

United States Institute of Peace

"Examining the 2024 Annual Trafficking in Persons Report: Progress over Politics"

Testimony before the U.S. House Committee on Foreign Affairs

Subcommittee on Global Health, Global Human Rights and International Organizations

Jason Tower, Myanmar Country Director, Asia Center United States Institute of Peace July 9, 2024 Chairman Smith, Ranking Member Wild, distinguished committee members, thank you for providing me with the opportunity to speak to: (1) the growing threat that forced labor scamming in Southeast Asia presents to the national security of the United States, (2) on what has been done until present to counter this growing global crisis, (3) on how this pertains to the recently launched Trafficking in Persons Report, and (4) on why the U.S. needs to advance a whole of government approach to addressing the rising threat stemming from Chinese origin crime groups operating sophisticated scam operations in Southeast Asia. Since early 2022, these criminal groups have targeted a global population with a scourge of online scamming based out of industrial scale scam compounds or "fraud factories" located in Cambodia, Laos and Myanmar. A USIP expert group concluded that as of the end of 2023, these criminal actors steal an astonishing 64 billion US dollars per year, including over 3.5 billion U.S. dollars from Americans. Equally concerning, the criminal syndicates have trafficked people from 66 countries into scam compounds, where they are forced to work as scammers and subjected to torture.

Before going deeper into these issues, please allow me to introduce myself. Since late 2019, I have served as the Myanmar Country Director in the Asia Center at the United States Institute of Peace, and since 2022, I have also served as director of a USIP program on Transnational Crime and Security in Southeast Asia. I have over 20 years of experience working on peace, security, and transnational crime in Asia, and since 2019 have focused much of my research and analysis on the growing influence of Chinese origin crime groups in the region.

For the past 40 years, USIP has worked to prevent armed conflict, support peace, and support U.S. national security interests around the world. As part of its work in Asia, USIP has supported peace and democracy in Myanmar, including through efforts to counter the growing influence of criminal groups which have become a key driver of the country's internal conflict; and by working to hold the military regime accountable for its direct involvement in protecting, supporting and even operating criminal enterprises as a means of generating financing for its ongoing war against the Myanmar people since the February 2021 military coup. USIP has also supported initiatives across the region and in the United States to raise awareness of the growing threats that transnational crime presents to peace, security, democracy and governance, and supported efforts of law enforcement and decision makers to map criminal actors, identify perpetrators, and strengthen local, regional and international responses. My presentation today will draw heavily on the final report of a senior study group on transnational crime in Southeast Asia which I co-authored, and which

was published by the Institute in May of 2024 with the support of the State Department's Bureau of International Narcotics and Law Enforcement Affairs.¹

Introduction

Over the past two decades, Chinese-origin transnational crime groups have become deeply embedded across Southeast Asia, establishing a web of influence and control over regional elites that enables them to perpetrate a wide range of crimes with impunity. While initially these criminal actors focused on illegal and unregulated online gambling operations targeting nationals of the People's Republic of China, by 2018, they increasingly engaged in cybercrimes, including online fraud and scams. On the eve of the pandemic, it was estimated that more than 500,000 PRC nationals were working for these criminal organizations, which were tapping into a 40 – 80 billion dollar per year market for online gambling in China – which is illegal under Chinese laws.

Throughout the 2010s, the Chinese government not only looked the other way as these transnational organized crime groups grew in power and influence across Southeast Asia, elements of the Chinese Communist Party, the Chinese government and Chinese State-Owned Enterprises directly benefited from the criminal activity. In Myanmar, Chinese State-Owned enterprises accepted hundreds of millions of dollars in contracts from criminal entities to construct crime cities in the country's borderlands; across the region, the criminal networks openly built associations with elements of the PRC government and Communist Party, supporting PRC political and economic initiatives including the Belt and Road Initiative and the Global Security Initiative in exchange for a veneer of legitimacy.²

While Chinese police occasionally cracked down on the criminal groups, often this was done through ad hoc, targeted law enforcement campaigns, which resulted in the criminal groups simply relocating their operations to other countries. From the early 2000s until 2019, the criminal groups spread from an initial focus on the Philippines and Northern Myanmar to Laos, which became a hub by 2009, and later to Cambodia and the Myanmar border with Thailand, which saw a massive upsurge in Chinese origin crime groups by 2017.

China's approach shifted significantly at the outset of the pandemic when it (1) called its nationals back to China as part of its draconian measures to control COVID-19; and (2) it initiated an unprecedented crackdown on scams, fraud and other cybercrimes targeting

¹ <u>Transnational Crime in Southeast Asia: A Growing Threat to Global Peace and Security | United States Institute of Peace (usip.org)</u>

² Myanmar's Casino Cities: The Role of China and Transnational Criminal Networks | United States Institute of Peace (usip.org)

Chinese nationals, including through the banning of crypto-currency and by instituting strict banking controls to prevent overseas financial transfers and capital outflows.

In response, the criminal networks pivoted in a dramatic way – first by rolling out a new and distinct form of sophisticated online scamming called "pig-butchering" that they now use to target a global population; second by trafficking a global population of victims into the scam centers to operate these "pig-butchering" scams. The Chinese crime groups behind these scams, and the regional elites that have aligned with them, have emerged as one of the most powerful organized criminal networks in the world.

What is Pig-Butchering?

Pig-butchering involves establishing a relationship of trust with a target over an online platform, establishing psychological control over this target, and ultimately compelling them to invest everything they own in a fraudulent, online investment platform. These platforms often mirror major trading platforms, conferring the appearance of legitimacy; however, they are fully controlled by the criminal syndicates.

These pig-butchering scams are also distinct in their utilization of forced labor. Criminals are now trafficking a GLOBAL population into compounds designed explicitly for these scam operations. They do this through another scam - the fake job scam, through which they present themselves as a legitimate company, offering employment opportunities with attractive wages and benefits. Survivors report going through several rounds of interviews before receiving an offer, including plane tickets and relocation expenses. On arrival in a transit hub country like Thailand or Vietnam, they are brought across borders into neighboring Cambodia, Laos or Myanmar, and only to realize they have been trafficked when they are told that they cannot leave the compound and that they must work as scammers. Failure to do so results in physical or psychological torture, or in many cases in the victims being sold to other compounds as "cyber-slaves." Numerous witnesses have reported being sold multiple times, and in some cases scam syndicate operators have threatened to sell victims to criminal groups involved in black market organ harvesting. According to our research, the nationals of 66 countries have been trafficked, including a small number of Americans. A 2023 United Nations report found that as many as 220,000 people have been trafficked into forced labor scam syndicates in mainland Southeast Asia.3

Why are Scam Syndicates Using Forced or Trafficked Labor

The use of forced labor distances the scam syndicate operators from the scams, making it more difficult for law enforcement to identify the real perpetrators. At the same time, this

³ ONLINE-SCAM-OPERATIONS-2582023.pdf (ohchr.org)

also presents an additional revenue generating opportunity – the open sales of trafficking victims across compounds and demands that victims either successfully scam to earn their freedom or pay a large ransom. Once in the control of the scam syndicates, it is extremely difficult for victims to regain their freedom. For individuals unwilling or unable to scam, the syndicates eventually gain access to their relatives, and coerce them into paying tens of thousands of dollars in ransom for their release. Family members are often sent videos of relatives being subjected to torture. In some cases, conditions in syndicates are so poor that victims commit suicide; in other cases, they lose their lives attempting to escape, or are killed when the syndicates go too far in subjecting them to torture. Videos of individuals falling out of high-rise scam compounds in Cambodia and Myanmar are now regularly circulated on social media.

Securitized Compounds

While the nature of scam compounds varies across countries, in all cases they rely on a range of security forces to prevent victims from escaping and to keep unwanted visitors from infiltrating the compounds. In the case of Myanmar, the Myanmar army's Border Guard Force in Karen State, which is directly involved in operating some of the country's largest scam syndicates deploys its forces to provide security outside the scam syndicates. In other parts of the country, ethnic armed organizations such as the United Wa State Army are some of the largest providers of security to scam compounds. Inside the compounds, scam syndicates rely on highly trained private Chinese security guards, many of which are ex-People's Liberation Army. Some of the same organized Chinese crime groups that own compounds in Myanmar, Cambodia or Laos also operate large scale security companies in each of these countries, as well as in Thailand. In Cambodia, current or former police are often hired by the scam compounds to provide security; meanwhile in Laos, security guards are often recruited from ethnic armed organizations in Northern Myanmar. The extreme securitization of these compounds represents a growing security challenge to governments and law enforcement across the region. In the case of Laos, the Lao government has largely lost the ability to enter the Golden Triangle Special Economic Zone, which is the location of majority of the country's scam compounds.

The role of social media and advanced financial technology

Victims of both trafficking and the pig-butchering scams are targeted using social media, professional networking or dating platforms such as Messenger, WhatsApp, Tinder, LinkedIn, Tik Tok, WeChat or Jobs.com. Pig-butchering scams often begin with what appears to be a misdirected message over one of these platforms from an account with an attractive profile picture. If successful, this leads to what can be an extended period of courting, until finally the victim is convinced to begin investing in an online platform, often in crypto-currency.

Human trafficking is facilitated over the same platforms, with the scam syndicates most commonly tricking victims into accepting seemingly lucrative jobs. To date, the private sector has failed to identify effective means of preventing this from happening, often claiming that it cannot distinguish between real and fake job opportunities.

Criminals also rely on advanced financial technologies to facilitate financial crimes and launder money. Over the past two decades the Chinese crime groups behind the online gambling and scams have invested heavily in the development of new crypto-exchange platforms and applications and in the development of leading programming and software development firms across Asia that produce a full range of technology solutions used by criminals to scam. Meanwhile, the same technologies are used to launder stolen crypto-currency across the region, with almost every country in ASEAN impacted by a range of new forms of money laundering using crypto-currencies. One of the main reasons why these scams are so difficult to combat is the fact that law enforcement around the world, including in the United States has very limited understanding of these technologies. In particular, very few law enforcement officials know how to trace stolen crypto currency.

How is this harming the United States?

U.S. interests are impacted most directly by the fact that hundreds of thousands of Americans are losing everything to these criminal syndicates. According to U.S. authorities, Americans are now targeted more than any other group in the world. ⁴ This is being accelerated by an aggressive crackdown that the Chinese government has undertaken since 2022 on Chinese scam syndicates targeting Chinese nationals. In May of 2024, the Chinese police reported that they have repatriated nearly 50,000 Chinese nationals out of scam syndicates in Southeast Asia. The result is that the criminals adapt – as China reports a 30% decrease in these scams over the past 8 months, the U.S. reports unprecedented increases.⁵

These trends also undermine years of U.S. investments in countering human trafficking, with these criminal networks now introducing a wide range of unprecedented forms of trafficking. For the first time, Myanmar, Cambodia and Laos are destination countries. According to INTERPOL, anyone anywhere can now become a victim of trafficking, and traffickers are using new technologies, new routes and new methods of accessing victims.⁶

Another threat to the U.S. stems from China's response to these crimes. The Chinese government has framed its response as part of its Global Security Initiative, which aims to challenge global security norms and dramatically increase Chinese security influence

⁴ CI issues red flags, tips to avoid falling victim to pig butchering schemes during International Fraud Awareness Week | Internal Revenue Service (irs.gov)

⁵ China Forces Myanmar Scam Syndicates to Move to Thai Border | United States Institute of Peace (usip.org)

⁶ INTERPOL issues global warning on human trafficking-fueled fraud

overseas. With many countries becoming more desperate to find a solution, China is leveraging this issue to strengthen the influence of its police and its authoritarian form of policing around the globe, threatening U.S. investments in democracy and human rights.

What has been done to counter this crisis?

The short answer is very little. While hundreds of thousands of people in the United States have fallen victim to these scams, we have not been able to indict the perpetrators behind these crimes; meanwhile in most cases, law enforcement cannot recover funds. Awareness raising about pig-butchering scams is minimal, lagging behind the moves of the criminal syndicates to develop new and more sophisticated iterations of the scams. Patterns are similar in other countries, with perhaps Singapore and Taiwan standing out as exceptions.

Meanwhile, the number of trafficking victims has also continued to grow over the past three years, with an additional 20 countries impacted by human trafficking between March 2023 and May 2024. One key reason for this is that the majority of countries have failed to invest in prevention. Airport authorities have done very little to attempt to screen for possible victims; social media and recruitment platforms have failed to issue warnings or remove harmful job advertisements; public announcements and awareness raising campaigns have been limited in most impacted countries; finally, international cooperation on these issues remains weak, as most governments around the world have yet to make this a priority.

Lack of information and limited accessibility presents serious challenges to response efforts. Most countries struggle to obtain information on when and where their nationals are trafficked, and even in cases where they can obtain this information, the response is ad hoc and reactive. In the case of trafficking victims in Myanmar, the illegitimate military regime has deep involvement in the scam business and has neither the capacity nor the political will to help victims. As a result, senior diplomats from victim countries often have no choice but to travel to Thailand to plead with the Thai authorities for assistance in gaining access to compounds across the border in Myanmar. In other cases, senior officials resorted to negotiating directly with the Chinese crime groups or paying ransoms to retrieve victims.

Some countries have started using sanctions as a tool to target criminals, notably the United Kingdom, which sanction 14 individuals and companies for forced labor trafficking in December of 2023. Others have issued arrest warrants targeting perpetrators. While so, coordinated action vis-à-vis sanction or warrants is almost non-existent.

In Southeast Asia, one significant challenge is that a regional response has proven difficult given that Cambodia and Myanmar continue to openly deny that this is a problem,

⁷ UK and allies sanction human rights abusers - GOV.UK (www.gov.uk).

undermining the efforts of ASEAN to mount a collective response. Elsewhere across the world, many multilateral and regional organizations have yet to take action.

The U.S. has played an important role in documenting these developments through the TIP report over the past two years. This offers a baseline for the U.S. to advance work with countries across the world to address various aspects of this problem. While so, human trafficking is only one symptom of a much bigger crisis – the real challenge lies in addressing the power and influence of the transnational criminal groups that are behind this scourge of forced labor scamming.

Policy Options

For the U.S., our SSG report identifies the following recommendations:

- (1) A whole-of-government response, headed by the National Security Council, which establishes an interagency task force to steer the effort both at home, as well as to assert U.S. leadership on this issue internationally;
- (2) Advance robust international cooperation to systematically constrain the criminal networks behind the scams; this may need to include leveraging sanctions or other punitive measures to target malign actors in countries that continue to provide the criminal actors with space to engage in forced labor scamming; USIP's SSG report identifies Myanmar, Cambodia and Laos the primary countries tolerating this activity.
- (3) Invest urgently in gathering and sharing information on all aspects of the scamming industry, in understanding the technologies deployed, and in building the capacity of law enforcement and regulatory agencies to counter these technologies, particularly with respect to crypto currency and fintech.
- (4) Engage in a nationwide, public awareness program to protect U.S. citizens, and support similar programs internationally to protect a global population.
- (5) Invest in prevention of new forms of technology fueled human trafficking, focusing especially on mobilizing the active involvement of private sector actors and platforms in reversing these trends.
- (6) Demand that the PRC share intelligence and information that it has gathered, and that it take decisive actor to prevent Chinese origin crime groups from harming the United States (similar to the response to the fentanyl crisis).

Thank you for inviting me to testify, and I look forward to your questions.

The view expressed in this testimony are those of the author and not the U.S. Institute of Peace.