and the cessation of entire industries, stalled human trafficking operations in some countries. In other places, however, traffickers pivoted to take advantage of these changes by shifting their strategies and leveraging pandemic-related economic hardships, increased global youth unemployment and international travel restrictions to exploit thousands of adults and children in a trend that has grown into a multi-billion dollar industry over the last two years: forced criminality in cyber scam operations.

Casinos and shell companies operating in unused hotels and other rented and bespoke commercial spaces have become hotspots for this growing criminal activity—especially within remote special economic zones, border towns, and other jurisdictionally complex geographic areas known for human rights impunity and minimal law enforcement penetration. Fearing significant downturns in revenue stemming from pandemic-related restrictions, and witnessing widespread unemployment during the pandemic, traffickers in Burma, Cambodia, Laos, Malaysia, the Philippines, Ghana, and Türkiye—including some with connections to the People's Republic of China (PRC)—saw an opportunity. They used fake job listings to recruit adults and children from dozens of countries, including Angola, Bangladesh, Brazil, Burundi, Cambodia, Eritrea, Ethiopia, Hong Kong, India, Indonesia, Japan, Kazakhstan, Kenya, Laos, Malawi, Malaysia, Mongolia, Nigeria, Pakistan, the PRC, the Philippines, Russia, Senegal, Singapore, South Africa, Sri Lanka, Taiwan, Tajikistan, Thailand, Türkiye, Uganda, the United Kingdom, the United States, Uzbekistan, and Vietnam.

Rather than fulfilling their advertised employment promises, many of these companies began forcing the recruits to run internet scams directed at international targets and subjecting them to a wide range of abuses and violations—including withheld travel and identity documentation; imposition of arbitrary debt; restricted access to food, water, medicine, communication, and movement; and threats, beatings, and electric shocks. The scam operations include quota-based fraudulent sales; illegal online gambling and investment schemes; and romance scams, in which the victim is forced to enter into a fake online relationship with and extract money from unsuspecting targets. Traffickers force the victims to work up to 15 hours a day and, in some cases, "resell" the victims to other scam operations or subject them to sex trafficking if they do not agree to fraudulently recruit additional members, or if the victims do not meet impossibly high revenue quotas. Pandemic-related travel bans have been used as excuses to keep victims captive under the guise of adherence to public health measures. There are even reports of casino-based cyber scam operators brutally murdering workers who try to escape.

Civil society groups worldwide have documented thousands of cases in recent years, with more than 10,000 estimated victims remaining in exploitation in individual compounds in Cambodia alone. In one case, an unemployed 26-year-old woman from the Philippines responded to a Facebook post offering call center jobs to English speakers. Several months pregnant and hoping to earn money before having her baby, she traveled to Cambodia to begin work, only to be flown to a shuttered hotel casino in Sihanoukville and locked in a cell without food or water for days. Her captors detained and abused her for months, forcing her to create fake profiles on dating apps and other social media platforms to lure people into fraudulent cryptocurrency and other investment schemes under impossible sales quotas. She managed to escape but, tragically, not before the loss of her unborn child.

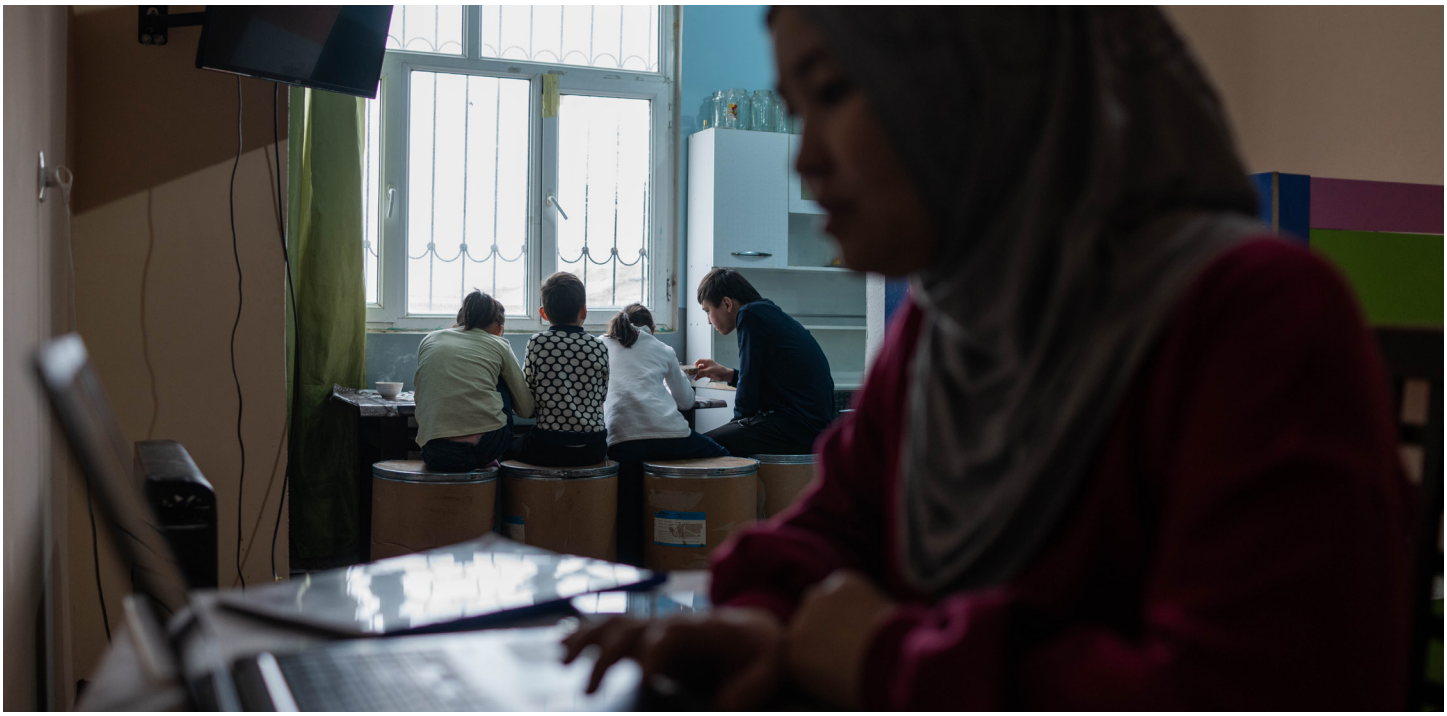

Photo Credit: Winrock International

NGOs have received an overwhelming amount of outreach via social media with similar stories; and many have decried a lack of global resources, capacity, or political will to begin to make a dent in the problem. The cyber scam industry often preys on older individuals with highly technical educational backgrounds—a demographic most authorities are unaccustomed to monitoring for trafficking vulnerabilities. Families desperate to be reunited with loved ones have turned to local authorities or made impassioned appeals to members of nearby diplomatic missions, only to be ignored or turned away. Survivors who escape with their lives are often met with administrative or criminal charges for immigration violations at home or in the countries to which they fled, rather than being identified as trafficking victims and having a chance to benefit from protection services. Many also owe large recruitment fees to locally based recruiters, exacerbating their vulnerability to threats, exploitative debt, and re-trafficking when they return home. Watchdog organizations have traced beneficial ownership directly to high-level officials in some countries.

Although this landscape is bleak, some countries have begun to mobilize resources and strategies to locate their citizens, remove them from their exploitative circumstances, and even initiate accountability processes, despite the aforementioned dangers and jurisdictional complexities. In 2022, Taiwan located and repatriated hundreds of individuals from cyber scam operations in Cambodia and indicted dozens of Taiwanese individuals allegedly complicit in their initial recruitment. In 2021, Laos began cooperating with international authorities to recover Lao victims from the Golden Triangle Special Economic Zone in Bokeo and, despite access challenges and the pervasive impediment of local official corruption, initiated investigations into labor trafficking allegations.

Governments hoping to address this growing trafficking problem should strive to increase awareness-raising among vulnerable communities, including through information campaigns, pre-departure trainings, and enhanced screenings to detect vague, abusive, or missing contract provisions for those migrating for work abroad. They should also collect and share with the public, law enforcement, and international partners information on known fraudulent recruitment channels. In turn, judicial authorities should prioritize the investigation, prosecution, conviction, sentencing, and incarceration of recruiters, brokers, and casino owners and operators knowingly perpetrating forced criminality in online cyber scam operations. Stakeholder ministries must train their diplomats, law enforcement officers, and border and judicial officials on how to detect and assist in these cases domestically and abroad to ensure victims are identified and provided access to robust protection services, rather than penalized solely for crimes they committed as a direct result of being trafficked. Civil society groups have also pointed

to an urgent need for

capacity building among social workers to absorb a fast-growing case load of profoundly traumatized survivors, who will need advanced reintegrative support as they return to their home communities. Finally, as no government can do this work alone, governments around the world must foster, cooperate with, and enhance their support to a free and healthy civil society, rather than restricting space for NGOs and complicating their ability to benefit from international donor activity. With these steps, countries can build deterrent power while better assisting their citizens in the search for safe employment prospects through safe migration channels and regular labor pathways—thereby constructing a preventative architecture around key vulnerabilities that cyber scammers are eagerly exploiting in the wake of the pandemic.

https://www.state.gov/reports/2023-trafficking-inpersons-report/