Crime, Corruption, and Power: The Rise of CCP-linked Scam Networks Targeting Americans and Threatening U.S. Security

Testimony before the House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party

Jason G Tower
Senior Expert
Global Initiative against Transnational Organized Crime (GI-TOC)
May 19, 2026

INTRODUCTION

Chairman Moolenaar, Ranking Member Ro Khanna, distinguished members of the House Select Committee on the Strategic Competition between the United States and the Chinese Communist Party, thank you for the invitation to speak about China-linked scam syndicates and the growing threat that they pose to American national security. In my remarks today, I draw on 8 years of work documenting the malign influence of China-linked organized criminal groups in Southeast Asia and beyond, as well as more than 20 publications on the topic.

Over the past decade, China-linked transnational criminal organizations have emerged as the most powerful and influential crime groups in Southeast Asia, and are increasingly expanding into other parts of the world and establishing dominance over major criminal markets. Over just the past 5 years, China-linked scam syndicates have transformed mainland Southeast Asia into the global hub for cyber-scams, undermining the reputation of the region, pushing out the licit economy, and inflicting deep harm on almost every Association of Southeast Asian Nations (ASEAN) country. China-linked scam syndicates operating globally now steal an estimated 175 million U.S. dollars per day from a global population of victims, and have trafficked tens of thousands of people from 80 countries around the world into forced criminality. They further operate the most extensive money-laundering and underground banking networks in the world, with a recent study identifying that they launder at least 20% of all illicit crypto-currency assets. The operations of these China-linked scam syndicates are now expanding rapidly across the globe, raising concerns that the global harm will increase exponentially over the coming months and years as international efforts to respond remain slow to mobilize.

While before 2020, most of these crimes targeted victims in the People's Republic of China (PRC), over the past 5-years, the criminal groups have globalized their operations making English speaking countries, and especially the United States their top targets, with U.S. authorities now reporting over 10 billion per year in direct financial losses. This does not include the large numbers of victims that do not report losses, nor does it include the indirect harm – including the devasting impacts that this has on the mental health of Americans, on American families and on U.S. financial systems. In some of the most extreme cases, victims and even their family members are pushed to the brink as a result of these crimes, with multiple documented cases of Americans committing suicide.

Beyond the direct harm to Americans, the unprecedented influence consolidated by Chinese criminal actors in a growing range of countries in Southeast Asia and beyond present additional threats to U.S. national security, particularly as they serve to undermine governance and democracy, spread corrupt practices, drive violent conflict, and undermine global financial institutions.

In my testimony today, I will highlight four key points, all with critical implications for U.S. national security:

(1) The Chinese Party State, wittingly or not, played a direct role in enabling this crisis in scams and fraud from 2006 to present, including through the involvement of Chinese State Owned Enterprises in constructing the infrastructure used for the scams; the

failure of Chinese police to prevent a global spread of China-linked criminal activity; and a web of corruption in China and across the Southeast Asia region that has fueled the growth of these criminal operations.

(2) More recently since 2020, the China-linked criminal networks operating across Southeast Asia have responded to the PRC's policy and law enforcement measures by developing increasingly sophisticated forms of cyber-crime, and by globalizing their criminal activities. This has resulted in the rise of what is known as "foreigner butchering" in Chinese, which refers to China-linked scam syndicates focusing their crimes on victims in other countries, and especially countries viewed as adversaries of the PRC. While the Chinese government is reporting a sharp decrease in loses to scams, these dynamics are fueling rising losses in the United States and other countries.

(3) There is a growing risk that the Chinese Party State may leverage the presence and influence of these crime groups in Southeast Asia to gain political advantage both vis-à-vis individual countries, but also in terms of dividing and weakening regional platforms. At present, these dynamics are most apparent in Myanmar, where China has deep geo-strategic interests and where it increasingly leverages responses to online scams as a tool to influence the behavior of conflict actors vis-à-vis these interests. Related to this, there are also clear signs that China is linking joint law enforcement cooperation that might address challenges related to online scams to its Global Security Initiative – a platform that runs counter to American national security interests.

(4) As the U.S. takes bolder action to address this malign criminal activity, international pressure on the epicenter countries and on China has increased, triggering significant instability around scam centers operations in mainland Southeast Asia. A lack of political will and genuine enforcement actions in the epicenter countries has left the door open for China-linked scam syndicates to adapt operating modalities and to expand operations at scale across the globe, including into additional Southeast Asian countries, South Asia, Africa, the Middle East and in Latin and South America. As this process of geographic disbursal continues, threats to the United States and challenges associated with disrupting the criminal activity will become more acute.

The growing threats posed by China-linked scam operations to U.S. national security make it increasingly imperative that the United States to address these dynamics within the broader context of strategic competition with the Chinese Communist Party. I will conclude my testimony by outlining a series of recommendations for the U.S. Congress and U.S. decision makers to consider as they pursue further actions to protect the American people from these malign activities and prevent the Chinese Party-State from deriving geostrategic advantage as this crisis continues to expand.

1. THE CHINESE PARTY STATE AND THE RISE OF CHINA-LINKED SCAM OPERATIONS IN SOUTHEAST ASIA

By mid-2025, China-linked transnational criminal groups had established hundreds of industrial scale scam compounds across Southeast Asia, concentrated particularly in Laos, Cambodia and Myanmar. In all three of these countries, "scam cities" – emerging and urbanizing territories under the control of China-linked criminal groups featuring hundreds of real estate projects designed explicitly for hosting online scam operations involving tens of

thousands of people – had emerged. The Golden Triangle Special Economic Zone located in Laos adjacent to the point along the Mekong River where Myanmar, Laos and Thailand intersect offers one of the best examples of these forms of scam cities. In mid-2024, the zone had developed to a point that it boasted capacity to host nearly 150,000 people, and at the time was in the midst of a major construction boom that would place capacity in excess of 300,000. Similar scam cities were emerging elsewhere in Poipet, Cambodia and in Shwe Kokko and Myawaddy, Myanmar, all of which boasted populations involved in online scams or scam adjacent activity in excess of 25,000 individuals.[1]

To understand how China-linked criminal groups grew in power, wealth and influence to the point that they might be able to establish entire cities purposed for online scams, it is critical to understand the rise of Chinese offshore online gambling syndicates since 2006. In China, any form of gambling or online gambling is illegal with the exception of state-run lotteries. Despite this fact, the market for gambling in China is enormous, with a study dating back to 2005 estimating the market at 20 billion U.S. dollars per year. As online gambling technologies became available in China in the 2000s, Chinese organized crime groups pivoted to tap this emerging illicit market. Similar to what happened with illegal casinos and gambling dens, Chinese police moved to begin cracking down. In response, however, China-linked criminal groups pivoted overseas, targeting countries with legal frameworks for gambling, and especially countries where regulatory capacity vis-à-vis casinos and online casinos was low. From 2006 – 2015, it is estimated that over 500,000 Chinese relocated to Southeast Asia to join offshore online gambling syndicates, which were increasingly lucrative. Chinese authorities continued efforts to crackdown, but the offshore online gambling syndicates invested heavily in cutting edge technologies, including blockchain and cryptocurrency, which were both exploited to move funds through online gambling platforms and out of China. Meanwhile, large IT teams built online gambling platforms that might remain accessible despite efforts by Chinese police to seize or shut them down.

As the size of the Chinese online gambling market grew to exceed 40 billion dollars per year, China-linked offshore online gambling syndicates saw opportunities to pour funds into the development of new "casino cities" across the region – from Sihanoukville, Cambodia to Shwe Kokko, Myanmar. They exploited several key vulnerabilities in doing this: (1) a surge of interest in special economic and industrial zones across mainland Southeast Asia as countries like Laos, Cambodia and Myanmar sought to attract foreign direct investment; (2) a strong interest in the part of Chinese State-Owned Enterprises and especially State construction firms in building a stronger presence in the region. Across Laos, Cambodia and Myanmar, the same trends played out with Chinese State-Owned Enterprises signing large contracts with front companies that were established to build what would eventually become the "scam cities" mentioned above. From 2017 – 2022, SOEs received hundreds of millions in contacts from entities owned or controlled by major players involved in online gambling across the region – many of which had histories of criminal records back in China related to online gambling or money laundering.

The expansion of Chinese offshore online gambling syndicates into online scamming occurred naturally given the fact that the human resource teams and operating modalities involved in

[1] These estimates are based on both the size of and number of buildings in the zones, as well as the membership of Telegram channels directly linked to each of these scam cities.

online gambling could easily be redeployed for online scams, and as crackdowns by Chinese police picked up in the late 2010s. Large marketing teams that had focused on luring Chinese nationals to online gambling platforms were redeployed to promote fraudulent investment opportunities or platforms, thus giving rise to the pig-butchering scam. China-linked criminal groups found these forms of scams much more lucrative, as they might be designed to compel victims to invest very large sums of money – even their entire net worth. Meanwhile, from the Philippines to Laos to Cambodia to Myanmar, it was easy for scam syndicates to maintain registration as offshore online gambling entities to conceal their activities and launder stolen funds. This became very evident in the Philippines particularly since 2023, when the country launched an unprecedented crackdown on Philippines Online Gambling Operators, which in many cases had effectively become front companies for industrial scale scam operations.

Three key factors converged to ultimately enable the rapid rise of China-linked scam syndicated in Southeast Asia starting from around 2006: (1) the growth of Chinese offshore online gambling operations, which the Chinese government was not able to effectively check from 2006 – 2020; this gave rise to the underground banking channels, technologies and consolidated networks that might be redeployed for scams; (2) the willingness of Chinese State Owned Enterprises and a wide range of other Chinese Party State actors to openly cooperate with individuals involved initially in online gambling, but later increasingly also in online scams; by accepting contracts from transnational criminal groups, powerful actors like the China State Construction Bureau Number 4 legitimized the activities of the criminal organizations and deterred moves by Chinese law enforcement to crackdown; (3) the ability of China-linked criminal groups to consolidate relationships with elites in countries that maintained close strategic relationships with China. In places like Laos, Cambodia and Myanmar, the involvement of local elites in legitimizing and openly cooperating with these actors made it less likely that China might crackdown. This is compounded by the fact that Chinese Party State actors implementing various aspects of overseas influence operations also maintain latent networks with many of these same criminal actors, supporting arguments that in some contexts China may engage in geo-criminality as it seeks to advance its strategic interest. Repeatedly, key criminal actors involved in advancing the development of "scam cities" such as She Zhijiang and Deng Pibing consolidated leadership positions especially in provincial business organizations which maintained networks of relationships with Chinese influence operations and a wide range of Chinese Party State actors in across China.

2. THE RISE OF FOREIGNER BUTCHERING: CHINA-LINKED SCAM OPERATIONS GO GLOBAL

On the eve of COVID-19, authorities in China found themselves battling two major sources of capital outflows: (1) continued outflows related to offshore online gambling, which continued to be a major illicit market from the vantagepoint of the PRC government; (2) growing losses to telecommunications fraud and scams being operated across Southeast Asia, in many cases by the same set of actors involved in the offshore online gambling operations. In 2020, with the rise of COVID-19, China took unprecedented actions to call its nationals back from Southeast Asia. This was accomplished using coercive means, including the freezing of bank accounts, seizure of assets back in China or other punitive actions that might it difficult for Chinese nationals to remain in the region. A mass exodus was triggered from scam compounds starting in mid-2020.

In response to these moves, the China-linked criminal groups adapted by globalizing their recruitment pipelines as well as the modalities used to recruit. This included by using more aggressive approaches to lure or traffic remaining Chinese nationals in the region, but also to use similar tactics to target a global population with what is now referred to as the "job scam." By 2022, industrial scale compounds across the region were already engaged in extreme forms of modern slavery and forced criminality, with the number of countries impacted rising rapidly from 66 by late 2023 to 80 by 2025.[2]

As recruitment pipelines globalized, it was only a matter of time before scam activity started to target victims outside of the Chinese speaking world. While some of the earliest non-Chinese victims started to emerge in late 2020, numbers of Western victims increased significantly from 2021 – 2025 as China scaled up its regulatory measures, including: (1) a ban on crypto-currency; (2) the introduction of an anti-scam application which gave Chinese police unprecedented access to monitor online activity of Chinese nationals; (3) the introduction of a "mass prosecution" strategy in China, which involved prosecuting over 338,000 individuals for crimes related to online scams from 2021-2025; (4) the use of the death penalty for some high-profile cases of individuals involved in providing security to or in the operations of industrial scale scam compounds on the direct China border; (5) increased restrictions on social media, which made it increasingly difficult to perpetrate scams on the various platforms that Chinese nationals have access to.

All of these actions resulted in further adaptations on the part of the China-linked scam syndicates. Of these, the most pronounced was a pivot towards "foreigner butchering," or the rise of what might be referred to as "patriotic scam syndicates" which exclusively target non-Chinese victims. By targeting non-Chinese, scam syndicates reduced the risk of being targeted for arrest by the Chinese authorities. Meanwhile, as most foreign countries lacked the awareness of the modalities of the scams, the capacity to investigate, and lacked channels for law enforcement cooperation with Asian countries including China, this meant that they would also not likely be targeted by law enforcement overseas.

As it evolved, patriotic scamming also emerged as a means for the scam syndicates to justify their activities vis-à-vis new recruits, who would be taught that scamming individuals from countries with adversarial relations with China was not a crime, or that it somehow served a Chinese national interest.

For its part, the nature of Chinese law enforcement operations and China's mass prosecution strategy have both functioned to incentivize a pivot towards foreigner butchering. Monitoring of Telegram groups provides some evidence of Chinese police only targeting syndicates that are scamming back in China. While this makes sense from the vantagepoint of Chinese prosecutors, a lack of broader Chinese action will eventually create perceptions in countries with growing numbers of victims that China might even be complicit in such activity. Another major challenge relates to China's blatant disregard for its commitments to international human rights instruments related to human trafficking such as the Palermo Protocol. Chinese courts are increasingly employing a 30-day rule to prosecute individuals lured into scam centers. According to this rule, simply being present in a scam center for 30-days is considered

[2] Author's ongoing tracking; 2025 Trafficking in Persons Report:

sufficient by the court to sentence a defendant in criminal proceedings related to online scamming. This effectively violates the non-punishment principle, leaving many victims of human trafficking re-victimized. In China's competitive job market, this leaves many of these convicted individuals unable to seek legitimate jobs due to having a criminal record. As these individuals have learned how to scam, they often begin to see scamming as a survival strategy. The end result is that since 2023, there has been a growth of "foreigner butchering" operations located across China. While most of these are clandestine, and while the Chinese police are increasingly signaling that they will crackdown on "foreigner butchering" the underlying drivers of this problem persist.

3. CHINA-LINKED CRIMINAL ACTIVITY AND RISING CHINESE SECURITY INFLUENCE

As the "foreigner butchering" crisis spreads across the globe, and as a broader range of countries see their nationals trafficked by China-linked scam syndicates, the Chinese government has sent stronger signals of its desire to provide public security goods relevant to cracking down on online scams and telecommunications fraud. While China should be encouraged to do more to reign in this plague of criminal activity, the current trajectory of China's response raises four key concerns:

(1) Dominance over narratives: one key element of China's response is focused on its domestic audience – demonstrating to the Chinese public that it can keep its population safe from online scams, job scams, trafficking and other forms of fraud. As such, China is increasingly framing its response to what it refers to as "telecommunications fraud" in Southeast Asia as a success story, and an issue area around which China can play a significant role in providing public security goods. This gives rise to several tendencies: one is for China to downplay in its public messaging the fact that the groups behind the "telecommunications fraud" are China-linked crime groups, and that this plague of online scams radiating across Southeast Asia and beyond is just as much, if not more a global China problem as it is a Southeast Asia problem. There is also a tendency towards disinformation campaigns, which attempt to present China only as the solutions rather than as a major part of the problem. This occurs repeatedly around disinformation campaigns that assert that scamming and human trafficking no longer occur along the China-Myanmar border, or that common transit countries like Thailand are not safe for Chinese tourism. In asserting claims, especially like the later, China risks doing significant harm to tourism economies.

(2) China will increasingly consider the issue of online scams in geo-politically important countries within the context of its broader geo-strategic footprint, ultimately undermining efforts to crackdown. The case of Myanmar illustrates such dynamics, where following the Myanmar military 2021 coup, scam syndicates ballooned across the country, resulting in astronomical losses for the Chinese population. As this situation continued to deteriorate in 2023, China increased pressure on the Myanmar military to address the problem. After months of the military ignoring China's demands to crackdown, China turned to support elements of Myanmar's resistance forces to take action, resulting in an unprecedented eradication of scam centers on the Myanmar-China border. By 2024 however, as China observed that

the Myanmar military had become increasingly fragile on both on the battlefield and politically, China shifted away from placing further pressure on the Myanmar military and instead towards providing it with strategic and political support to ensure the security of China's geo-strategic interests in the country. Since this pivot, challenges in Myanmar have continued to evolve, with scam compounds moving increasingly inland away from border regions, just as lighter and more mobile forms of clandestine "jungle scam centers" have started to emerge across the country. Meanwhile, China has largely ignored the efforts of revolutionary actors to get involved in subsequent crackdowns, instead emphasizing in its public statements a strong preference for cooperation with the Myanmar military in addressing the challenges.

(3) China's attempts to frame law enforcement cooperation to address scams within the context of its Global Security Initiative (GSI). While on one level, GSI is a platform through which China aims to scale up its contributions to public security goods, on the other, the platform is of concern for many countries which perceive it as a move to reshape security norms and advance China's global security interests. As such, countries interested in law enforcement cooperation with China may find these associations problematic, and efforts by the PRC to frame cooperation on a very specific emerging non-traditional security threat as part of GSI to be counter-productive.

(4) China's tendencies to maintain monopolies over intelligence related to China-linked scam syndicates: given that these are China-linked crime groups, and given further that China has since 2023 been involved in dismantling major scam hubs along its border through which it seized tens of thousands of devices, China at this point has access to critical intelligence on the scams that would be of great use to countries around the world. However, China has not openly shared this evidence. Instead, it has gone out of its way to prevent authorities involved in facilitating the repatriation of Chinese nationals that have escaped from scam centers from interviewing or gathering data from them. As recent U.S. indictments revealed, one reason why China might be taking this approach is because some of this evidence might implicate Chinese officials complicit in the scam operations. Beyond this though, it is also likely that China will take a transactional approach to sharing such information – meaning that other countries will need to bring something to the table to gain access.

4. THE GLOBAL SPREAD OF CHINA-LINKED SCAM SYNDICATES

Particularly following the U.S. – U.K. joint sanctions and seizures targeting an extensive web of transnational criminal actors and linked front companies and financial institutions in Cambodia last October, and the establishment of the U.S. Strike Force last November, conditions are changing rapidly in the traditional epicenter countries.

In Cambodia, largely due to growing Chinese pressure on state embedded criminal actors occupying positions at the apex of political power in the country, the past three months have seen chaos play out around scam centers across the country, with the Cambodia government

openly claiming that over 200,000 suspected cybercriminals have left the country. This repeats one very concerning trend currently in the region: the complete lack of effective law enforcement campaigns. In countries like Cambodia, Myanmar and Laos, the dominant response to international pressure is to engage in campaign style clearance operations, which enable the vast majority of criminals to get away, while subjecting trafficking victims to even further hardship, as a combination of trafficking groups and corrupt officials exploit them as they attempt to flee compounds. One key reason for this is the fact that these "crackdowns" are led by the very individuals benefiting from and complicit in the scams.
Scam operations are now adapting rapidly in light of these new realities, with some syndicates pivoting to set up lighter more mobilize operations in residential buildings, hotels and resorts, while others move into rural areas. Meanwhile, in Myanmar, scam syndicates are building new layers of elite protection with elites that are based in territories that are more distant from borders and harder to detect from neighboring countries.

Perhaps more concerning is the global expansion of China-linked scam operations that is currently underway. Since 2023, there has been a marked increase in China-linked scam syndicates operating across South Asia, in Africa, and in additional ASEAN countries. There have also been growing reports of them getting involved across the Western Hemisphere, including in Mexico, Chile, and Paraguay. In all of these countries, there are signals that the same patterns of corruption, involvement of Chambers of Commerce and networks connecting into the Chinese Party State are playing out. Increasingly this issue cannot be seen only as a Southeast Asia problem, but needs to be more accurately framed as a global China problem. Meanwhile, there is also a clear convergence across transnational organized criminal groups that is underway, with domestic criminal actors from South Asian and African countries also adopting the same scam methodologies, or in other cases fusing with China-linked criminal groups.

POLICY RECOMMENDATIONS

The global threat stemming from China-linked scam operations continues to evolve as do the forms of scams that are perpetrated from within the scam compounds that are currently expanding to new locations across the globe. Addressing these challenges will require a full of government approach similar to that articulated in the draft Dismantling Foreign Scam Syndicates Act. To enhance further its response to these challenges, the U.S. should consider the following:

(1) The U.S. should breakdown China's intelligence monopoly over online scams by establishing a global operations center, and partnering with frontline states to access devices deployed in scams. This will provide the U.S. with the intelligence needed to approach China from a position of strength on these issues. In this regard, establishing strong partnerships with frontline countries such as the Philippines, Thailand, Vietnam, Sri Lanka, and the United Arab Emirates will be critical.

(2) The U.S. should partner with key allies that are seriously impacted by China-linked scam syndicates to develop training modules, to invest in frontline response to trafficking for forced criminality, and to highlight the advantages of democratic institutions and civil society when it comes to address the root causes of this plague of criminality. Such moves are critical also as China increases its own moves to gain access internationally

for its own law enforcement and as it attempts to maintain its dominance over narratives and intelligence flows around online scams.

(3) The U.S. should directly engage China on these issues, and push for China to share intelligence related to American victims; in return the U.S. might offer to share U.S. intelligence on illicit financial flows that might link to Chinese victims or which might illustrate the various tools that China-linked crime groups are utilizing to move illicit funds out of China. The U.S. should also coordinate efforts with China insofar as China is willing to delink its response from platforms such as the Global Security Initiative.

(4) Follow the money: China-linked money laundering operations have scaled to a point that they now represent the most significant channels for illicit financial flows. Most of these operations are being conducted in a very public way, particularly on platforms like Telegram, which numerous of "payment guarantee" platforms boast memberships in excess of 100,000 people. Decentralized crypto-currency platforms and technologies have emerged as a major threat to global financial systems, and represent the main tools that these China-linked money laundering syndicates leverage to facilitate illicit flows. The U.S. has recently started taking action on Telegram channels being used for malign purposes. These forms of actions need to go to scale, and should target especially these illicit financial operations.

(5) In the case of Myanmar, the situation remains dire as scam centers continue to spread like wild-fire in the Myanmar military's control areas and beyond. To present, the most impactful actions taken to counter scam centers in the country have been implemented by non-state governance actors. Most recently, one of the leading pro-democracy governance actors in the country, the Karen National Union (KNU) seized a large-scale scam center which it demobilized, systematically collecting evidence. This evidence was eventually shared internationally, and has directly helped the United States and Thailand indict and ultimately arrest two senior compound managers. The KNU also went out of its way to invite international media into the seized scam compound to educate a global public regarding the threats emanating from inside. The KNU has by all measures outperformed the Myanmar military and the Cambodian authorities, and could potentially emerge as a key governance actors in dismantling and eradicating scam centers in Myanmar. Given the special circumstances of the country, the U.S. should consider providing robust support to pro-democracy groups like the KNU to continue this response and to build across the country the capacity needed to replicate what the KNU has completed since November of 2025.