United States Institute of Peace

Crossroads of Competition: China in Southeast Asia and the Pacific Islands

Testimony before the USCC

China-Linked Transnational Organized Crime in Southeast Asia: A Rising Threat to U.S. National Security

Jason G Tower

Myanmar Country Director and Team Lead, Program on Transnational Crime and Security in Southeast Asia

United States Institute of Peace

March 20, 2025

Introduction

Commissioner Price and Commissioner Schriver, distinguished members of the U.S.-China Economic and Security Review Commission, thank you for the invitation to speak about China-linked Transnational Organized Crime in Southeast Asia and the growing threat that it presents to America's national security. In my remarks today, I draw heavily on the findings of USIP's Senior Study Group Final Report published in May of 2024 titled Transnational Crime in Southeast Asia: A Growing Threat to Global Peace and Security[1], as well as over 7 years of work, and more than 20 USIP reports on China-linked Transnational Organized Crime (TOC) groups in Southeast Asia.[2]

Since early 2022, these criminal groups have begun targeting a global population with a scourge of sophisticated online scamming based out of industrial scale scam compounds or "fraud factories" located in Cambodia, Laos and Myanmar. As of the end of 2023, a USIP expert group estimated that these criminal groups stole nearly 64 billion US dollars per year, including over 3.5 billion U.S. dollars from Americans. In 2024, losses to Americans continued to rise, with estimates of 5 billion U.S. dollars[3] – an increase of 42%. Equally concerning, the criminal syndicates have tricked or trafficked people from 70 countries, including Americans into scam compounds, where they are forced to scam and subjected to torture.[4]

Also of direct concern to U.S. national security is the role of China in this crisis. Since the mid-2000s, Chinese government actors played a direct role in enabling the rise of these criminal groups by legitimizing them, accepting lucrative contracts from them to build out the infrastructure now housing the criminal activity, and piggybacking on them to build Chinese security influence across the region. Since 2019, China has advanced an unprecedented crackdown, but in ways that incentive the crime groups to increasingly target Americans and the nationals of other countries. Meanwhile, China continues to fail to hold its own officials accountable for their involvement in enabling this crisis, while it refuses to share critical intelligence on the perpetrators that might be used by U.S. and other international law enforcement to crackdown. The harm that China is doing to the United States with these online scams now parallels that related to fentanyl.[5]

---

[1] Transnational Crime in Southeast Asia: A Growing Threat to Peace and Security, United States Institute of Peace, May 2024, ssg_transnational-crime-southeast-asia.pdf.

[2] These reports are available at Transnational Organized Crime in Southeast Asia | United States Institute of Peace

[3] The FBI has estimated losses to the scams in 2024 at over 5 billions U.S. dollars. FBI says 'pig butchering' cryptocurrency scams hit victims in all 50 states. Given also that case of fraud are generally underreported by a factor of 10 or more, this means that these are very conservative estimates.

[4] USIP documented 68 countries at the time of publication of its SSG Report in May of 2024. It has subsequently identified two additional victim countries, bringing the total to 70.

[5] See for example, Sean O'Conner, Fentanyl, China's Deadly Export to the United States, USCC, 2017, USCC Staff Report_Fentanyl-China's Deadly Export to the United States020117.pdf; and more recent reporting from the Brookings Institute: The fentanyl pipeline and China's role in the US opioid crisis.

Before going deeper into these issues, please allow me to introduce myself.[6] Since late 2019, I have served as Myanmar Country Director in the Asia Center at the United States Institute of Peace, and since 2022, I have also directed 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 Southeast Asia, and since 2019 have focused much of my research and analysis on the growing rise and influence of China-linked 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 worked to support peace and address security threats stemming from 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 the criminal actors, identify perpetrators and to strengthen local, regional and international responses.[7]

Background: Chinese criminals take to the Belt and Road and how China Enabled a Global Crisis

Despite being illegal in China, the market for gambling is enormous, with online gambling alone constituting annually a US$25 – 60-billion-dollar illicit market.[8] Throughout the first decade of the 2000s, as online gambling technologies became more readily available, they spread almost completely unchecked across China. In 2006, Chinese authorities launched a major crackdown,[9] displacing large numbers of operators overseas into especially Myanmar, the Philippines and Laos, where they leveraged the presence of poorly regulated physical casinos to begin building a massive network of offshore online gambling facilities that would permit them to continue tapping the vast Chinese market. While the Chinese government continued some measure of efforts to crackdown, by the mid-2010s, it was estimated that over 500,000 Chinese nationals

[6] The views expressed in this testimony are those of the author and not the U.S. Institute of Peace.

[7] Transnational Organized Crime in Southeast Asia | United States Institute of Peace

[8] More conservative estimates placed the size of this market in 2018 at 25 billion U.S. dollars; see: World Gaming Information, "Foreign Media: China's Annual Illegal Gambling is 25 billion uS Dollars; The Government Is Cracking Down" [in Chinese], September 20, 2018, www.wgi8.com/news/news_27049.html

[9] See: China Criminal Law Analysis of the Crime of Establishing Online Casinos (in Chinese)

were working for the offshore gambling syndicates. They had become especially embedded in Northern Myanmar, where both local militia groups with close ties to China, as well as the Myanmar military provided protection for their activities, as well as in Laos and Philippines, where they had built deep ties with local authorities.

As China introduced its Belt and Road Initiative (BRI) in 2013, the offshore gambling syndicates almost immediately took up the mantra of the BRI as a means of legitimizing their activities and gaining support from powerful Chinese government actors that might shield them from Chinese law enforcement.[10] Key individuals from across these illicit capital networks began investing billions of dollars in an infrastructure development spree across the region, slapping the label of BRI on casino and "smart city" projects, offering lucrative construction contracts to Chinese State-Owned Enterprises desperate to increase their overseas market share. To cite one example, in the case of Myanmar, an illicit capital network hired a government think tank under China's premier state planning body to design a high-level plan for a new "smart city" as part of China's Belt and Road Initiative. They then plunged millions of dollars into buying influence and official titles in Chinese Chambers of Commerce across the region, eventually managing to convince the Federation of Overseas Chinese Entrepreneurs and the Chinese Embassy in Myanmar to host a signing ceremony of a multi-billion dollars project designed explicitly to host thousands of online gambling syndicates.[11] One of China's largest state-owned companies, the Metallurgical Corporation of China received a 350-million-dollar contract to construct the first phase of the infrastructure. Similar developments took place across Southeast Asia from 2016 – 2020, with the leaders of Chinese online gambling syndicates building unprecedented influence in a wide range of Chinese agencies and organizations involved in implementing the Belt and Road Initiative.[12]

The China-linked crime groups also found ready partners in Chinese agencies tasked with overseas influence operations. This included national and provincial foreign affairs offices (FAOs) and agencies linked to the Communist Party's United Front. The illicit capital networks proved to be ready partners in assisting these agencies towards meeting their objectives of influencing overseas Chinese to support China's narratives and interests overseas. The case of Wan Kuok-kui, aka Broken Tooth, one of Asia's most notorious criminal figures, illustrates this point. Having spent nearly a decade in prison for a wide range of crimes, Broken Tooth became deeply involved in online gambling and money laundering in Southeast Asia following his release from prison in 2010. He rebuilt his criminal organization under a front know as the Hongmen World Cultural and

[10] Jason Tower and Priscilla Clapp, Myanmar's Casino Cities: The Role of China and Transnational Criminal Networks, USIP, July 2020, 20200727-sr_471-myanmars_casino_cities_the_role_of_china_and_transnational_criminal_networks-sr.pdf

[11] Ibid.

[12] In Cambodia, the Dara Sakor project represents a similar example: Reflecting On China-Cambodia's Dara Sakor Project, 15 Years In – The China-Global South Project; while in Laos the Golden Triangle Special Economic Zone is a commonly cited case.

Historical Association, which claims to promote the Chinese "Freemason culture." This organization publicly claims to be deeply patriotic and mobilizes its members to parrot the propaganda of the Chinese Communist Party, attacking the United States, and threatening the human rights of Chinese dissident actors.[13] Famously, Wan Kuok-koi's public motto was "I used to fight for the triads, and I now fight for the Community Party."[14]

From Casino Cities to Industrial Scale Scam Cities: The Rise of the Scamdemic

By 2019, the China-linked transnational criminal groups behind the online gambling syndicates had emerged as one of the region's most powerful crime networks. This was despite occasional crackdowns by Chinese authorities, which rather than eradicating the syndicates from any particular country, instead resulted in their expansion into a broader range of geographies. Crackdowns in the Philippines from 2014-2016 resulted in the syndicates pouring into Cambodia, where by 2019 they had become the dominant players in Sihanoukville, which emerged as one of the region's largest unregulated gambling hubs.[15] A sudden crackdown in Cambodia triggered a massive movement into the Myanmar-Thailand border, where the Myanmar military's border guard force (BGF) was quick to provide territory and security to the crime groups to build out another network of "casino cities," even though this was illegal under Myanmar's national laws.[16] Meanwhile, in response to crackdowns on money laundering back in China, the criminal networks also began to invest heavily in crypto-currencies, underground banking networks, and sophisticated financial technologies as a means of circumventing the moves of Chinese police to follow their money trails.[17] This, combined with a growing number of wealthy Chinese looking to evade China's increasingly draconian capital controls resulted in the China-linked transnational crime groups also emerging as some of the most influential regional players in facilitating illicit capital flows.

By 2019, China-linked crime groups controlled vast territories across borders in Myanmar, Laos and Cambodia, and had managed to lobby the government of the Philippines to provide a formal legal framework to support their activities. They had invested tens of billions of dollars to construct entire online gambling cities, with the capacity to house well over 1 million people.

---

[13] See case study in USIP 2024, p.45.

[14] How Chinese mafia are running a scam factory in Myanmar – DW – 01/30/2024

[15] Ivan Franceschini and Roun Ry, Sihanoukville: Rise and Fall of a Frontier City, Global China Pulse, 2024, Sihanoukville: Rise and Fall of a Frontier City

[16] Ibid, USIP 2020.

[17] See, Jason Tower and Priscilla Clapp, Myanmar: Casino Cities Run on Blockchain Threaten Nation's Sovereignty, USIP, 2020, Myanmar: Casino Cities Run on Blockchain Threaten Nation's Sovereignty | United States Institute of Peace.

While so, competition and growing campaigns back in China targeting online gambling platforms resulted in a gradual pivot from online gambling to online scamming. By 2016, tens of thousands of online gambling platforms were struggling to expand their customer base in China, and the industry pivoted towards a more customized marketing strategy. Gambling syndicates would hire large numbers of "marketers" who were tasked with doing whatever they possibly could to compel people to open and fund online gambling accounts. This increasingly involved using some form of grooming process – building friendships or even romantic partnerships online to gain new customers. As this form of grooming process became the norm, some of the syndicates pivoted in 2017 towards what is now referred to as the "pig-butchering scam." Instead of using these unconventional marketing methods to entice gamblers, they instead marketed investment opportunities, introducing fraudulent crypto-currency platforms or securities trading platforms that would be used to get their targets to part with much greater sums of money.[18] On the eve of COVID-19, this "scamdemic" was beginning to take a large toll in China.

COVID-19 presented a major shock to the China-linked TOC groups. First, China called its nationals back from Southeast Asia, the Chinese police launching an unprecedented campaign to require that all individuals that had been staying Myanmar, Laos, Cambodia or the Philippines return or face serious fines or even confiscation of assets back in China if they failed to do so. This move caused the gambling syndicates to suddenly lose access to their primary labor supply. Second, China banned crypto currency[19] and ramped up its crackdown on both online gambling and scamming during the early phases of the pandemic, making it much more costly for the syndicates to scam Chinese.

This resulted in three very sinister adaptations: (1) the pivot further towards online scamming in place of or alongside online gambling; (2) the use of kidnapping, trafficking and deception to bring individuals into the compounds under control of the syndicates hosting the activity; (3) the rapid globalization of the operations of the China-linked scam syndicates.

From 2020-2021, the China-linked crime groups began a new building spree, this time though constructing facilities in Cambodia, Laos, Myanmar and the Philippines that looked less like luxurious casino cities and instead appeared more like penal colonies.[20] These facilitates were in close proximity to the casino cities, which were also rapidly converted into similar sorts of compounds that were built to prevent people from getting out. In 2020, rumors emerged in cities across mainland Southeast Asia of Chinese being kidnapped or forced into compounds. By 2021,

[18] For a quick overview of these pig-butchering scams, see: Jason Tower on the Dangerous Proliferation of Scam Compounds in Southeast Asia | United States Institute of Peace; or The Pig Butchering Invasion Has Begun | WIRED.

[19] China banned crypto-currency in 2019, and launched major crackdowns on foreign crypto-exchange platforms operating in the country in 2021: China declares all crypto-currency transactions illegal.

[20] See for example: The Myanmar Army's Criminal Alliance | United States Institute of Peace

this evolved further as reports emerged of desperate job seekers from Thailand, Cambodia, Laos, Myanmar and Malaysia being tricked into crossing borders illegally for what they thought were legitimate jobs, only later to discover that they had been trafficked into cyber-slavery and forced to scam. Conditions inside these compounds were horrifying – individuals were tortured if they failed to meet aggressive targets or if they refused to scam. They were also openly sold between compounds, treated by the Chinese scam syndicate bosses as commodities.[21] By 2022, as air travel began to open once again, the scam syndicates continued to globalize, targeting people across the world with fake job opportunities, and setting up elaborate websites for fake companies to deceive people into the compounds.[22] This resulted in Interpol releasing a warning in 2023 that "anyone in the world could fall victim to the human trafficking or the online scams carried out through these criminal hubs,"[23] and alarm bells in media and from law enforcement and immigration authorities across the world.[24] For the first time in history, Myanmar, Laos and Cambodia had emerged as destination countries for trafficking, and with cyber-enabled trafficking into scam compounds emerging as the newest threat.

Meanwhile, access to a global labor market meant that the China-linked crime groups could now target a global population with scams. Beginning in early 2022, they began targeting the United States, the U.K., Australia, and other developed economies, as well as wealthy countries in the region such as Singapore and Japan. By 2024, they targeted middle class individuals from across the world. In just 5 years, the China-linked TOC groups emerged as a global threat, now with the capacity to scam or traffic people from across the world, and to rapidly move and launder funds on a global scale.

Host States and Elite Capture

While a broad range of Chinese state and party actors were key to enabling the rapid rise of the China-linked crime networks behind the global pandemic of scams, money laundering, cyber-slavery and trafficking, corrupt elites across Southeast Asia and beyond also played a major role in fueling their rise. The three countries that represent the epicenter of this crisis – Myanmar, Laos and Cambodia – also represent the countries in the region with the weakest governance,

[21] See, UN OHCHR, Online Scam Operations and Trafficking into Forced Criminality in Southeast Asia: Recommendations for a Human Rights Response, United Nations, 2023, Online Scam Operations and Trafficking into Forced Criminality In Southeast Asia

[22] Al Jazeera released a documentary including interviews for rescued trafficking victims inside the compounds in July of 2022: Forced to Scam: Cambodia's Cyber Slaves | Human Trafficking | Al Jazeera

[23] Interpol Issues Global Warning on human trafficking-fueled fraud, June, 2023: INTERPOL issues global warning on human trafficking-fueled fraud

[24] The FBI first issued a warning to Americans in May of 2023: Internet Crime Complaint Center (IC3) | The FBI Warns of False Job Advertisements Linked to Labor Trafficking at Scam Compounds

highest levels of corruption, greatest levels of instability, and those that are most politically aligned with China.

China-linked TOC groups became involved in illicit gambling and narcotics earliest in Myanmar, preying on the instability in Myanmar caused by the country's 7-decades long civil war. In the case of Myanmar, China-linked crime groups have been central for decades to the Myanmar military's efforts to weaken ethnic insurgent groups, to extend its control into territories long under the control of minority groups seeking autonomy – many of these also having deep connections in China, including with Chinese illicit capital networks. On the Myanmar – China border, the three areas where the scam syndicates developed to industrial scale proportions included areas controlled by two ethnic armed groups with longstanding ceasefire agreements with the Myanmar military – the United Wa State Army and the National Democratic Alliance Army (Mongla Army). Both of these groups have a long history of involvement in narcotics[25], and are former members of the Burmese Communist Party, which was a communist insurgency group that the Chinese government supported from the 1960s until its collapse in the late 1980s.

The third, which until late 2023 was the largest player in Myanmar's scam industry was the Myanmar military' Border Guard Force (BGF) in a border territory known as Kokang, or as Self-Administered Region #1. This Kokang BGF illustrates perfectly how the Myanmar military used criminal activity to consolidate its control.[26] In the mid-2000s, the military demanded that all EAOs drop their arms and fold over into BGFs as a prerequisite to participating in a national peace process. After the majority rejected these demands, the military used a combination of force and co-optation to splinter and ultimately defeat several key armed groups. On both the China and Thailand borders, the army cut a deal with corrupt elements of local armed groups, whereby which they accepted the deal, defected with troops and joined the military as BGFs in exchange for the right to engage in any form of illicit activity as they saw fit. In 2009, four key clans central to the leadership of an EAO known as the Myanmar National Democratic Alliance Army (Kokang) accepted this deal, defected, and received the rights to develop massive casino cities in Kokang, largely in partnership with Chinese crime groups. From 2009 until 2023, the scale of these operations grew to the point that by early 2023 there were over 50,000 foreign nationals under more than 200 scam syndicates spread across more than 30 industrial scale scam centers. All of these were directly owned and operated by the Myanmar military's own BGF, which at the same time had close ties with Chinese government officials in Yunnan Province as well as in other parts of China.[27] Scam facilities operated on a similar scale in the UWSA and NDAA territories, in these

[25] The UWSA has been the focus of a series of sanctions by the U.S. Treasury Department since at least 2000; see: Treasury Action Targets Burmese Drug Cartel | U.S. Department of the Treasury

[26] Myanmar Regional Crime Webs Enjoy Post-Coup Resurgence: The Kokang Story | United States Institute of Peace

[27] For years, the Fully Light Group, which was the front company for many of the Kokang based scam syndicates poured money into formal trade platforms with the Chinese government. This continued until August of 2023, only 2 months before a major crackdown began, see: Chinese media report.

two cases, the scam centers being directly under the control of these armed groups. These facilities brought in billions of dollars in revenue annually, largely targeting Chinese nationals, with a significant amount of the proceeds going both to the military and to EAOs to purchase weapons. Similar developments took place later on the Thailand border, with the Myanmar army's BGF there once again partnering with China-linked TOC groups beginning from late 2016.

While the democratically elected National League for Democracy government attempted to crackdown on the criminal groups from 2016 – 2020, following the 2021 military coup, the development of scam compounds was thrown into overdrive, as the situation created by the coup morphed the country into a breeding ground for illicit activity. According to the Global Organized Crime Index, following the coup, Myanmar emerged as the country with the lowest resilience to crime in the world, and is now the number one illicit market for scamming and narcotics.[28]

Whereas in Myanmar, the Myanmar military's willingness to build alliances with crime groups to consolidate power made conditions perfect for the rise of this criminal activity, in Laos, the country's weak governance made it a hub for criminal actors. In particular, the Laos government has long struggled to govern territory adjacent to the Mekong River in the Golden Triangle where Laos, Myanmar and Thailand connect. This area has been central to the global drug trade for decades, and Myanmar's war has frequently spilled over across this region. Beginning from the mid-2000s, Chinese crime groups in partnership with the NDAA and the UWSA pushed into Laos, where they aimed to consolidate the drug trade and build a new casino hub to launder proceeds from the drugs. The Lao government agreed to a scheme in 2007 which effectively brought control of the Golden Triangle under a Chinese criminal named Zhao Wei who had amassed a fortune operating casinos in Northern Myanmar since the late 1990s. The territory under his control was given status as a Special Economic Zone (SEZ) known as the Golden Triangle SEZ (GTSEZ), and he became the effective governing authority over the zone. Zhao Wei constructed one of the largest casinos in the region and poured funds into developing the area into a hub for online gambling and scamming. In this case, the Lao government played a direct role in enabling the illicit activity by granting a concession that effectively brought Laos territory under the control of an alliance of China-linked crime groups and Myanmar armed groups deeply involved in narcotics.[29]

In the case of Cambodia, elites welcomed the arrival of powerful Chinese gambling syndicates starting from 2015. Nearly all of the known players in China's online gambling sector have well documented and public dealing with top elites, including the former Prime Minister's Nephew, Hun To and senator Ly Yong-Phat.[30] During the 2019 pandemic, the scam syndicates became the main investors in the economy, the scam business growing so rapidly that by 2023 it had emerged

[28] Myanmar's ranking on the Index is available here: Criminality in Myanmar - The Organized Crime Index
[29] See case study on the GTSEZ in USIP 2024, p. 37.
[30] See Jake Sims, Coercion and Criminality: Cambodia's Dual Threat to Regional and Global Security, January 15, 2025: Coercion and Criminality: Cambodia's Dual Threat to Regional and Global Stability – The Diplomat

as the largest sector in the Cambodia economy.[31] This has resulted in the Cambodia government emerging as one of the most vocal international defenders of the online scam syndicates, actively denying that there is human trafficking, slavery and scamming operating on an industrial scale even though the scam syndicates have expanded across all of the country's borders and even into inland provinces.[32]

In addition to these three mainland Southeast Asian countries, the Philippines represents the fourth country which hosts the scam syndicates at a significant scale. In this case, it was largely the interests of the Duterte Presidency that fueled their rise.[33] The Philippines provided initially the online gambling syndicates with a legal platform to operate offshore gambling facilities targeting China – something which became a major flashpoint in the China-Philippines relationship. While so, under Duterte, the country opted to make major political concessions to China as a means of reducing Chinese state pressure on the country related to the online gambling issue.

This trade off resulted in serious harm to the country's sovereignty, which ended up coming back to haunt Duterte in the 2022 election. The current President came into office with a direct focus on the issue of the illegal activity under the POGOs and the social instability that they had produced. Unlike Cambodia, Myanmar or Laos, the Philippines launched an unprecedented crackdown on the POGOs and the scam syndicates hiding behind them in 2023, making major progress in addressing the problems, but on the Philippines own terms.[34] While the problems persist, the Philippines has emerged as one of the countries in Southeast Asia with the highest levels of political will to address the problems.

The case of the Philippines also underscores another darker side of Chinese influence operations, unearthing strong evidence of direct ties between scam centers and Chinese influence operations, including even covert military operations. For example, the Philippines military documented a presence of scam centers adjacent to military facilities, and seized sophisticated listening equipment through raids on the centers.[35] Meanwhile, they also found evidence of state sponsored hackers having used space in or working with the scam syndicates. In another case, a

[31] UNODC estimated the size of the scam economy in "one Southeast Asian state" at 7.5 to 12.5 billion U.S. dollars: UNODC joins regional crime fighters to tackle scams and human trafficking in SE Asia | UN News; this tracks with USIP's 2024 estimate: ssg_transnational-crime-southeast-asia.pdf

[32] See for example: Cambodia Challenges UN on Scam Center Claims | Cambodianess.

[33] See: Hontiveros says Rodrigo Duterte benefitted from illegal POGOs - Philippine Information Agency; as well as a wide range of in depth media reports highlighting the history of the rise of the POGOs, [Closer Look] Drugs, POGOs, Quiboloy: Duterte's tyranny at the service of corruption

[34] Help eradicate POGOs, Marcos tells LGUs | Philippine News Agency

[35] See: China, Scam Centers, and National Security in the Philippines - Inkstick

Chinese criminal kingpin has even publicly alleged that he and several other kingpins operating in the Philippines were Chinese spies.[36]

Meanwhile, the China-linked crime groups behind the scamdemic have a web of influence that extends across every country in ASEAN.[37] This enables them to launder money, to develop, register and operate sophisticated fintech, to traffic individuals from across the region and to obtain "golden passports" or new identities by exploiting corruption or gaps in the capacity of states when it comes to determining the identity of their nationals. It is important to note that the China-linked crime groups have attempted to establish scam centers in other countries in the region, including Malaysia, Vietnam, and Thailand, but that authorities in these countries have cracked down relatively swiftly on any sizable scam operations in their territories. Until very recently though, countries like Thailand have demonstrated a lack of will to crackdown on cross-border operations, resulting in it becoming a significant transit hub for the criminal activity, as well as an operations center for many of the criminal kingpins involved.

How the Scams Work[38]

Criminals engaged in pig-butchering scams are adept at using current digital technology—social media, artificial intelligence (AI), cryptocurrency, and blockchain—to lure potential victims, operate the financial side of the scams, and launder the proceeds of their crimes. They use crypto-currency for several reasons. The most basic is that victims are usually unfamiliar with cryptocurrency and can be easily manipulated to follow the damaging suggestions of their new romantic or investment partner from the beginning of the scam. Most pig-butchering scams run roughly according to the following script: The perpetrator reaches out on social media or a dating platform to a victim flagged as belonging to one of several vulnerable groups—for example, a single individual between ages 40 and 60. The initial hook is what appears to be a misdirected message, such as "J are we still meeting in 5 minutes?" that comes from an account with an attractive profile picture. The potential victim responds that he is "not J," and the perpetrator then attempts to begin a conversation and get to know the victim on a personal level. A period of courtship follows, during which the perpetrator forms a romantic relationship or friendship with the victim that sometimes lasts for months and involves video calls to deepen trust. On video or in photographs shared with the victim, the scammer may appear in luxurious surroundings that the scammer says are the product of their financial acumen. With trust established, the perpetrator introduces what they assure the victim is a moneymaking opportunity. Victims are

[36] 101 East, She Zhijiang: Discarded Chinese Spy or Criminal Mastermind, Al Jazeera, September 2024: She Zhijiang: Discarded Chinese spy or criminal mastermind? | Crime | Al Jazeera.
[37] Ibid, USIP 2024.
[38] Note that this section draws heavily on pages 21-22 of USIP 2024.

encouraged to wire funds to an unregulated cryptocurrency exchange they may be familiar with, such as Coinbase or Gemini, and to convert their currency to Tether, a "stablecoin" that is tied to the US dollar and that is fast and inexpensive to move. The victim is then directed to download a bogus "investment platform" app provided by the perpetrator, open an account on it, and move their cryptocurrency from the exchange where it is under the victim's control to the platform account controlled by the scammers. A sham dashboard on the platform will show the victim is booking impressive profits—encouraging continuing deposits—as their money is being moved out and laundered through a chain of "crypto wallets" (devices or platforms that store cryptocurrency) and off the blockchain completely. The relationship and subsequent deposits in the scheme continue until the perpetrator determines that the victim has been bled dry of assets. The scammer then "slaughters the pig" and disappears. All of this, accomplished by scam syndicates working in highly specialized teams, can leave the victim financially and emotionally devastated, even suicidal. In many cases in the United States, losses range from 100,000 to over 1 million dollars per victim, with several cases involving much higher losses. In one case in 2023, a victim from Kansas lost 47 million U.S. dollars, most of which he managed to embezzle from a bank, resulting in the failure of the bank and serious damage to people across a small town.[39]

For investigators, the transparency of the blockchain is helpful—to a point. By looking at the blockchain, law enforcement can follow the transactions but cannot identify the owners of the wallets. Investigators are unable to determine the identity of the wallet owners until the cryptocurrency lands in an exchange where customer information is mandated. Many exchanges are deliberately housed in locations not subject to US law and are unwilling to cooperate voluntarily with criminal probes. Law enforcement internationally is plagued by insufficient understanding of how to use blockchain in investigating financial crime. The gap between scammers' and investigators' knowledge is wide and grows daily. While law enforcement struggles to catch up, the scammers stay dangerously ahead.

But there is still more to the story – often the person on social media perpetrating the scam is also a victim. Since 2021, the scam syndicates have used another form of fraud to deceive and traffic tens of thousands of people into modern slavery. While the modalities of trafficking continue to evolve, the majority were tricked using advertisements on common social media platforms for high paying jobs in key transit cities such as Bangkok, Dubai, or Kunming. The individuals pass through several rounds of online interviews, and once they are "hired," have plane tickets purchased for them. On arrival in the transit city, they are told that they need to hand over their passport to process work visas before being trafficked, often across borders into the scam compounds.

[39] Crypto scam wrecks Kansas bank, sends CEO to prison

Over the past year, even more sinister forms of trafficking have been devised by the China-linked crime groups. This includes a much more customized approach involving reaching out to professionals with a very specific job or business opportunity, such as a chance to engage in business negotiations for a sizable contract, or to audition for a part in a movie.[40] In late December a group of Chinese movie professionals were trafficked using this modality, and it is likely that the syndicates will continue to use this and even more complex forms of tricking victims into the scam centers.

Moving the Money: Criminal Fintech and Underground Banking Networks

The China-linked crime groups behind the scams have also emerged as some of the most dominant players globally in laundering illicit capital around the world. In conjunction with the rapid development of online gambling syndicates throughout the 2000s, a web of underground banking facilities began to emerge across Southeast Asia, which enabled Chinese to move money offshore without having to make overseas transfers. These underground money facilities or "Dixia Qianzhuang" now operate globally, providing Chinese illicit capital networks with many options for moving illicit cash. Common platforms are based in countries like Myanmar and Cambodia, with some of the largest including Huione,[41] Yatai Exchange and Fully Light Guarantee. Each of these maintains a network of exchanges across multiple cities and countries that enable scam syndicates to access cash where needed. The key service provided is moving massive amounts of stolen crypto currency across tens of thousands of wallets before pulling it out into the formal economy, often then laundering it through a web of upscale restaurants and often Chinese Hot Pot restaurants, casinos, nightclubs, bars and e-commerce platforms. A recent study by the University of Texas illustrates the scale of these money laundering operations. By following movements of stolen crypto-currency across the blockchain, researchers identified that over 75 billion US dollars was moved through a web of consolidation accounts using a full range of crypto-currency exchanges.[42] Another media expose illustrates the direct involvement of Chinese business groups in laundering this money, linking a Chinese Chamber of Commerce in Thailand to the laundering of 90 million dollars stolen from American victims.

These money laundering rings have a thriving business including in China, where hundreds of millions of dollars are laundered back into the otherwise suffering Chinese economy. In the case

[40] A recent USIP report documents this: China Exploits Thailand's Crackdown on Scam Compounds to Grow Security Influence | United States Institute of Peace

[41] For a full expose on Huione, see: Elliptic, Huione: the company behind the largest ever illicit online marketplace has launched a stablecoin, 14 January 2025, Huione: the company behind the largest ever illicit online marketplace has launched a stablecoin.

[42] John Griffin and Kevin Mei, How do Crypto Flows Finance Slavery? The Economics of Pig Butchering, SSRN, March 2024, How Do Crypto Flows Finance Slavery? The Economics of Pig Butchering by John M. Griffin, Kevin Mei :: SSRN

of Cambodia, billions of dollars of stolen money go directly into real estate in the country and represent the main source of capital funding new real estate projects. Much of the proceeds from Myanmar move into countries across the rest of the region, including into Cambodia, but also Thailand. Singapore has also featured significantly in the operation of these money laundering syndicates,[43] as has Malaysia. Many of the syndicates also are looking to move assets into a much broader range of markets, including key financial centers around the world. Evidence of movement of such assets into the Isle of Man, for example have recently been exposed, as well as the presence of the scam syndicates there.[44]

China's Crackdown and the Global Security Initiative: Rising Chinese Security Influence

Chinese court cases and state media reports highlight how China has scaled up its moves to crackdown on offshoring online gambling networks and scam syndicates especially from 2012. While so, until very recently, these moves failed to rein in any of the significant Chinese criminal kingpins involved – largely due to the protection they enjoy vis-à-vis a web of elites across Southeast Asia and extending back into China. The case of the notorious criminal kingpin behind one of the world's largest scam cities, the Shwekokko Yatai New City Project on the Myanmar – Thailand border illustrates this point. She Zhijiang AKA She Lunkai was targeted by Chinese police from 2012-2014 for hundreds of millions of dollars of financial crimes related to his operation of illegal offshore gambling operations from the Philippines. Chinese courts sentenced several individuals in his network to multiple years in prison, issuing a warrant for his arrest.[45] By 2019 though, She had scaled up his illicit operations in the Philippines, obtained a Cambodian passport, and established direct business relationships with representatives of China's People's Consultative Conference (CPPCC) to build a scam city in Myanmar. He did all of this and made numerous trips to China despite being wanted by Chinese police.[46]

China's posture towards these scam syndicates began to shift however in mid-2019 when the Myanmar government decided to raise directly with Beijing concerns about the rampant criminal activity surging on its border with Thailand. At the time, Myanmar elected National League for Democracy government demanded that China explain why a "casino city project" – which was

[43] See CNA reporting on a mulit-billion dollar money laundering case linked to these criminal networks from August 2023: All the convicts in Singapore's S$3 billion money laundering case have been sentenced. What now? - CNA
[44] See BBC Investigative report: Chinese scammers used Isle of Man for 'pig-butchering' con; a recent UNODC report also highlights this trend: TOC_Convergence_Report_2024.pdf
[45] See: Fugitive Behind $15 Billion Myanmar Business Hub Arrested in Thailand - Caixin Global; original court case heard by the Yantai City Court on December 22, 2014.
[46] Jason Tower and Priscilla Clapp, Myanmar's Criminal Zones: A Growing Threat to Global Security, November 2022, Myanmar's Criminal Zones: A Growing Threat to Global Security | United States Institute of Peace.

not approved by the central government -- was advancing as part of China's BRI outside the formal mechanism between the countries that had been established to negotiate BRI projects. This, combined with strong media pressure prompted China to distance itself from the criminal activity, and the Chinese Embassy in Myanmar publicly pledged to assist in addressing the illegal activity in August 2020. This incident marked a significant shift with China suddenly turning to target some of the criminal groups that had previously openly partnered with Chinese state actors.[47]

This coincided with rising public pressure in China, as tens of thousands of victims began to publicly protest the failures of the Chinese government to help them recover lost funds. With the collapse of the Chinese economy during COVID-19, China began to increase dramatically attention on these issues, this becoming one of the top issues of concern for Chinese police by 2022. China began to leverage a response to the offshore online scam syndicates to advance at least four objectives: (1) to deepen Chinese state control over the Chinese public. This was accomplished through the introduction of a wide range of new monitoring and surveillance technologies that were framed as measures to keep Chinese safe from scams, such as an anti-scam application.[48] This in reality provided the Chinese police with a wide range of new tools to monitor both online and offline activities of the public; (2) to promote the role of Chinese police overseas as part of a propaganda effort to demonstrate to the Chinese public and to overseas public audiences their ability to keep Chinese nationals safe; (3) to assert control over increasingly powerful overseas Chinese crime groups, some of which had started to openly counter the Chinese state and Communist Party narratives;[49] (4) to dominate the police intelligence space around these issues by repatriating back to China millions of devices that have been seized in raids on scam centers. China gained access to a massive database of information in late 2023, when a military operation on its border in Kokang resulted in a sudden flood of 50,000 plus individuals streaming across the border. China has not shared this information with other countries, even though the phones and computers certainly contain important intelligence on and private information of individuals from around the world targeted by scammers.

China began ramping up its efforts to "shock and awe" the Chinese public by televising the repatriations of Chinese criminals from overseas, and by regularly reporting on the "interception" of and prevention of billions of dollars in losses from scams.

[47] The Chinese police went on to issue a new arrest warrant for She Zhijiang in 2022, leading to his arrest in Bangkok in August 2022.

[48] Human rights groups have raised a range of concerns about the usage of the Chinese anti-scam application; see: "Anti-fraud" (反诈) spyware apps, phone inspections in China · Issue #354 · net4people/bbs

[49] This is especially the case for She Zhijiang who now openly claims to be a Chinese dissident: Detained gambling tycoon She Zhijiang faces rendition to China – Radio Free Asia

In 2022, China unveiled its Global Security Initiative (GSI), which aims to reshape global security norms and structures to give China advantage in terms of securing its overseas economic interests and dramatically increasing China's overseas security influence.[50] Since the introduction of GSI, China has started to link the involvement of its police in cracking down on online scam syndicates as part of the initiative. Increasingly, China is demanding that countries across Southeast Asia and beyond accept "Joint Law Enforcement Cooperation" as a means of cracking down on these criminal syndicates. In reality, what China is seeking through these joint law enforcement cooperation frameworks is access for its police overseas, and an opening to increase Chinese influence in the security space.

Since 2023, this has become very apparent in the Mekong Region, which not coincidentally is the "pilot zone" for China's GSI according to a 2023 White Paper on the Initiative.[51] Throughout 2023, China became very aggressive in demanding that Myanmar's military regime crackdown on criminal scam networks operating under its control, and after it refused, China openly partnered with Ethnic Armed Organizations on its border which launched a military operation to advance a crackdown. This resulted in the Myanmar military losing control of dozens of towns in the China-Myanmar border area, and ultimately in the Myanmar military dismantling its own border guard force (BGF) and handing its leaders over to the Chinese authorities after China issued a warrant for their arrest.[52] Following this development, the Myanmar military has become one of the most vocal advocates for China's GSI, and has made a series of concessions allowing the Chinese police, as well as armed Chinese security to operate in the country.

In Thailand, China has also used coercion to push Thai authorities to accept Chinese police access. In early 2024, following the trafficking of several Chinese nationals into Myanmar through Thailand, the Chinese government permitted and even openly encouraged disinformation about public security concerns in Thailand to surge in Chinese media and social media. This resulted in serious economic losses for Thailand, which is highly dependent on tourism, especially from China. To reverse this, Thailand made very significant concessions to China in the security space in exchange for getting China's support in addressing the public safety narratives and restoring confidence on the part of Chinese tourists. What has resulted is that China now has an active police presence on the ground on the far south of the Thailand – Myanmar border. China has used its growing security presence in Thailand and the leverage gained from the scam syndicate issue to push Thailand to cave to Chinese demands that threaten to seriously undermine Thailand's

[50] Carla Freeman, Bates Gill, Alison McFarland, China's Global Security Initiative Takes Shape in Southeast Asia and Central Asia, USIP, November 2024: sr534_chinas-global-security-initiative-takes-shape-southeast-central-asia.pdf
[51] China's GSI White paper refers to Lancang-Mekong Cooperation (LMC) as a pilot zone: The_Global_Security_Initiative_Concept_Paper.pdf.
[52] Jason Tower and Priscilla Clapp, Myanmar's Collapsing Military Creates a Crisis on China's Border, USIP, April 2024, Myanmar's Collapsing Military Creates a Crisis on China's Border | United States Institute of Peace.

relations with other countries.[53] In February of 2025, this included Thailand's deportation of 40 Uyghurs who had been seeking asylum in the country for over 8 years.

China has also leveraged this issue to deepen its security influence vis-à-vis countries across Southeast Asia and even within international institutions. It has pushed countries across the region to accept a stronger presence of Chinese police on the ground, and it has pushed to frame any moves to crackdown on crime as part of its GSI. Meanwhile, it has managed to compel the UN Office on Drugs and Crime (UNODC) to introduce a China-ASEAN roadmap for work on the crisis related to online scamming,[54] ignoring the fact that this crisis now impacts almost every country across the world. Such moves risk mainstreaming China's authoritarian approach to policing across the region and beyond.

Perhaps of most significant concern to the United States is the way in which China's crackdowns are increasingly incentivizing the China-linked scam syndicates to make America their number one target. With China deepening its control over the social media platforms used to scam Chinese, and with it putting in place much stricter controls over the banking system and even on Chinese travel to certain Southeast Asia countries, this has increased the cost of scamming in China dramatically. In response, the scam syndicates are increasingly pivoting to target the rest of the world, and especially Americans. In 2024, China reported a year on year decrease in losses to scams of 30% -- whereas the U.S. saw an increase of over 40%. At the same time, it is also clear that China is much less concerned about cracking down in cases in which the crime groups are: (1) laundering money back into China; (2) have deep connections with Chinese political elites and are openly patriotic. The case of Wan Kuok-kui and his Hongmen network, discussed above underscore this point.

Recommendations for U.S. Policy

To address this growing crisis, the U.S. needs nothing less than a whole of government, whole of society approach. This should begin by focusing on immediate steps that can be taken to keep Americans safe from this scourge of online scamming. Several immediate steps could prove to be critical in this regard: (1) a nationwide awareness raising campaign to help prevent people from falling prey to the scams; (2) training of law enforcement in addressing sophisticated forms of scams and fraud, particularly those employing crypto currency; (3) mobilizing the U.S. private sector to systematically prevent criminal actors from exploiting U.S. social media, dating,

[53] Jason Tower, China's Exploits Thailand's Crackdown on Scam Compounds to Gain Security Influence, USIP February 2025, China Exploits Thailand's Crackdown on Scam Compounds to Grow Security Influence | United States Institute of Peace.

[54] ASEAN, China, and UNODC agree to a plan of action to address criminal scams in Southeast Asia

professional networking, and recruitment platforms, which are the main entry points that the criminal actors use to target Americans. Some interesting initiatives have already been undertaken in this regard to increase transparency when fraud occurs on dating applications.[55]

Second, the U.S. could establish a task force, potentially under the National Security Council to coordinate government and law enforcement efforts to address these problems. This could potentially be coupled by the creation of a Congressional Caucus that might be tasked with monitoring trends, identifying policy options to keep the U.S. safe, and aiding states and/or districts that have been hit particularly hard by the scams. Such initiatives could also take the led in holding China to account for this crisis, including demanding that China share with the United States intelligence that it has collected from raids and seizures on scam compounds that might be helpful for the U.S. in combating these problems and in seizing and returning stolen assets. The U.S. may also push for China to hold its officials accountable for their role in enabling this crisis, and to prevent China's crackdown from incentivizing the criminal groups to pivot towards targeting Americans. ***In this regard, the U.S. could consider this issue alongside fentanyl, as a second case where China looks the other way or even benefits as China-linked crime groups harm the American public.***

Third, the United States can consider strategic partnership in the region, particularly in countries like the Philippines or Thailand. In the case of the Philippines, political will to crackdown is high, and the government is openly concerned about the national security implications related to both the China-linked TOC groups and China's response. Philippines has access to large amounts of intelligence related to the scam centers draw from recent crackdowns but lacks the capacity to harvest and analyze this data. In both the Philippines and Thailand, the U.S. might provide direct technical assistance into this process, which could put the U.S. in a much better position to advance a crackdown.

Fourth, the U.S. can hold other countries actively protecting the crime groups or obstructing efforts to crackdown accountable. This might include through sanctions targeting malign actors and elites especially in Myanmar and Cambodia. Finally, in the case of Myanmar, given that problems around transnational crime will continue to flourish as long as the Myanmar military continues its war against the Myanmar people, the U.S. might play a greater role in addressing the crisis. Insofar as China has deepened its security influence in Myanmar following the 2021 military coup, such a move could also help combat Chinese designs on establishing dominance over the Indo-Ocean region through Myanmar – a direct threat to a U.S. interest in free, open and fair trade in the Indo-Pacific.

[55] See for example, a piece of legislation aimed at increasing responsiveness and accountability on the part of dating applications: House Passes Congressman Valadao's Online Dating Safety Act | U.S. Congressman David Valadao.

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