JOURNAL
OF
ACADEMICS STAND AGAINST POVERTY
e-ISSN 2690-3458 ISSN 2690-3431
Volume 6, 2025: pages 43-69
Research Paper

Cybercrimes and the illicit financial flows in Myanmar

Thant Thura Zan[1] & Soe Thaw Tar Kyaw Min[2]

[1] Graduate School of Global Environmental Studies, Kyoto University, Kyoto, Japan. ORCID: 0009-0002-4837-9649
Email: *thantthurazan@gmail.com*
[2] Eberswalde University for Sustainable Development, Eberswalde, Germany, ORCID: 0009-0008-6776-2751
Email: *sttk.min@gmail.com*

Abstract: The rapid expansion of online gambling in Southeast Asia has created an alluring yet deceptive environment, promising financial gain while fostering fraudulent activities and illicit financial flows. This study explores the intersection of online fraudulent gambling and transnational organized crime in Southeast Asia, with a particular focus on Myanmar. Criminal syndicates exploit regulatory loopholes and weak enforcement to orchestrate scams, including rigged games, catfishing schemes, and human trafficking. The anonymity of digital platforms enables large-scale fraud, such as the "pig-butchering" scam, which inflicts severe financial and psychological harm on victims. Beyond individual losses, online scams fuel money laundering, economic destabilization, and corruption, while exacerbating social problems like addiction, debt, and family breakdown. Vulnerable groups, including the young, elderly, and low-income populations, are disproportionately affected, but even wealthy individuals from the West are targeted. Myanmar's ongoing political instability has further enabled these illicit operations, allowing criminal networks to exploit weakened regulatory structures and facilitate money laundering linked to arms and resource smuggling. This research underscores the urgent need for national, regional, and global cooperation to strengthen regulatory frameworks, enhance enforcement mechanisms, and mitigate the growing threat of online gambling-related crime in Myanmar and Southeast Asia.

Keywords:

1. Cybercrimes
2. Transnational crime
3. Money laundering
4. Myanmar

2025 Journal ASAP

DOI: 10.5281/zenodo.15467435

Received 17 November 2024
Revised 11 May 2025
Accepted 12 May 2025
Available online 19 May 2025

1. Overview of online fraud and illicit financial flows in Southeast Asia

Southeast Asia has emerged as a fertile ground for transnational organized crime, with fake online casinos serving as a pivotal nexus for illicit activities (Lusthaus, 2020; OHCHR, 2023; UNODC, 2020). This region's unique blend of economic disparities, and porous borders has

created a conducive environment for criminal networks to flourish. Especially, the rapid advancement of digital technology, coupled with increasing internet penetration, has facilitated the rise of online fraudulent activities (Jackson, 2024; Leo, 2024). Access to affordable smartphones and widespread internet connectivity has expanded the reach of these scams, allowing criminals to target a broader audience. The intricate interplay between these factors has resulted in a complex ecosystem where online scamming, fraud, and illicit financial flows are endemic.

Online scamming and fraud are closely intertwined with fake casinos (Kennedy & Southern, 2022; UNODC, 2024). These platforms serve as a front for a variety of criminal activities. By enticing victims to deposit funds, these operations generate substantial revenue, which is subsequently laundered through complex financial networks. The anonymity afforded by the digital realm allows perpetrators to operate with impunity, making it challenging for law enforcement agencies to disrupt their activities. These scams often involve sophisticated social engineering tactics, where perpetrators build trust with victims before defrauding them (Leo, 2024).

The operations behind these fake online casinos are typically orchestrated by transnational organized crime syndicates. These groups possess the resources, expertise, and connections to establish complex networks that span multiple countries. They often collaborate with corrupt officials to facilitate their activities and evade law enforcement. The decentralized nature of these syndicates makes it difficult to dismantle them, as they can easily adapt to changing circumstances and relocate their operations.

Illicit financial flows are a critical component of this criminal ecosystem. The proceeds of online scams and fraud are funneled through a labyrinth of financial institutions to obscure their origins. These funds are often used to finance other criminal activity, such as drug trafficking and human smuggling. The lack of robust anti-money laundering measures in some Southeast Asian countries has exacerbated the problem, allowing criminals to launder their illicit gains with relative ease. According to a report by the United States Institute of Peace, criminal organizations in Cambodia, Laos, and Myanmar are allegedly siphoning off about USD 43.8 billion annually through scams. There are over 300,000 people involved in these horrific activities (Walker, 2024).

These transnational criminal networks are centered in countries such as Myanmar, Thailand, Laos, Vietnam, and with significant influence extending into and from China, exploiting these nations' complex socio-economic and political landscapes (USIP, 2024). Money laundering has become a common tactic in the Chinese real estate market, where criminals exploit complex ownership arrangements and high-value deals to funnel illicit funds into the legitimate economy (Hogan, 2024). The convergence of online scamming, fraud, and illicit financial flows poses a significant challenge to the region's security and economic prosperity. Even not anymore on a national and regional level, it has become a global threat (USIP, 2024).

To illustrate the complex workings of these criminal networks, the consequences of their activities, and the responses required, this essay will use Myanmar as a critical case study. Myanmar's unique socio-economic context, political instability, and weak regulatory environment provide a detailed account of how transnational organized crime syndicates operate fake online casinos. By examining specific instances of fraud, the methods used for money laundering, the impact, driving forces and responses, we can better understand the broader implications for Southeast Asia. This case study will also highlight the necessary steps forward to mitigate these illicit activities.

2. Background of the study country: Myanmar

A brief profile of Myanmar is provided here to offer context. Myanmar, the second-largest country in Southeast Asia, occupies a distinctive geographical position. The country borders China, Laos, Thailand, Bangladesh, and India. Myanmar's location at the crossroads of South and Southeast Asia has endowed it with a strategic importance. Its extensive coastline provides access to vital sea lanes, while its land borders facilitate connectivity with neighboring countries. This geopolitical position has made Myanmar a historical crossroads for trade, cultural exchange, and, at times, geopolitical competition.

Myanmar's political landscape has been characterized by a tumultuous interplay of military rule and democratic aspirations (Vakulchuk et al., 2018). Since gaining independence from British colonial rule in 1948, the country has endured a complex journey marked by periods of relative stability and prolonged periods of authoritarianism.

A military coup in 1962 ushered in a protracted era of military dictatorship under General Ne Win. This period was characterized by economic mismanagement, isolationism, and widespread human rights abuses. The regime's policies fueled growing discontent among the population, culminating in mass protests in 1988 (Devi, 2014). While these demonstrations were brutally suppressed, they marked a turning point, leading to the formation of the National League for Democracy (NLD) under the leadership of Aung San Suu Kyi.

The NLD's landslide victory in the 1990 elections was annulled by the military, and Suu Kyi was placed under house arrest. Despite international pressure and sanctions, the junta maintained its grip on power for several more years. A gradual process of political liberalization began in 2011, with the formation of a nominally civilian government. However, the military retained significant control over the state, and the 2015 elections, which saw another NLD victory, failed to deliver substantive democratic reforms, including addressing the ongoing Rohingya issues (Akins, 2018).

The fragile democratic gains which fostered a moment of prosperity were shattered by a military coup in February 2021, plunging the country back into turmoil. The junta's crackdown on dissent, widespread protests, and the emergence of armed resistance groups have exacerbated the crisis. The situation remains volatile, with the military facing growing opposition domestically (Jordt et al., 2021).

2.1. How Myanmar became the hub of Kyar Phyant

Myanmar's porous borders with China and Thailand, coupled with internal political instability, have created a fertile ground for illicit activities, particularly online gambling, known locally as "Kyar Phyant," and associated financial crimes in recent decades (ISP Myanmar, 2024). Following the 2021 military coup, the State Administration Council (SAC) lost control over parts of the country, allowing scam syndicates like Kyar Phyant to operate freely in regions controlled by ethnic armed groups and border guard forces. These groups provide protection in exchange for financial payments, turning scam compounds into semi-autonomous zones.

Additionally, Myanmar’s proximity to China and Thailand makes it an ideal base for cyber fraud targeting Chinese citizens, while corrupt officials and limited international oversight enable these operations to flourish. Most recently, during 2023, these Kyar Phyant are moving to Yangon, the commercial city of Myanmar and the central city of upper Myanmar, Mandalay, flaunting their audacity by spreading their shadows to urban centers as if brazenly challenging the laws and orders. (Irrawaddy, 2024b).

2.2. What is Kyar Phyant?

The term "Kyar Phyant" is a Burmese transliteration of the Chinese term "诈骗" (zhà piàn), which directly translates to "fraud" or "scam" (ISP Myanmar, 2024). While the term originally denoted a broader spectrum of deceptive practices, it has become synonymous with the burgeoning fraudulent online gambling industry and its associated criminal activities in Myanmar.

Kyar Phyants headquarters thrive in border areas with weak regulatory frameworks and armed group control. These operations often involve criminal syndicates and rely on human trafficking for labor. The ill-gotten gains are then laundered through a network of informal money changers, real estate investments, and cryptocurrency, creating significant illicit financial flows.

2.3. Illicit activities along the Myanmar-China border

The Myanmar-China border is a hotspot for various illicit activities. The criminal groups originally emerged from the Cambodia-Thai border region, where they were predominantly involved in the gambling industry. However, following the Cambodian government's decision to shut down casinos in this area between late 2017 and 2018, these groups relocated their operations (Thul, 2019). They migrated to various regions in Myanmar, including Myawaddy, Shwe Kokko, KK Park, Laukkai, Chin Shwe Hao, Pan San, and Mong Phyak where they continued their illicit activities (ISP Myanmar, 2024).

Cross-Border gambling and criminal activities in Laukkai

Laukkai, a city in northern Shan State, is widely recognized as the gambling capital of the Kokang Autonomous Region, which shares a border with China's Yunnan Province (Fishbein & Lusan, 2024). Laukkao serves as the headquarters of the Kokang Autonomous Region, which is jointly controlled by the Myanmar military (Tatmadaw in Burmese term) and Kokang military.

The Myanmar military's regional command headquarters (DSK)[1] is stationed in Laukkai. Unlike the other major cities in Myanmar, where any form of gambling is considered illegal, the Kokang region is full of casinos (Fishbein & Lusan, 2024). With the money flowing through casinos and associated businesses, Kokang has developed modern infrastructure, including buildings, roads, and electricity, where the highest administrative organization is the Kokang Autonomous Region Management Committee.

Although the Myanmar military holds some power in Laukkai, permission to open a casino is not solely granted by the military or the Ministry of Hotel and Tourism; it must also be obtained from the Kokang Autonomous Region Management Committee. Thus, Kokang became a border city where Chinese nationals as well as Chinese residents of Myanmar go to indulge in gambling activities. Moreover, due to the lack of workers in Laukkai, where the casinos host a great number of Chinese visitors, gambling halls and hotels are recruiting and training poker workers. In this way, it has become a situation that creates opportunities to open casinos. These casinos include both legitimate and fake establishments.

The fake ones are often set up to deceive victims and evade regulatory scrutiny, typically operating under the guise of legitimate businesses while engaging in fraudulent practices. Due to this situation, young people from regional countries such as Cambodia, Laos, Thailand, and

[1] The Myanmar military has 14 regional command headquarters, referred to as "Da Sa Ka" in Burmese term. Each of these regional commands oversees military operations within its designated area in Myanmar.

Vietnam, including Myanmar young people from cities like Yangon, Mandalay and Lashio, have been lured to work in online scams that have emerged with the development of Laukkai gambling. Victims of these scams hail from various countries, including the United States, the United Kingdom, and Australia, often being deceived with promises of substantial financial returns or false romantic relationships (Clapp, 2024).

Prominent groups, such as the Wa State Army and the Kokang Group, are heavily involved in cross-border smuggling and online scam activities (Irrawaddy, 2023). Online scam syndicates operating in Kokang are primarily controlled by “the Big Four”, the richest and most powerful families in the Kokang Autonomous Region linked to Myanmar’s military (Irrawaddy, 2024a).

The rise in power and wealth of the Bai, Ming, Wei, and Liao families can be traced back to the 2009 Kokang conflict. During this conflict, the Burmese army clashed with the Phun family, the very first ruling family of the region, led by followers of Kokang ruler Phun Ndushin. Unlike Phun Ndushin, Bai Suocheng and Ming Shochin chose to align themselves with the Myanmar army, operating under its protection. According to the Global Times, the Kokang business community estimates that the annual revenue generated by the casinos owned by these four families could reach up to 10 million yuan (USD 1.4 million).

Residents and workers in Laukkai report that both the four families and the Myanmar military have been aggressively promoting the Kyar Phyant in the city. All these families have strong interest ties with the Myanmar Military. Bai Suocheng, Ming Sheok Chin, Yang Song, and Liao Da Pao have solidified their influence in Kokang by strategically positioning their descendants in various armed and political roles. In the 2010 election, Bai Suocheng was elected as a member of parliament as a candidate represented by the Union Solidarity and Development Party (USDP) and became the chairman of Kokang Autonomous Region. Ming Xue-Chang became the provincial representative of Laukkai and became the head member of Kokang Autonomous Region. Yang Song of the Wei House became Colonel Wei San of the No. 1006 Border Guard Force. Corruption among local government officials in Myanmar and China further enables these illicit activities, with specific officials and departments, including factions of the Myanmar Military and local police in Yunnan Province, China, being implicated.

Thus, the Chinese government has been paying special attention to the involvement of Chinese citizens in online money laundering gangs based on the China-Myanmar border. At the end of 2023, in the meeting between Chinese government officials and Myanmar military officials, the issues of Kyar Phyant were among the topics discussed (Zhou, 2023). Although the officials have met and discussed with each other several times, the Myanmar military side has not been able to catch the online money fraud gangs wanted by the Chinese.

However, along with China's crackdown on online money fraud gangs, family members from Ming House, Wei House and Liao House were arrested after being invited to a trade fair in China on October 1, 2023. Ming Xue-chang, Ming Guoping, Ming Julan, and Ming Zhenzhen are the principal figures behind the Kyar Phyant in northern Myanmar. The founder of the Kokang region’s Border Guard Force, who has received backing from Myanmar’s military regime, has been identified by Chinese authorities as the 'main suspect' in cybercrimes occurring in the region. Thus, an arrest warrant was issued on other senior figures allegedly involved in online scams.

Meanwhile on October 27, 2023, The Three Brothers Alliance consisted of the Rakhine Army, the Myanmar National Democratic Alliance Army, and the Taung National Liberation Army issued a joint statement on the launch of Operation 1027 to control the growing online money laundering gangs in the northeastern China-Myanmar border region and suppress the Myanmar military and subordinate militias involved (Crisis Group Asia, 2024). In 2023, after the suppression of money laundering gangs in the Wa region controlled by the Wa State Army and

Operation 1027 in the Kokang region, the money laundering gangs from northern Shan State moved en masse to the Tachilek area.

In the period of October, November and December 2023, the traffic congestion in Tachilek increased by 3-4 times due to the influx of people related to money laundering gangs. In Tachilek City, a large wall was built on the land that was previously used as a Covid-19 center, and hundreds of people and gangs of money-grubbers came in droves. In addition, within the vast acres of land owned by the ethnic armed forces and militias, Chinese people have been working on a large scale by building money laundering gangs and buildings. The Myanmar-China border remains a critical area for combating online fraud, scamming, and illicit financial flows. Although significant progress was made in 2023 and 2024, continuous efforts are needed to address the evolving nature of these crimes.

2.4. Illicit activities along the Thailand-Myanmar border

The Thailand-Myanmar border is home to several organized crime groups deeply entrenched in online fraud, scamming, and other illicit activities. The Shwe Kokko New City and KK Park are particularly notorious for their involvement in money laundering and other financial crimes. Situated on the banks of the Thaung River and just 10 miles north of the Myawaddy commercial zone, Shwe Kokko has become infamous for harboring hundreds of online fraud gangs.

Cross-Border gambling and criminal activities in Shwe Kokko

Following the Tatmadaw-affiliated Border Guard Force's (BGF)/ Karen National Army (KNA) takeover of the Shwe Kokko region, business opportunities surged, leading to the controversial Yatai New City project, a joint venture between the Chinese investment group Yatai International and the Karen BGF's Chit Lin Myain Company. In February 2017, a joint venture was established between She Zhijiang and the BGF, creating the Myanmar Yatai International Holding Group Company Limited (Myanmar Yatai) to spearhead the development of the "Yatai New City" project in Shwe Kokko. The project is directed by Saw Min Min Oo on behalf of the Karen BGF/KNA, with the Chinese consortium holding a 70 percent stake and BGF's Chilin Myain Company holding 30 percent. The consortium invested approximately 15 billion USD in the project, which also secured a Myanmar Investment Commission permit in 2018 under She Zhijiang's Cambodian alias, Tang Kriang Kai. The permit allowed for an initial investment of 22.5 million USD for the construction, operation, and leasing of high-end villas (FRONTIER, 2022; Justice for Myanmar, 2024).

Shwe Kokko is not a development zone but a shadow hub for cyber scams and illegal online gambling operations, with Myanmar Yatai profiting from these illicit businesses. The BGF/KNA benefits from these activities through various revenue streams, including taxing businesses and workers in the area. The BGF/KNA reportedly imposes a 10% tax on businesses, alongside a one-time fee of 8,890 Thai Baht (USD 264) for new workers, who are also charged a monthly fee. After rebranding as the KNA, the monthly tax on workers was increased from 1,000 Thai Baht to 2000 (USD 59), according to a Yatai notice on Telegram (Justice for Myanmar, 2024).

According to interviews conducted by the FRONTIER (2023a) with two workers in Shwe Kokko's cyber scam operations, all employees must undergo an interview with Yatai before being approved to apply at scam centers. These centers have become notorious for their illicit activities, including the widespread availability and use of drugs. Victims of scams originating from Shwe Kokko, many of whom have been sold or tortured, have been reported in over 30 countries. International governments and news outlets have raised alarms, with particular concern from China, India, Indonesia, Malaysia, Thailand, and the United States due to the

involvement of individuals sought by these countries (ANN, 2022; Hunt, 2024; Irrawaddy, 2022, 2023; Naing, 2023; RFA, 2024).

Cross-Border gambling and criminal activities in KK Park

The project known as Huanya International City, located in the Karen National Union (KNU) Brigade (6) area south of Myawaddy city has been rebranded as KK Park. The groundbreaking ceremony for KK Park took place on February 10, 2020, involving Mu La Ei Ahlin and Trans-Asia International Holding Group (Thailand) Co., Ltd. A banner at the ceremony read: "KNU – Huanya Cooperative Signature and Foundation Stone Laying Ceremony, suggesting direct involvement by the ethnic armed group. Pado Saw Roja Khin, a KNU Central Executive Committee member and Head of the Department of Defense, personally attended and signed the ceremony (Justice for Myanmar, 2024).

Mu La Ei Ahlin, a company registered in Myanmar's Mon State, partnered with Trans-Asia, which is registered in Hong Kong and is reportedly a subsidiary of Huanya International Holdings Group. Despite initial claims that Mu La Ei Ahlin withdrew from the project in 2022, and was replaced by TrustStar Co., Ltd., there are allegations that this was merely a facade. According to a source within the Border Guard Force (BGF), the two companies are closely linked, with their managers having a close relationship. The source suggested that the KK Park project shares similarities with the controversial Shwe Kokko development, with Huanya remaining the driving force behind Trans Asia (FRONTIER, 2023b; Justice for Myanmar, 2024).

KK Park comprises casinos, hotels, restaurants, and nightclubs. However, these establishments have been implicated in financial scams, human trafficking, forced labor, and even the torture and killing of those who refuse to comply with the fraudulent activities. The Kyar Phyant operating within KK Park has been accused of violently punishing individuals who resist, including cutting off food supplies and committing murders. In just two years of operation, KK Park has become notorious for its involvement in human trafficking, online financial fraud, forced labor, and the trade of human body parts (Kennedy & Southern, 2022). Victims forced into Kyar Phyant are coerced into conducting online fraud, with the proceeds being funneled into KK Park's private cryptocurrency digital wallets. These funds are then transferred to digital wallets controlled by Chinese mafia networks, with one such wallet reportedly created by Wang Yi Cheng, a Chinese businessman based in Thailand. Wang Yi Cheng, is the Vice President of the Thai-Asia Economic Exchange, a Thailand-China Friendship Association. His role in facilitating these fraudulent activities highlights the deep connections between the criminal networks operating within KK Park and influential figures in the region and he has allegedly received over USD 10 million for his involvement (Justice for Myanmar, 2024). Thus, the project has become a significant hub for illicit activities, operating under the guise of legitimate business development.

Key actors of illicit activities at the China-Myanmar and Thailand-Myanmar borders**,** several organized crime groups and businesses are heavily involved in online fraud, scamming, and illicit financial flows.

2.5. Analysis of border city cases along the China-Myanmar and Thailand-Myanmar frontiers

Building on the contextual understanding of Myanmar's border dynamics, this section shifts focus to a systematic analysis of cyber scam operations proliferating along the China-Myanmar and Thailand-Myanmar borders. Unlike the previous studies, which provided historical and geopolitical context, this analysis employs a stakeholder mapping framework specifically the

Interest-Influence Matrix (Parmar et al., 2010) to identify and assess the key actors involved in these illicit economies.

The stakeholders are gathered through 40 news articles, Facebook posts and web articles published before and during 2024. Notable actors and words associated with cyber scams are shown in Figure 1 and Figure 2.

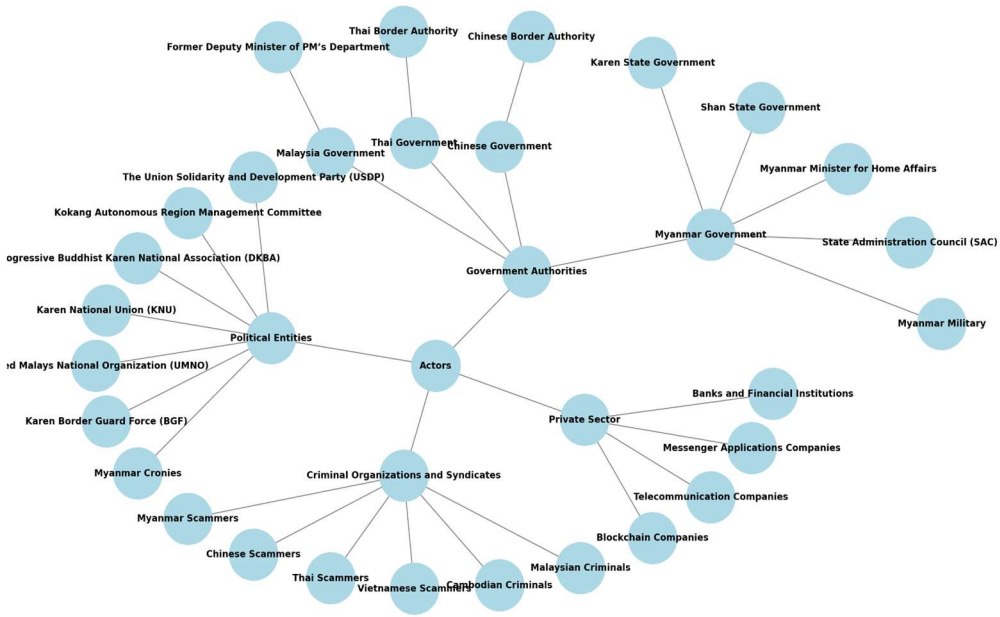


Figure 1. Key actors involved in illicit online scam activities at the Myanmar borders
Source: Authors, 2024 based on the collected 39 gray literatures.

Figure 2. Word cloud of the most frequently found words regarding the cyber scams
Source: Authors, 2024 based on the collected 39 gray literatures.

The stakeholder mapping of Myanmar's cyber scam industry highlights the key actors based on their influence over and interest in the issue. Influence refers to a stakeholder's power to control or disrupt scam operations, while interest reflects their level of involvement or impact. This classification results in four distinct groups: key players, influencers, affected parties, and bystanders.

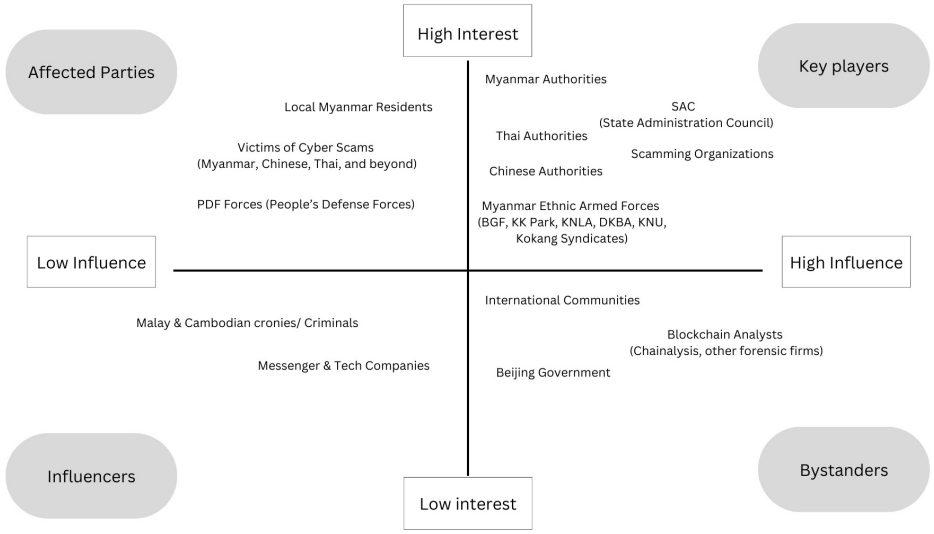


Figure 3. Interest-Influence matrix of scams key players
Source: Authors, 2024, own complication

Key Players (High Influence, High Interest) – These are the most influential and influential people who control, govern, or profit from the scam industry. The State Administration Council (SAC) which is the military government of Myanmar, Chinese officials, and Thai authorities either regulate, safeguard, or try to stop scams. Kyar Phyant and other scam syndicates operate in this area, exploiting lawless border areas. Myanmar ethnic armed organizations (EAOs) and/or SAC benefit from backing those con groups.

Influencers (High Influence, Low Interest) – The scam problem in Myanmar may not be a top priority for these actors, but they do have the ability to act. This includes Chinese authorities, international communities (U.S. authorities, international law enforcement (Interpol), etc.), and financial institutions that monitor money laundering. Although they may step in during well-publicized cases, they don't always commit resources to addressing the underlying issues.

Affected Parties (Low Influence, High Interest) – Although they cannot alter the situation, these are the people who suffer the most. Scam victims throughout Asia (and beyond), local Myanmar residents, People's defense forces (PDF) caught in conflict, and trafficked scam workers are all included in this category. They have little power to halt the operations, despite their intense concerns.

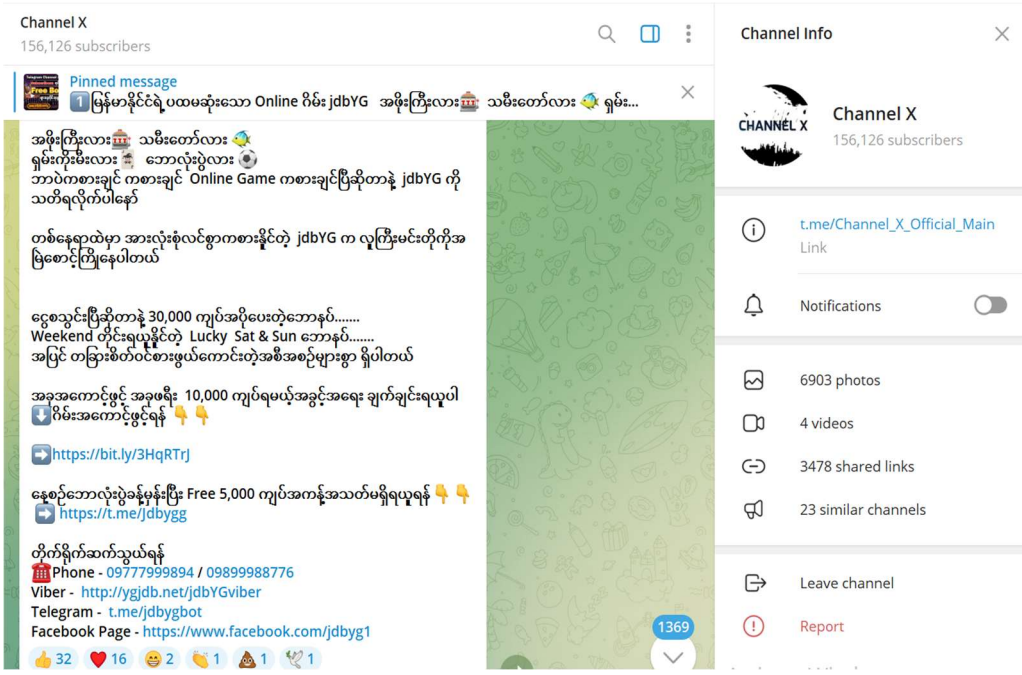
Bystanders (Low Influence, Low Interest) - These stakeholders are neither significantly impacted by nor have significant influence over the scam industry. This includes Vietnamese scammers who operate within the ecosystem but lack significant power in Myanmar, criminal organizations from Cambodia and Malay countries (who support scams but have little influence), and messaging apps (sometimes unknowingly helping scams but taking a long time to step in who do not have a major role but may indirectly support operations).

3. Scamming tactics

3.1. Social media exploitation

Kyar Phyant mainly uses two online medium platforms to find their targets. They are Facebook and Telegram. With over 18.8 million Facebook users in Myanmar as of February 2023, accounting for 33.1% of the population[2], Facebook has become a primary platform for online scammers. These groups often create multiple pages dedicated to sharing short, viral videos, dark humor, or trending content to attract followers. Embedded within these videos or in the comment sections of popular posts, scammers insert advertisements for online casinos featuring games like slots, fishing, and poker. These ads direct users to fraudulent websites designed to trap them into gambling schemes.

Since the military crackdown on social media in 2021, Telegram has gained significant traction in Myanmar[3]. Scammers exploit this platform by infiltrating or creating entertainment-focused Telegram groups. These groups often share free Hollywood and Bollywood movies, including adult content, to attract users. Some groups even charge entrance fees. Within these groups, scammers promote their fraudulent gambling sites, enticing users to play games that are rigged against them. Once a user engages, the scammers hack their personal information through malicious links. If the victim stops playing the games, the scammers threaten to contact the victim's family, friends, and colleagues, whose contact details they have already accessed. Some sample Facebook pages, groups and Telegram groups are shown (Figure 4).



[2] Number of Facebook user in Myanmar see at https://napoleoncat.com/stats/facebook-users-in-myanmar/2024/02/
[3] About Telegram application in Myanmar https://insightmyanmar.org/all-about-burma/2022/8/29/telegram-in-burmese-language

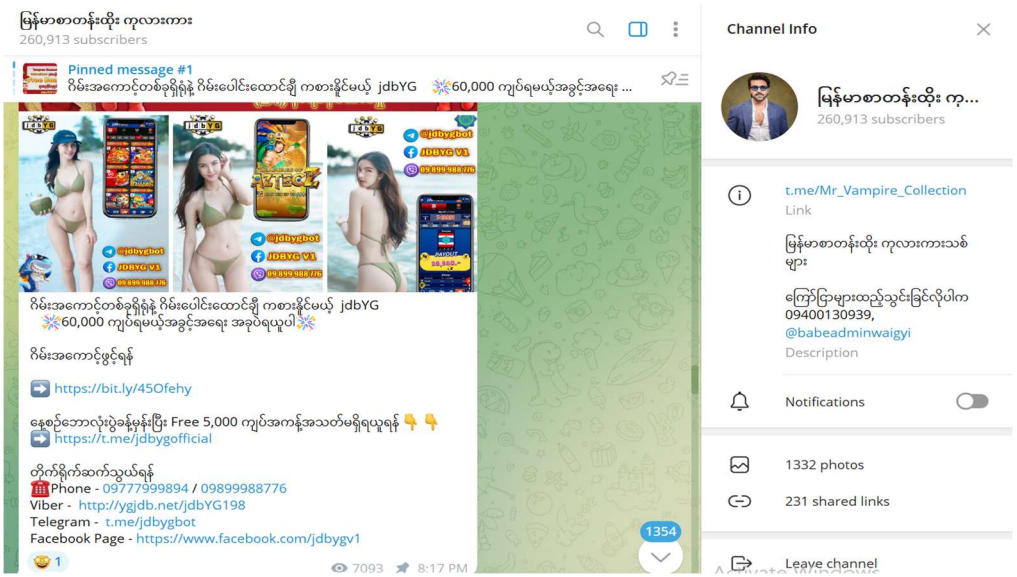


Figure 4. Screenshots of some scam's advertisements in telegram groups in Myanmar
Source: Authors, 2024.

3.2. Romance scams

Scammers create fake online personas on social media or dating platforms to target individuals seeking romantic relationships. They invest time in building trust, often fabricating elaborate backstories. Once they have gained the victim's confidence, they begin requesting money, citing various emergencies such as medical bills or travel expenses. These scams are emotionally manipulative and often result in significant financial losses for the victims. Sometimes they appear in the form of call centre scams.

3.3. Phishing links

Another common tactic is posting malicious links in the comments of popular Facebook posts or within widely shared content. When a user clicks on these links, scammers gain access to their personal information, including contact lists and financial data. Initially, scammers may demand a small amount of money, promising not to harm the victim if paid. However, these demands typically escalate over time. If the victim refuses to pay, the scammers resort to harassment, making threatening phone calls to the victim's contacts and causing further distress.

3.4 Job scams

Scammers also exploit the desperate search for employment by creating Facebook groups that advertise job opportunities. Some of these ads explicitly state that the job involves working for online fraud operations, while others lure applicants with promises of unusually high salaries without revealing the nature of the work. Many job seekers, drawn by the potential earnings, unknowingly become involved in these illegal activities, further perpetuating the cycle of online scams and fraud.

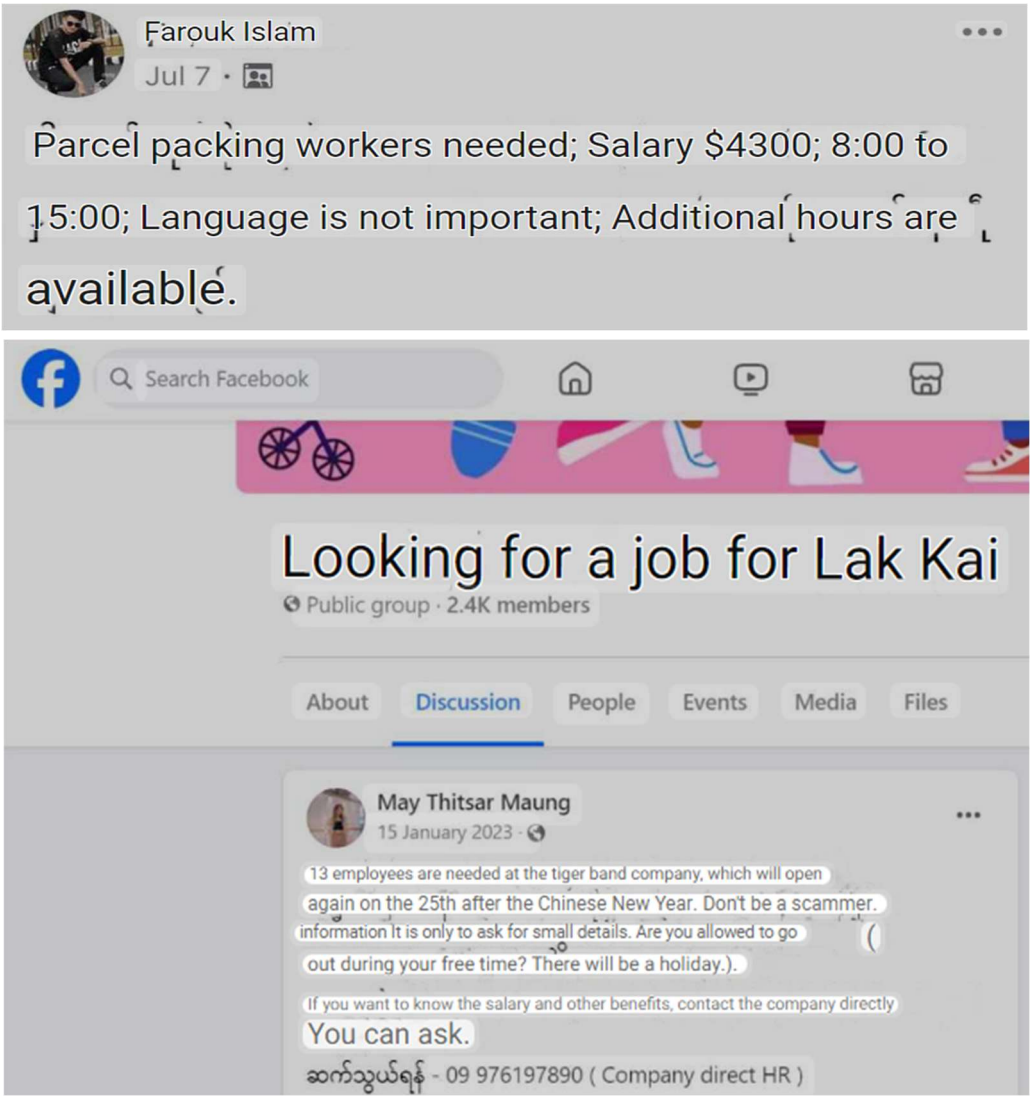


Figure 5. Screenshots and Google translation of some samples of the job scams.
Source: Authors, 2024.

4. Magnitude of Illicit financial flows and action taken against the Kyar Phyant

At both borders, substantial sums of money are involved in illicit financial flows, though exact amounts are difficult to estimate. However, on a global scale, Southeast Asian online scamming gangs stole 75 billion USD in 2020-2024, highlighting the pervasive nature of these illicit activities (Faux, 2024).

Various reports suggest that billions of dollars are siphoned off annually through these operations. For instance, a single Chinese company based in KK Park in eastern Myanmar has swindled over USD 100 million from victims through cryptocurrency scams over the past two years, according to a report by blockchain analytics firm Chainalysis and the US anti-slavery group International Justice Mission (IJM). The analysis found that Tether, a major

cryptocurrency, was used for these scams, with over USD 100 million funneled into two digital wallets linked to the company (Chipolina, 2024).

Other reports indicate that the value of online fraud in Thailand alone reached 110 million baht (USD 3 million) per day in April 2023 (Tortermvasana, 2024). Kyar Phyant scammed USD 4 billion from American citizens in 2023, marking a 53% increase from the previous year (Rebane & Watson, 2024). This group's activities also benefited the Border Guard Force (BGF) in Myanmar by USD 7 million (Tower & Clapp, 2020).

Illicit activities extend beyond financial scams, encompassing severe human trafficking and forced labor. The USIP estimates the number of scammers who have been coerced into labor through online scams at approximately 100,000 in Myanmar, 120,000 in Cambodia, and 85,000 in Laos (USIP, 2024).

Authorities have made substantial progress in arresting and deporting those involved in online fraud. Over 51,000 Chinese nationals were transferred from Myanmar to China as part of Operation 1027 between 2023 and 2024[4]. Some were arrested, along with the seizure of 900 phones and other materials used in fraudulent schemes[5]. Specific efforts, such as "The Purge Operation," resulted in 26 arrest warrants and the capture of four key suspects linked to scamming activities[6]. In addition, Thailand's Anti-Money Laundering Office (AMLO) ordered the seizure and freezing of assets valued at 600 million baht (approximately USD 16.3 million)[7]. China also supported Myanmar's junta police force with a 5-million-yuan (around USD 690,000) investment to eradicate online scams and human trafficking[8].

5. Driving factors of the Kyar Phyant

This section shows the deeper structural and systemic drivers that enable the rise of networks like Kyar Phyant syndicates. These criminal ecosystems do not emerge in a vacuum. They are products of intersecting economic, political, technological, and social vulnerabilities. The following subsections examine the key enablers of this phenomenon, from entrenched poverty and widespread corruption to digital platforms, regulatory loopholes, and the global operations of transnational crime networks.

5.1. Economic disparities

In regions where the gap between the rich and the poor is wide, and economic opportunities are scarce, individuals may feel compelled to engage in illicit activities as a means of survival. As Myanmar is a least developed country and country of conflict, economic desperation often leads to the proliferation of scams, fraud, and other illegal ventures as people seek quick financial gains.

The lack of social safety nets and limited access to legitimate employment can further exacerbate the situation, driving more people towards these activities. Areas with weak

[4] https://english.news.cn/20240821/e518a7c8181a4944a496cdb8f4f42dcc/c.html

[5] Myanmar Junta Hails Chinese Scammer Arrests (irrawaddy.com)

[6] Thai Police Crack Down on Transnational Criminals in “The Purge” Operation, Seize Assets Worth Over 250 Million Baht https://thepattayanews.com/2024/04/18/thai-police-crack-down-on-transnational-criminals-in-the-purge-operation-seize-assets-worth-over-250-million-baht/

[7] Thai Police Seize 80 million Baht in Cash Sent to Myawaddy by Scammers (khaosodenglish.com)

[8] China Hands Medal and 5m Yuan to Myanmar Junta for Border Crackdown https://www.irrawaddy.com/news/myanmar-china-watch/china-hands-medal-and-5m-yuan-to-myanmar-junta-for-border-crackdown.html

financial regulations or entirely unregulated markets become hotspots for illicit financial flows and scams. In such environments, criminals can easily manipulate the system to their advantage. The absence of stringent oversight and regulatory frameworks allows illegal activities to flourish, as there are few deterrents to criminal behavior. These unregulated markets also attract international criminal networks that exploit local vulnerabilities to launder money or conduct fraud on a global scale.

5.2. Corruption and weak governance

Corruption is a significant enabler of illicit activities, particularly in regions where law enforcement and regulatory agencies are compromised. When officials are bribed or coerced into turning a blind eye to illegal activities, it creates an environment where criminals can operate with minimal fear of prosecution. Corruption can permeate various levels of government, from local police forces to national regulatory bodies, further undermining efforts to combat transnational crimes. As seen in the above, many levels of Myanmar officials are involved in these corrupt practices, exacerbating the problem, and making it more difficult to address illicit activities effectively. Law enforcement agencies that are under-resourced, poorly trained, or lacking in technological capabilities are often ill-equipped to tackle sophisticated criminal networks. These agencies may struggle to enforce laws, investigate crimes, or prosecute offenders, allowing criminal activities to continue unchecked. The lack of effective law enforcement also emboldens criminals, who perceive a low risk of being caught or punished for their actions.

5.3. Political instability

Regions affected by political instability or armed conflict often experience a breakdown in governance and law enforcement, creating a fertile ground for criminal activities. In these areas, the absence of a stable government can lead to a surge in illicit activities such as online scams, human trafficking, and illegal trade. Myanmar, as a country experiencing ongoing conflict, exemplifies how conflict zones attract transnational criminal networks that exploit the chaos to expand their operations.

5.4. Technological advances

The rapid growth of digital platforms e.g., Telegram application, WhatsApp application, Facebook, and internet technologies e.g., Starlink has revolutionized the way crimes are committed, particularly in the realm of online fraud and scams. The internet provides criminals with a global reach, allowing them to target victims across borders with relative anonymity.

The rise of social media, e-commerce, and other online services has also created new opportunities for fraudulent activities, such as phishing, identity theft, and online extortion. Cryptocurrencies and other digital financial tools have also become popular among criminals for their ability to obscure transactions and facilitate money laundering. The decentralized nature of cryptocurrencies makes it difficult for authorities to trace the flow of funds, allowing illicit financial flows to occur with minimal detection. Criminals often use these digital currencies to move money across borders, evade taxes, and finance illegal activities.

5.5. Transnational criminal networks

Sophisticated transnational criminal organizations are highly adept at exploiting global networks to facilitate a wide range of illicit activities, including online scams and fraud. These organizations often have extensive resources, connections, and expertise, enabling them to operate across multiple countries and evade detection by law enforcement. Their global reach and coordination make them formidable opponents for national and international authorities. Established smuggling routes, often used for drug trafficking, human trafficking, and arms smuggling, are also employed for other forms of transnational crime, including online scams and money laundering.

These routes involve complex logistics and coordination among various criminal groups, making them difficult to disrupt. The use of these routes allows criminals to move illicit goods and funds across borders, further complicating efforts to combat transnational crime.

5.6. Regulatory gaps

The variability in financial regulations and enforcement across different countries creates opportunities for criminals to exploit gaps in the legal system. Differences in legal frameworks, regulatory capacities, and enforcement practices can hinder effective international cooperation and enforcement. Criminals take advantage of these inconsistencies to move money, goods, and information across borders without being detected or prosecuted. Moreover, the absence of effective coordination among international and regional authorities can severely limit their ability to combat transnational crimes. Criminal networks often exploit these gaps in coordination to operate across jurisdictions, knowing that law enforcement agencies may struggle to share information, collaborate on investigations, or synchronize enforcement actions. This lack of coordination also allows criminals to use multiple countries as safe havens for their illicit activities.

5.7. Social factors

In regions where individuals face severe financial hardship, there is a higher likelihood of involvement in or victimization by online scams and other illicit activities. Financial desperation can drive people to take risks they would otherwise avoid, such as engaging in fraudulent schemes or falling prey to scam artists. This desperation is often exacerbated by economic downturns, high unemployment, and limited access to credit or financial assistance. In Myanmar and other ASEAN countries experiencing similar conditions, economic instability and inadequate social safety nets have intensified vulnerabilities.

Cultural or societal norms may tolerate or even encourage certain forms of illicit activities. For example, informal economic practices, such as unregulated trade or unofficial money transfers, may be seen as acceptable or even necessary in areas where formal financial systems are inaccessible or unreliable. Additionally, in some cultures, corruption may be viewed as a normal part of doing business, further enabling the proliferation of illicit activities. In Myanmar, corruption is often regarded as a social norm and a routine aspect of business, further entrenching illicit activities and complicating efforts to combat them.

6. Adverse effects of online scamming, and illicit financial flows

Building on the analysis of underlying drivers, this section explores the wide-ranging consequences of online scams and illicit financial flows (IFFs) linked to the Kyar Phyant networks. These activities not only destabilize local economies but also produce ripple effects across regional and global systems.

6.1. Country level

Economic impact

Illicit financial flows (IFFs) represent a significant drain on national resources. Money that could have been used for development, infrastructure, and social services is instead lost to illegal channels. This deprives governments of much-needed revenue, exacerbating fiscal deficits and limiting the ability to invest in public goods. The cumulative impact can slow economic growth and perpetuate poverty cycles. The flow of illicit funds is often associated with the rise of organized crime and corruption. As criminal networks become more entrenched, they exert greater influence over the economy, politics, and society. This leads to a vicious cycle where crime breeds more crime, undermining legal economic activities and fostering an environment where illegal activities flourish.

Additionally, workers who leave these criminal casino scams often find themselves returning to them. Many lack the necessary skills and experience for other types of employment, as their only work background involves these illegal operations. Criminal casinos not only welcome them back but also offer a quick and easy way to earn money, further trapping them in this cycle of exploitation and crime.

Social impact

The victims of online scams often suffer significant financial losses which lead to the psychological impact, including stress, anxiety, and loss of confidence. They can be profound, affecting the mental health and well-being of individuals. Online fraud and scams disproportionately affect marginalized and vulnerable populations, such as the elderly, low-income individuals, and those with limited digital literacy. As these groups are already at a disadvantage, the financial and psychological impacts of becoming a victim exacerbate existing inequalities, leading to further social stratification and potential social unrest.

6.2 Regional level

Adverse economics

Illicit financial flows infiltrate regional markets, often being funneled into sectors like real estate, leading to market distortions. Inflows of illegally obtained funds can drive up asset prices, making it difficult for legitimate businesses and individuals to compete. This influx of illicit capital creates an uneven playing field, contributing to inflated property prices and speculative bubbles, as seen in countries like China. Over time, these distortions can lead to adverse economic conditions, stunted development. Illicit activities, including online fraud and scamming, often spill over borders, complicating regional economic cooperation. Criminal networks exploit differences in national regulations and enforcement capabilities, creating transnational crime networks that are difficult to dismantle. This cross-border crime threatens regional stability and undermines efforts to build integrated, cooperative economic frameworks.

Social stability

The social and economic impact of online fraud and scamming can contribute to regional instability, particularly in areas already facing economic or political challenges. As criminal networks grow and cross borders, they destabilize not only the affected countries but also their neighbors. This instability can lead to a breakdown in regional cooperation, increased conflict, and a rise in migration and refugee flows, further straining social and economic systems.

Security

As regional crime networks become more entrenched, they pose significant challenges to regional security. These networks often involve drug trafficking, human trafficking, and other forms of organized crime, all of which require coordinated regional responses. The complexity and scale of these networks make them difficult to combat, leading to increased violence, corruption, and lawlessness across the region. Moreover, the increase in cross-border human trafficking and exploitation is a significant security and human rights issue. Regions with weak governance, poor law enforcement, and economic instability are particularly vulnerable to becoming hubs for human trafficking, leading to widespread abuse, exploitation, and a deterioration of regional security and human rights standards.

6.3. International level

Economic impact

Illicit financial flows undermine the integrity of the global financial system by introducing vast amounts of unregulated and often illegal money into circulation. This can lead to financial instability, as it distorts markets, encourages risky behavior, and undermines efforts to maintain transparency and accountability in financial transactions. Over time, these flows can weaken global financial institutions and erode confidence in international markets. The proliferation of illicit financial flows also contributes to significant global tax revenue losses. When individuals and corporations engage in tax evasion through illegal means, it reduces the funds available for public services, infrastructure, and development projects. This loss of revenue impacts both developed and developing countries, hindering efforts to address global challenges such as poverty, inequality, and climate change. For perspective, the Just Energy Transition Partnerships (JETPs)[9], a four-year initiative to support equitable energy transitions in both developing and developed countries, are valued at only USD 20 billion. In contrast, Southeast Asian online scamming gangs are estimated to have stolen USD 75 billion between 2020 and 2024, highlighting the enormous financial impact of illicit activities compared to the investments in sustainable development efforts.

Social impact

Online fraud and scamming contribute to the growth and sophistication of international crime networks. These networks are often involved in a range of illegal activities, including drug trafficking, money laundering, and cybercrime, which pose significant challenges to global security. The transnational nature of these crimes complicates efforts to combat them, requiring international cooperation and coordination. Illicit activities, particularly those involving human trafficking, forced labor, and exploitation, have significant human rights implications. These violations affect individuals and communities across the globe, undermining international human rights standards and commitments.

[9] See the details of the JETP https://www.undp.org/indonesia/projects/indonesia-just-energy-transition-partnership-jetp

Political impact

The international community faces significant challenges in regulating and combating cross-border illicit activities. Differences in national interests, legal frameworks, and regulatory capacities can hinder efforts to agree upon and enforce international standards. These challenges are compounded by the global nature of online fraud and scamming, which require robust, harmonized responses from multiple countries and international organizations.

7. How can one drive change?

The previous sections detailed the scale and complexity of online scams and illicit financial flows in Myanmar where state actors are often complicit. This section shifts from analysis to action, outlining how various actors governments, civil society, international organizations, the media, and the private business sector can work together to disrupt these networks. Addressing the problem requires coordinated, multi-level responses grounded in legal, political, will to act, and community-based strategies.

7.1. Government level actions

Myanmar

The Myanmar military, which seized power in a coup against the democratically elected government in 2021, lacks both the legal authority (*de jure*) and the political will to combat online scams, financial crimes, and illicit financial flows. In reality, the military itself is deeply involved in these illegal activities, profiting from transnational cyber scams, money laundering, and illicit trade. Any expectation that the junta would implement genuine reforms against financial crimes is unrealistic, as doing so would threaten its own interests and revenue streams.

Given this, the international community must recognize that Myanmar's military regime is not a legitimate governing authority and should not be treated as such. Instead of pressuring the junta to act, efforts should focus on isolating it economically and politically. Targeted sanctions against military leaders, financial institutions linked to the regime, and entities facilitating illicit financial flows are essential. The Financial Action Task Force (FATF), the UN, and key regional powers Association of Southeast Asian Nations (ASEAN), China, India, and Western countries must coordinate enforcement measures to cut off access to offshore accounts and criminal networks sustaining the junta.

At the same time, support must be directed toward democratic resistance forces, including ethnic resistance organizations (EROs), and civil society groups that are working to build an alternative, legitimate governance structure. International organizations such as the UN, the World Bank, and regional development banks should engage with these actors to provide technical assistance, training in financial regulation, and cybersecurity support. Strengthening border control and intelligence-sharing with Myanmar's neighbors especially Thailand, India, and China can help disrupt the military's illicit financial networks.

The goal should not be to reform the military regime but to weaken its financial and political grip and take it down while empowering democratic forces to take control of Myanmar's governance. A coordinated strategy combining economic pressure, legal enforcement, and support for opposition movements is the only viable path to addressing both financial crimes and the broader crisis in Myanmar.

To reinforce this strategy of international isolation and accountability, it is crucial to examine Myanmar's obligations under international law. Legal instruments such as the United Nations Convention against Transnational Organized Crime (UNTOC) provide a normative and

institutional framework that not only highlights the regime's failures but also offers a basis for coordinated international action.

Myanmar's involvement in transnational organized crime networks, particularly in relation to the Kyar Phyant scam syndicates, must be assessed through the lens of the United Nations Convention against Transnational Organized Crime (UNTOC)[10]. Although Myanmar signed the Convention in 2004 and ratified it in 2005, there has been a conspicuous absence of genuine domestic enforcement of its provisions, especially under the post-coup military regime. The Convention imposes clear legal obligations that, if implemented, could serve as powerful tools to combat the intertwined phenomena of online scamming, corruption, and illicit financial flows. Specifically, articles 5, 6 and 9 are needed to be considered.

Article 5 of the UNTOC, concerning the criminalization of participation in organized criminal groups, directly targets the operational core of Myanmar's digital scam economy. It requires States Parties to adopt legislative or other measures to criminalize conduct by individuals who participate in or direct the activities of organized criminal groups. The structures described in this paper ranging from scam compounds to transnational networks backed by armed groups and military officials easily meet the definitional thresholds under the Convention. Myanmar's failure to prosecute such conduct or dismantle the enabling networks reflects a breach of its obligations under Article 5.

Article 6, which obligates States to criminalize money laundering, is also relevant to tackle the scams. The syndicates not only defraud victims through digital means but also launder proceeds via cryptocurrency, real estate, and informal banking systems. This article also mandates preventive measures, such as the regulation of financial institutions, customer identification, and record-keeping, all of which are currently lacking or deliberately undermined in Myanmar. As such, non-compliance with Article 6 is not merely theoretical; it has tangible effects in facilitating the recycling of criminal proceeds, including those generated from human trafficking and forced labor.

Article 9 which is about measures against corruption is also important for Myanmar where scam businesses are deeply embedded in networks of protection involving both state and non-state actors. The article requires States to take effective action to prevent, detect, and punish corruption, including through the establishment of oversight bodies. In practice, the corruption that underpins the scam economy is institutionalized, with parts of the military, border guard forces, and local officials profiting directly from the criminal enterprises. The failure to institute or empower independent anti-corruption mechanisms, therefore, constitutes a serious violation of this obligation.

Beyond treaty obligations like UNTOC, Myanmar's failure to prevent or suppress transnational organized crime may also attract responsibility under customary international law, as codified by the International Law Commission's (ILC) Draft Articles on State Responsibility[11]. Although these Articles are not a treaty, they are widely regarded as reflecting customary law and have been invoked by international tribunals including the ICJ and human rights courts. Their relevance lies in their ability to assign international legal responsibility not only for direct wrongful acts but also for complicity or failure to act.

Under Article 1, "every internationally wrongful act of a State entails the international responsibility of that State." The hosting and facilitation of organized crime, human trafficking,

[10] See the full version of the United Nations Convention against Transnational Organized Crime (UNTOC) here https://www.unodc.org/documents/middleeastandnorthafrica/organised-crime/united_nations_convention_against_transnational_organized_crime_and_the_protocols_thereto.pdf

[11] See the full version of the International Law Commission's Draft Articles on State Responsibility here https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf

and massive financial fraud often involving coerced labor and abuse may amount to a violation of peremptory norms (jus cogens) and human rights obligations. When state organs, such as military commands, knowingly permit or benefit from these acts, their conduct is attributed to the State itself under Article 4, which provides that the acts of any state organ are considered acts of the state under international law.

Even more directly relevant are Articles 16 and 17, which address complicity in another State's internationally wrongful acts or the direction and control of such acts. For instance, if Myanmar's military regime and ethnic armed organizations have knowingly allowed transnational criminal groups to operate with impunity and has materially supported their activities through official facilitation, border access, or security protection, it may be considered complicit in the resulting harm to victims both within and outside its borders. This raises the possibility that Myanmar could be held responsible not only for its own misconduct but also for the transnational harm caused by actors it aids or fails to control.

Another key provision is Article 14, which deals with continuing wrongful acts. The Kyar Phyant system is not a one-time offense; it constitutes an ongoing pattern of organized crime and systematic abuse. Continued tolerance or enabling of these crimes by Myanmar's authorities may trigger liability for a continuing breach, requiring cessation and assurances of non-repetition. In the long term, this may open legal pathways to international claims for reparations or restitution on behalf of victims.

Furthermore, Article 41 stipulates that states shall not recognize as lawful situations created by serious breaches of peremptory norms. If it is established that Myanmar's military regime is engaged in practices violating norms such as the prohibition of slavery or trafficking in persons, other states may be under an obligation not to recognize or cooperate with the regime reinforcing arguments for diplomatic isolation, suspension from international institutions, or even targeted interventions by bodies such as the UN Security Council. In practical terms, invoking these legal frameworks does not necessarily require a formal ICJ judgment. International tribunals, regional human rights bodies, and even domestic courts (under universal jurisdiction principles) may incorporate the ILC Draft Articles in assessing Myanmar's liability. Advocacy organizations, transitional justice commissions, and accountability-focused UN bodies can leverage this framework to document abuses, guide sanctions regimes, and justify actions taken against Myanmar's officials under international law.

China and Thailand

Given the regional scope of Myanmar's scam syndicates and financial networks, particularly their links to **Chinese and Thai territory**, cross-border accountability becomes essential. As key regional actors, China and Thailand cannot remain passive observers. Both countries play a pivotal role in either enabling or disrupting the transnational criminal networks operating across their shared borders with Myanmar. Both nations must recognize that the Myanmar military is the driving force behind many illicit activities, including online scamming operations. To address these challenges effectively, regional cooperation must be contingent upon the formation of legitimate, people-elected central and regional governments in Myanmar. Efforts to improve border security, share intelligence, and conduct coordinated operations will only be effective when conducted with a government that genuinely represents the people's interests. Until such a government is established, any military-led initiative will likely be superficial and ineffective.

7.2. Communities and civil society

Grassroots action

Empowering people with digital literacy is critical to reducing the prevalence of online scams. They need to report to the police and authorities about the scam case. Informing authority and taking necessary actions is as important as returning the fraud money to them. Grassroots organizations can spearhead educational campaigns that inform the public about the risks associated with online gambling, romance scams, and phishing schemes. These campaigns should be tailored to reach different demographics, using local languages and culturally relevant messaging to maximize impact. By raising awareness, communities can become less susceptible to manipulation by online scammers. In areas where government enforcement is weak or compromised, civil society organizations can establish community watch programs. These programs can act as the eyes and ears of the community, monitoring suspicious activities and reporting them to authorities or trusted local leaders. Community-driven vigilance can be particularly effective in rural or underserved areas where scammers often target vulnerable populations. For example, there is a dedicated Facebook group[12] where victims of Kyar Phyant come together to organize, educate, and raise awareness about its threats. Currently, the group has nearly 1,000 members, and we need more community initiatives like this.

Another notable example is a Nairobi-based NGO called Awareness Against Human Trafficking (HAART) Kenya, which has adopted the UN Four P's Strategy as a guiding principle in its anti-trafficking efforts. HAART's work has benefited over a thousand survivors and connected with over one hundred people through their workshops (HAART Kenya, n.d.). Head of protection from HAART, Mercy Otieno stated that contacting and assisting Kenyans trafficked to Myanmar is significantly more challenging than for those trafficked to countries like Laos, a situation that highlights urgent calls for grassroots action within Myanmar and enhanced international collaboration (Fishbein, 2024). As a further illustration, IJM Hong Kong prioritizes public education in its efforts to raise awareness regarding modern slavery through its community-oriented approaches (IJM, n.d.). IJM's 2024 annual report states that in 2023, they assisted in freeing over 200 individuals from forced scamming, spanning multiple countries in Southeast Asia, including Cambodia, Laos, Myanmar, and the Philippines (IJMHK, 2024).

Victims of online scams often face significant financial, emotional, and social challenges. Providing support services such as legal assistance, counseling, and financial advice can help victims recover from these crimes and avoid further exploitation. Community-based support networks can also play a role in helping victims navigate the legal system and rebuild their lives.

7.3. Cybersecurity measures

Enhancing security

To combat the growing threat of online scams and cybercrime, regional governments and businesses must invest in advanced cybersecurity infrastructure. This includes deploying sophisticated threat detection systems, implementing robust data protection protocols, and regularly updating security measures to counter emerging threats. Regional organizations like ASEAN should prioritize cybersecurity discussions at their meetings, focusing on coordinated efforts to combat transnational crimes.

This could involve harmonizing laws across member states, improving cross-border enforcement, and facilitating intelligence sharing. Promoting good cyber hygiene practices is

[12] The link to this Facebook group https://shorturl.at/BXYOe

essential to reducing vulnerabilities to cybercrime. This involves educating the public and organizations on basic security measures, such as using strong passwords, enabling two-factor authentication, and recognizing phishing attempts. Regular training and awareness campaigns can reinforce these practices, helping to build a more secure online environment.

7.4. Media and journalists

Investigative reporting

Journalists and media outlets have a crucial role in uncovering and exposing online scams, bringing these activities to the public's attention. Investigative reporting can shed light on the methods used by scammers, the scale of their operations, and the impact on victims. By holding perpetrators accountable, journalists can help deter future scams and encourage authorities to act against these criminal networks. Media campaigns can also play a significant role in raising public awareness about the risks associated with online transactions.

By educating the public on how to recognize and avoid scams, the media can reduce the number of potential victims and promote safer online behavior. Given the nature of this topic, which is less covered in academic literature, nearly all the sources for this essay come from journalists and media outlets. This underscores the vital role that the media plays in addressing and understanding online scams.

7.5. International organizations

International financial institutions

Organizations like the International Monetary Fund (IMF) and World Bank can provide critical support to countries vulnerable to illicit financial flows by offering technical assistance and funding. This support can be used to strengthen financial regulations, improve enforcement capacities, and enhance transparency in financial transactions. By building the capacity of local institutions, these organizations can help create a more resilient financial system that is less susceptible to exploitation by criminal networks.

Foreign aid and assistance

Developed countries and international organizations have a role to play in providing technical assistance, funding, and expertise to countries like Myanmar. This support can be directed towards improving border security, enhancing law enforcement capabilities, and building the legal and institutional frameworks needed to combat online scams and financial crimes. By supporting local efforts, the international community can help create a safer and more stable environment in Myanmar and the surrounding region.

7.6. Private sector involvement

Financial institutions

Banks and money transfer services are at the forefront of the fight against money laundering and other financial crimes. By implementing stricter know-your-customer (KYC) protocols and closely monitoring transactions for suspicious activity, financial institutions can disrupt the flow of illicit funds. Collaborating with government agencies and international organizations, these institutions can play a key role in identifying and stopping money laundering networks associated with online scams.

Financial institutions should be required to report suspicious transactions to relevant authorities promptly. This requires establishing robust monitoring systems that can detect unusual patterns of behavior indicative of fraud or money laundering. Enhanced communication and cooperation between banks, regulators, and law enforcement agencies are essential for effective intervention. While blockchain technology and Web3 have advanced, demonstrable success stories, particularly in contexts similar to Myanmar, where crypto wallets are illegal, are still lacking. Addressing this requires cooperation from widely used local fintech services like Wave Pay and Kpay, a digital payment method from KBZ bank , also known as KBZ pay. Implementing robust KYC protocols and providing a streamlined mechanism for reporting scams with evidence would enable these platforms to track patterns and limit scammers' operational scope.

Technology companies and telecommuncation companies

Online platforms such as Facebook and Telegram that host websites or services used by scammers have a responsibility to monitor and moderate content to prevent fraud. This includes implementing user verification processes, removing, or blocking access to known scam sites, and working with law enforcement to identify and shut down illegal activities. Telecommunication companies such as Myanma Post and Telecommunications (MPT), Ooredoo Myanmar, ATOM Myanmar, and Mytel Myanmar should take active measures to block spam SMS messages. This can include identifying and investigating SIM card holders involved in scams and taking appropriate action. These companies must also invest in AI and machine learning tools to detect and prevent scams in real-time, ensuring a safer online environment for users.

8. Conclusion

The situation on Myanmar's borders has become a complex web, with multiple actors benefiting from the illicit financial ecosystem. The landscape surrounding Kyar Phyant is changing rapidly, especially since the start of 2025.

If we are to suggest the most realistic and effective solutions from our recommendations, the first and most important point is that as long as the military regime remains in power in Myanmar, these issues cannot be fully resolved. While some symptoms of the problem can be mitigated, the root cause remains. Therefore, the downfall of the regime is essential, and the international community should support Myanmar’s resistance forces—directly or indirectly—not only to address the scam crisis but also to end the broader humanitarian and political disasters created by the junta.

Second, public awareness must be raised in every country about the methods and tactics used by scammers. People should be encouraged to report scam cases, and law enforcement agencies must establish an accessible and efficient reporting system that minimizes bureaucratic barriers.

Third, social media, messaging platforms and telecommunication companies must implement stricter controls on scams, as these platforms serve as the primary channels for scam operations. Enhanced monitoring, better content moderation, and stronger cooperation with law enforcement can help disrupt scam networks at their source.

Acknowledgement
This paper is based on the first prize-winning essay from the Eleventh Amartya Sen Essay Prize Competition (2024). The authors would like to thank the reviewers as well as the Journal ASAP editors, organizers, and sponsoring organization. The presentation of the paper is available on the official Yale Global Justice Program YouTube channel: https://youtu.be/7Dd8e5GWEB8

Disclaimer
The authors did not receive any financial assistance for this study except for the Amartya Sen award. The views expressed are solely those of the authors and do not reflect their affiliated institutions. The authors declare no conflicts of interest related to the research, authorship, or publication of this article.

References

Akins, H. (2018). The two faces of democratization in Myanmar: A case study of the Rohingya and Burmese nationalism. *Journal of Muslim Minority Affairs, 38*(2), 229–245. https://doi.org/10.1080/13602004.2018.1475619

ANN. (2022). *After son's death, dad wants other scam victims saved. Asia News Network*. https://asianews.network/after-sons-death-dad-wants-other-scam-victims-saved/

Chipolina, S. (2024). *$100mn in crypto payments traced to Myanmar-based 'scammers.' Financial Times*. https://www.ft.com/content/fbe27292-4df9-4610-99e0-a93121e06dd3

Clapp, P. A. (2024). Southeast Asia web scams reach U.S., setting off alarms for law enforcement. *The United States Institute of Peace*. https://www.usip.org/publications/2024/08/southeast-asia-web-scams-reach-us-setting-alarms-law-enforcement

International Crisis Group. (2024). *Scam Centres and Ceasefires: China-Myanmar Ties Since the Coup* (Briefing No. 179). International Crisis Group. https://www.crisisgroup.org/asia/north-east-asia/china-myanmar/b179-scam-centres-and-ceasefires-china-myanmar-ties-coup

Devi, K. S. (2014). Myanmar under the Military Rule 1962-1988. *International Research Journal of Social Sciences*, *3*(10), 46–50.

Faux, Z. (2024). *New Study Estimates as Much as $75 Billion in Global Victims' Losses to Pig-Butchering Scam. Time Magazine*. https://time.com/6836703/pig-butchering-scam-victim-loss-money-study-crypto/

Fishbein, E. (2024). *A global monster: Myanmar-based cyber scams widen the net*. *Frontier Myanmar.* https://www.frontiermyanmar.net/en/a-global-monster-myanmar-based-cyber-scams-widen-the-net/

Fishbein, E., & Lusan, N. N. (2024). *Under siege in Myanmar's cyber-scam capital. ALJAZEERA*.https://www.aljazeera.com/news/longform/2024/7/29/under-siege-in-myanmars-cyber-scam-capital

Frontier, & Gao, G. (2022). *Scam City: How the coup brought Shwe Kokko back to life*. *Frontier Myanmar*. https://www.frontiermyanmar.net/en/scam-city-how-the-coup-brought-shwe-kokko-back-to-life/

Frontier. (2023a). *A day in the life of a Shwe Kokko scammer. Frontier Myanmar*. https://www.frontiermyanmar.net/en/a-day-in-the-life-of-a-shwe-kokko-scammer/

Frontier. (2023b). *Controversial border project looms over KNU congress. Frontier Myanmar*. https://www.frontiermyanmar.net/en/controversial-border-project-looms-over-knu-congress/

Global Times. (2025*). First trial of Ming family suspected of telecom frauds in northern Myanmar held in Zhejiang. Global Times.* https://www.globaltimes.cn/page/202502/1328727.shtml

HAART Kenya. (n.d.). *Home Page: Awareness Against Human Trafficking (HAART) Kenya* [NGO website]. HAART Kenya. https://haartkenya.org/

Hogan, M. (2024). *Chinese Money Laundering: A Comprehensive Analysis of Methods, Impacts, and Countermeasures* [LinkedIn post]. https://www.linkedin.com/pulse/chinese-money-laundering-comprehensive-analysis-matthew-hogan-ms-krsre/

Hunt, L. (2024). *Indonesia Rescues 20 From Traffickers in Myanmar. The Diplomat*. https://thediplomat.com/2023/05/indonesia-rescues-20-from-traffickers-in-myanmar/

IJM. (n.d.). Our Work in Hong Kong. International Justice Mission Hong Kong. https://ijmhk.org/en/work-in-hk/

IJM. (2024). 2024 Annual Report [Annual Report]. International Justice Mission. https://ijmhk.org/wp-content/uploads/2024/10/IJMHK-2024-Annual-report.pdf

Irrawaddy. (2022). *Hundreds of Indians Reportedly Trafficked to Myanmar by Cybercrime Operations. Irrawaddy*. https://www.irrawaddy.com/news/burma/hundreds-of-indians-reportedly-trafficked-to-myanmar-by-cybercrime-operations.html

Irrawaddy. (2023). *China's Crackdown on Cyber Scams in Myanmar Nets UWSA Deputy Chief. Irrawaddy*. https://www.irrawaddy.com/news/burma/chinas-crackdown-on-cyber-scams-in-myanmar-nets-uswa-deputy-chief.html

Irrawaddy. (2024a). *Myanmar Military 'Provided Protection for US$ 14 Billion a Year Scam Hub' on China Border*. *Irrawaddy*. https://www.irrawaddy.com/news/burma/myanmar-military-provided-protection-for-us-14-billion-a-year-scam-hub-on-china-border.html

Irrawaddy. (2024b). *Scam Operations Flourish in Myanmar's Biggest City. Irrawaddy*. https://www.irrawaddy.com/news/investigation/scam-operations-flourish-in-myanmars-biggest-city.html

ISP Myanmar. (2024). Kyar Phyant Crackdown. *Institute for Strategy and Policy – Myanmar*. https://ispmyanmar.com/kyar-phyant-crackdown/

Jackson, W. (2024). *How South-East Asia's pig butchering scammers are using artificial intelligence technology. ABC*. https://www.abc.net.au/news/2024-05-16/pig-butchering-scams-artificial-intelligence-ai-face-swapping-/103804830

Jordt, I., Than, T. & Ye Lin, S. (2021). How Generation Z Galvanized a Revolutionary Movement against Myanmar's 2021 Military Coup. In *How Generation Z Galvanized a Revolutionary Movement against Myanmar's 2021 Military Coup* (pp. 1-33). Singapore: ISEAS Publishing. https://doi.org/10.1355/9789814951746-003

Justice for Myanmar. (2024). *The Karen Border Guard Force/Karen National Army criminal business network exposed. Justice for Myanmar.* https://www.justiceformyanmar.org/stories/the-karen-border-guard-force-karen-national-army-criminal-business-network-exposed

Kennedy, L., & Southern, N. P. (2022). *Inside Southeast Asia's Casino Scam Archipelago*. *The Diplomat*. https://thediplomat.com/2022/08/inside-southeast-asias-casino-scam-archipelago/

Leo, L. (2024). *AI in Southeast Asia: As new frontier opens in scams and cyberbullying, authorities wage high-tech battle. CNA*. https://www.channelnewsasia.com/asia/artificial-intelligence-southeast-asia-deepfakes-cyberbullying-scams-cybersecurity-threats-4159006

Lusthaus, J. (2020). *Cybercrime in Southeast Asia Jonathan Lusthaus Policy Brief Report Combating a global threat locally* (Policy Brief No. 29/2020). The Australian Strategic Policy Institute. http://ad-aspi.s3.amazonaws.com/2020 05/Cybercrime%20in%20Southeast%20Asia.pdf

Naing, I. (2023). *Chinese Cybercrime Syndicates in Myanmar Now Target Victims Worldwide. VOA*. https://www.voanews.com/a/chinese-cybercrime-syndicates-in-myanmar-now-target-victims-worldwide/7158750.html\

OHCHR. (2023). *Online Scam Operations And Trafficking Into Forced Criminality In Southeast Asia: Recommendations For A Human Rights Response*. Office of the United Nations High Commissioner for Human Rights. https://bangkok.ohchr.org/wp-content/uploads/2023/08/ONLINE-SCAM-OPERATIONS-2582023.pdf

Parmar, B. L., Freeman, R. E., Harrison, J. S., Wicks, A. C., Purnell, L., & De Colle, S. (2010). Stakeholder Theory: The State of the Art. Academy of Management Annals, 4(1), 403–445. https://doi.org/10.5465/19416520.2010.495581

Rebane, T., & Watson, I. (2024). *Killed by a scam: A father took his life after losing his savings to international criminal gangs. He's not the only one. CNN*. https://edition.cnn.com/2024/06/17/asia/pig-butchering-scam-southeast-asia-dst-intl-hnk/index.html

RFA. (2024). *800 Chinese deported from Myanmar's Thai border. RFA Burmese*. https://www.rfa.org/english/news/myanmar/chinese-deported-03142024062659.html

Thul, P. C. (2019). Thousands lose jobs, casinos shut as Cambodia bans online gambling. *Reuters*. https://www.reuters.com/article/world/thousands-lose-jobs-casinos-shut-as-cambodia-bans-online-gambling-idUSKBN1YZ0XH/

Tortermvasana, K. (2024). *Fraud raid seizes 58 satellite devices. Bangkok Post*. https://www.bangkokpost.com/business/general/2813459/fraud-raid-seizes-58-satellite-devices. View our policies at http://goo.gl/9HgTd and http://goo.gl/ou6Ip.

Tower, J., & Clapp, P. (2020). *Myanmar's Casino Cities: The Role of China and Transnational Criminal Networks*. UNITED STATES INSTITUTE OF PEACE. https://www.usip.org/sites/default/files/2020-07/20200727-sr_471-myanmars_casino_cities_the_role_of_china_and_transnational_criminal_networks-sr.pdf

UNODC. (2020). *Darknet Cybercrime Threats to Southeast Asia*. United Nations Office on Drugs and Crime.

UNODC. (2024). *Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia: A Hidden and Accelerating Threat*. United Nations Office on Drugs and Crime (UNODC). https://www.unodc.org/roseap/uploads/documents/Publications/2024/Casino_Underground_Banking_Report_2024.pdf

USIP. (2024). *Transnational Crime in Southeast Asia A Growing Threat to Global Peace and Security*. United States Institute of Peace. file:///C:/Users/Lenovo/Downloads/ssg_transnational-crime-southeast-asia.pdf

Vakulchuk, R., Stokke, K., & Overland, I. (2018). *Myanmar: A Political Economy Analysis* (pp. 1–98) [Technical Report]. Norwegian Institute of International Affairs. https://doi.org/10.13140/RG.2.2.27989.93928

Walker, T. (2024). *Southeast Asia scam centers swindle billions. VOA East Asia*. https://www.voanews.com/a/report-southeast-asia-scam-centers-swindle-billions/7655765.html

Zhou, L. (2023). *China and Myanmar pledge to fight online scams as Beijing seeks stronger ties with junta. South China Morning Post*. https://www.scmp.com/news/china/diplomacy/article/3232852/china-and-myanmar-pledge-fight-online-scams-beijing-seeks-stronger-ties junta?module=perpetual_scroll_0&pgtype=article