NHSMUN

National High School Model United Nations

Table of Contents

Committee History 3

Topic A: Scam Compounds (Operation Shadow Storm) 4

Introduction 5

History and Description of the Issue 6

Current Status 13

Bloc Analysis 18

Committee Mission 20

Character Biographies 21

Research and Preparation Questions 25

Important Documents 25

Committee History

Before the 19th century, international police cooperation was only conducted on an ad hoc basis, meaning that it was informal, temporary, and as needed. These temporary initiatives were primarily focused on very specific goals or criminal organizations. The early 20th century saw the beginning of a more concerted effort to rally and coordinate the efforts of different policing organizations. The International Criminal Police Congress was held in Vienna in 1923, where a group of 22 delegations founded the International Criminal Police Commission.[1] The commission's membership grew from its original 22 members to 58 member states by 1934 before the commission became dormant during World War II. In 1946, leaders in the United Kingdom, Belgium, France, and Scandinavian nations reorganized and founded the International Criminal Police Organization, now known as INTERPOL.[2]

The constitution of INTERPOL, adopted in 1956, outlines two primary mandates that the organization must follow. Article 2, clause 1 of the constitution states that INTERPOL is "to ensure and promote the widest possible mutual assistance between all criminal police authorities within the limits of the laws existing in the different countries and in the spirit of the Universal Declaration of Human Rights." Clause 2 states that INTERPOL is "to establish and develop all institutions likely to contribute effectively to the prevention and suppression of ordinary law crimes." Additionally, article 3 forbids INTERPOL from undertaking "any intervention or activities of a political, military, religious or racial character."[3]

In 2018, INTERPOL launched the Global Policing Goals (GPGs). These initiatives were designed to work with the United Nations Agenda for Sustainable Development and sought to curb the effects of crime on a global scale. The seven GPGs are to "Counter the threat of terrorism," "Promote border integrity worldwide," "Protect vulnerable communities," "Secure cyberspace for people and businesses," "Promote global integrity," "Curb illicit markets," and "Support environmental security and sustainability."[4] Any initiatives that INTERPOL pursues should take concrete steps to support these goals.

The primary governing body of INTERPOL is the General Assembly. The INTERPOL General Assembly meets annually, with delegates attending from every member state. Typically, delegates are "chiefs of police and senior ministry officials." During these assemblies, delegates collaborate to write resolutions. These resolutions must be passed by either a simple or two-thirds majority (depending on the topic of the resolution), with each member state receiving one vote. The General Assembly also elects the Executive Committee, a 13-delegate organization that organizes the implementation of INTERPOL resolutions. The delegates of the Executive Committee meet three times per year to ensure the smooth execution of INTERPOL missions and prepare the agenda for General Assembly meetings.[5]

1 "Our History," INTERPOL (International Criminal Police Organization), accessed September 19, 2021, https://www.interpol.int/en/Who-we-are/Our-history.
2 "Key Dates," INTERPOL (International Criminal Police Organization), accessed September 19, 2021, https://www.interpol.int/en/Who-we-are/Our-history/Key-dates.
3 "Legal Documents," INTERPOL (International Criminal Police Organization), accessed September 19, 2021, https://www.interpol.int/en/Who-we-are/Legal-framework/Legal-documents.
4 "Global Policing Goals." INTERPOL. Accessed September 20, 2021. https://www.interpol.int/en/Who-we-are/Strategy/Global-Policing-Goals.
5 "Governance." INTERPOL. Accessed September 20, 2021. https://www.interpol.int/en/Who-we-are/Governance.

TOPIC A

Scam Compounds (Operation Shadow Storm)

Photo Credit: UNODC / Laura Gil

Introduction

The International Criminal Police Organization (INTERPOL) is an international organization that addresses crime.[1] It unites 196 member countries as a hub for international crime. INTERPOL coordinates border-crossing investigations and international threats. This is primarily done through sharing vital information by sending notices and through global databases. These are pivotal for police forces from a local to a global level. By combining and analyzing shared data, INTERPOL can prepare for and respond to potential and active threats. These threats include cybercrime, organized crime, financial crime, and terrorism.[2] INTERPOL is vital to protecting and supporting victims around the world. They advocate for international cooperation by sharing data and creating universal databases for all nations. It backs investigations and assists in operations. As our world becomes more globalized, INTERPOL becomes much more crucial in facing future threats.

However, INTERPOL cannot act alone. It does not independently arrest suspects, prosecute crimes, or enter into a country. Instead, INTERPOL connects national law-enforcement agencies, distributes information about suspects and criminal methods, coordinates multinational operations, and provides tools for tracing stolen funds.[3] To close a scam compound, local authorities need to step in. Once the problem has been identified, then national authorities conduct arrests, rescues, and prosecutions within their own territories. When governments lack resources, do not cooperate with INTERPOL, or are affected by corruption, then INTERPOL's response could be limited.

Launched in March 2026, Operation Shadow Storm aims to resolve the growing financial fraud issue centered in Southeast Asia.[4] The United Nations Office on Drugs and Crime estimated that scams caused between USD 88.3 billion and USD 114.1 billion in losses across Southeast Asia, Australia, and New Zealand in 2025.[5] These losses show that a scam compound operating in just one country can financially harm victims across an entire region and beyond. People around the world lose money and personal information to the scams, and many of the workers contacting them have themselves been trafficked and forced to commit crimes. Distinguishing between willing operators and coerced workers is necessary when addressing the issue.

Scam compounds in Southeast Asia are an increasingly common and thriving industry, becoming much more industrialized. Scam bosses have adapted to the ever-changing technological environment. Scam compounds have also adopted Artificial Intelligence, forced labor, and collaborations with other crime bodies. These include, but are not limited to drug trading, human trafficking, and money laundering.[6] This issue is very recent and still developing today. As scam compounds become more advanced, it is vital that INTERPOL and Operation Shadow Storm adapt, and respond accordingly.

Operation Shadow Storm focuses on uncovering the individuals and financial networks who control scam compounds. These criminal leaders can disguise themselves or blend in. Third parties like recruiters, local businesses, shell companies, or casinos can facilitate the fraud.[7] Digital assets and bank accounts can be spread across multiple countries, making the money trail harder to track. Shadow Storm allows participating law-enforcement agencies to combine information and identify connections that may not be visible within a single national investigation.[8] However,

INTERPOL must still depend on national authorities and financial institutions to conduct investigations, freeze assets, make arrests, and prosecute suspects.

History and Description of the Issue

EVOLUTION OF SCAM COMPOUNDS AND ONLINE FRAUD

Online fraud has been an issue since the creation and rising popularity of the Internet. Specifically, phone scams and fake lotteries are very common. According to the Washington State Attorney General's Office, many people throughout the United States report receiving messages from telemarketers offering shares in foreign lotteries.[9] Like many common scams, these primarily targeted the elderly, taking advantage of their limited technology proficiency and scamming them upwards of thousands of dollars. People deceived and financially harmed by the scams are one group of victims. People trafficked into compounds and forced to conduct these scams are a separate group of victims.

Many of these scams originate from cyber scam centers, or compounds, where hundreds or thousands of workers operate under strict quotas and surveillance. Once trafficked into compounds in Southeast Asia, victims are frequently forced to carry out pig butchering scams.[10] These scams are similar to romance scams, often playing the long game to exploit their victims financially. Victims are lured into what they believe to be a romantic relationship, friendship, or situation with a trusted financial expert. Over time, this gradually "fattens up" a victim for later financial exploitation.[11] Victims often invest or donate money through a source controlled by the criminal organization. These scams generate billions of dollars each year. They are one of the most profitable forms of transnational organized crime, rivaling the profitability of even the drug trade.

Compounds may also conduct impersonation scams. In this, workers pretend to represent banks, police agencies, delivery companies, government offices, or victims' family members and collect money.[12] Other schemes direct victims to fake gambling or shopping platforms or use phishing links to steal passwords and financial information. Workers often follow prepared scripts, operate false online identities, and communicate with many potential victims at once. Artificial intelligence also allows for scammers to operate at even higher rates of productivity.[13] Like a legitimate business, supervisors monitor scammer conversations and require workers to meet financial quotas.

These organized fraud operations developed over several decades. The compounds in Southeast Asia that Operation Shadow Storm targets can be traced back to Taiwan in the late 1990s. During this time, phone scams and fake lotteries began to develop and became increasingly popular. By the 2000s, these operations spread throughout mainland China.[14]

In 2004, after a well-known professor lost 147,000 yuan to scammers and launched a complaint to the government, the Fujian province launched a special campaign to crack down on these scams. However, scam compounds continued to grow smarter, using newer and more advanced technologies and methods to continue targeting mainland Chinese citizens.[15] These scam compound centers started establishing secure hubs. They fortified them and expanded their global reach, evolving to become more serious global threats.[16] This led to China and Taiwan signing the 2009 Cross-Strait Joint Crime Fighting and Mutual Legal Assistance Agreement. Among other things, the agreement outlined mutual police cooperation, including conducting joint operations against fraud and trafficking. Using extensive resources from both parties, online scams were heavily reduced around this time.[17]

As a result, many criminal compounds set their sights on locations with weaker regulations, like Southeast Asia. From 2017 to 2019, Sihanoukville, Cambodia served as a hub for one of the largest Chinese-run online gambling platforms. While gambling is not inherently a scam, it can be predatory. The odds are generally designed to favor the operator rather than the participant. Additionally, illegal online gambling networks have developed facilities, payment systems, recruitment channels, and relationships with local authorities that can later support other criminal activity.

Gambling operators housed their operations in Sihanoukville because it had easy access to the capital, a large airport, an abundance of land available for rent or purchase, and relaxed law enforcement. Due to the increase of Chinese-funded infrastructure, crime syndicates also had strong connections to find victims in mainland China. At its peak, the online gambling sector accounted for 90 percent of the gambling industry's revenue of USD 5 billion.[18] Online gambling became a global concern as globalization increased, expanding its reach from Southeast Asia.[19]

Cambodia banned online gambling in 2019, disrupting many gambling operations based in the country. Some criminal organizations relocated, while others repurposed their facilities and networks for online fraud.[20] These organizations increasingly recruited workers through fake job advertisements and then used confinement, threats, violence, or fabricated debts to force them to conduct scams.[21]

As the past decades have shown, it is increasingly difficult to identify, prosecute, or arrest scammers. Often disguised as simple office buildings or hidden by local elites in casinos, illegal operations can be challenging to find. Even if a major figure is caught, it does not take long before another operation pops up just miles away from the original site.[22] Many individuals are also performing the work of various scams. As of 2026, an estimated 220,000 trafficking victims are held in scam compounds in Myanmar and Cambodia alone.[23] Their passports are often confiscated, preventing them from escaping. Failed attempts to escape or refusal to work could lead to beatings or other forms of punishment.

As of 2026, the INTERPOL Global Financial Fraud Threat Assessment warns that online crime is no longer just a threat to the online world, but

Gambling table at raided gang-run internet 'scam farm' in Bamban, north of Manila, the Philippines

Credit: UNODC / Laura Gil

a center of polycriminality. Polycriminality is the act of combining many forms of organized crime, such as human trafficking and cybercrime. In response, INTERPOL has enacted and launched campaigns aimed to prevent scam compounds from multiplying. Notably, the organization has strengthened relations with member states. This fosters more collaboration on such issues. Since 2024, INTERPOL has flagged 54 percent more fraud-related notices. Over the same period, INTERPOL supported member countries in more than 1,500 transnational fraud cases involving reported losses of approximately USD 1.1 billion.[24] Though scam compounds have been continuously adapting and evolving, so have INTERPOL and Operation Shadow Storm.[25]

HUMAN RIGHTS VIOLATIONS

A key complexity in addressing online scam compounds is that the individuals executing the scams are often victims themselves. People making phone calls, sending fraudulent messages, and interacting directly with victims might be coerced or directly forced to do so. However, not everyone working in a compound is trafficked. INTERPOL specifically notes that some participants willingly commit fraud, while others are held through force, threats, or debt bondage.[26] This makes raids especially complicated. Authorities must distinguish criminal organizers and willing participants from trafficking victims who were forced to break the law.

While the exact details vary from operation to operation, victims are frequently lured with fake advertisements promising well-paid work in fields such as technology, customer service, or online marketing. Recruiters may transport them through several countries before bringing them to guarded compounds. Once inside, their passports and phones may be confiscated. Their travel or recruitment costs may be used to place them in debt. Operators then claim that victims must work or earn a certain amount of money before they can leave.[27] At these compounds, victims can face beatings and other forms of physical abuse if their daily quotas are not met.[28] Compound operators may provide limited food and shelter, but these necessities are used to maintain victims' captivity rather than compensate them for freely chosen work.

Trafficking occurs at an international level. INTERPOL, through Operation Storm Makers II, uncovered instances of individuals being trafficked in Malaysia, Peru, Uganda, Dubai, and India.[29] The INTERPOL-coordinated operation brought together law-enforcement agencies from 27 countries and resulted in 281 arrests and the rescue of 149 trafficking victims.[30] While trafficking is a global issue, INTERPOL has found Southeast Asia to be a hotspot for such activities. However, recruiters, victims, compounds, financial accounts, and scam targets may all be located in different countries, requiring authorities to share information throughout an investigation.

Rachel Yoong's account provides a firsthand example of the coercion, exploitation, and violence experienced by victims trafficked into online scam compounds. Yoong, a resident of Malaysia, saw a well-paying job listing for a position at a casino in the capital of Myanmar and applied. After a few successful interviews, Yoong booked a flight to Myanmar. After a couple of days, the company who recruited her sent a car to her hotel. In the car, there were "two big, tough guys with guns," according to Yoong.[31] She was driven multiple hours to a more rural region near Myanmar's border with China and then sent to work in a tall, concrete building with around 200 other trafficking victims. At the facility, Yoong recounted that eight people were forced to sleep in one room and victims were forced to run scams for around 17 hours per day. If the victims did not meet their daily quota of at least USD 1,000 every three days, they would suffer beatings, electrocution, and other forms of abuse. Multiple people died from both suicide and punishment methods.

Yoong specifically conducted romance-centric scams targeting men in the United States. As a

particularly high earner, Yoong received many perks, such as being able to take home a portion of her earnings and go out to fancy dinners with her bosses. However, receiving limited payment or privileges did not mean that she was free to leave. This illustrates why authorities cannot determine whether someone was trafficked solely by asking whether that person earned money or participated successfully in the fraud. Yoong was eventually able to convince her bosses to sell her to a new compound. The sale of workers is a common practice across the scam compound business. While at this new compound, the Chinese government conducted a raid, arresting many and freeing the Chinese nationals on site in the process. However, as a Malaysian national, they did not send Yoong back home. Two weeks after the raid, Yoong and the other non-Chinese workers at the compound were released from the local police station. Their captors subsequently collected them and brought them to a camp in the jungle with significantly worse conditions.

Following a failed escape, Yoong's situation only grew more precarious. Her friend took beatings for her that left him bedridden for a week. Still, she persisted in her plan to escape. Eventually, she was able to get in touch with a local who helped her call the police. This led to the arrest of various people at the camp, yet the Malaysian embassy claimed they were unable to help her. Instead, Yoong coordinated another sale of herself to another gang with more lax security. In this new setting, Yoong was finally able to get the help of the Malaysian embassy and escape back to Kuala Lumpur.[32]

A rescue does not always end a victim's vulnerability. Authorities may initially treat people found inside compounds as criminal suspects or immigration offenders because they participated in fraud or entered the country without proper documentation. Victims may then face detention, prosecution, or deportation without being screened for trafficking. Trafficking victims should not be punished for unlawful acts they were compelled to commit as a direct consequence of their exploitation.[33] Effective operations therefore require trained interviewers, interpreters, safe shelters, medical and psychological care, contact with embassies, and procedures for safe repatriation.

While Yoong's story is horrific, it is not unique. Although no reliable worldwide count exists, scam compounds are estimated to have exploited hundreds of thousands of trafficking victims. By March 2025, INTERPOL estimated that around 300,000 people from 66 countries are suffering worldwide in scam compounds.[34] Scam compounds therefore create two groups of victims, those defrauded online and the people coerced into conducting that fraud. As INTERPOL and its affiliates work to dismantle scam compounds and hold their operators accountable, they must also prioritize rescuing and protecting victims, both targeted by the scams and those coerced into carrying them out.

ASSOCIATED CRIMES

Scam compounds depend on several interconnected crimes. In addition to online fraud, their operators may engage in human

By March 2025, INTERPOL estimated that around 300,000 people from 66 countries are suffering worldwide in scam compounds.

trafficking to obtain workers, money laundering to conceal profits, and corruption to avoid government intervention. INTERPOL describes this overlap among different criminal activities as "polycriminality."[35]

Criminal organizations must quickly move and conceal money before authorities can recover it. Thus, to obtain money from a victim, scammers often direct victims to send money to accounts controlled by "money mules."[36] Money mules allow criminals to use their bank accounts to receive or transfer stolen funds. This can be done either knowingly or because they were also deceived. The money may then pass through numerous accounts, shell companies, cryptocurrency exchanges, underground banking networks, or businesses that appear legitimate.[37] Each transfer makes it more difficult for investigators to identify where the money originated and who ultimately controls it. This process is called money laundering.[38]

Casinos and online gambling accounts can also be used to conceal stolen funds.[39] Criminals may launder the money so that it appears to be gambling revenue. Because scam proceeds can move through several countries within hours, national police may lose the opportunity to recover funds if they cannot quickly contact foreign banks and law-enforcement agencies.[40] INTERPOL therefore helps member countries exchange financial intelligence and request that suspicious transfers be stopped before the funds are moved again.

The use of shell companies, casinos, and international financial networks also helps explain why some criminal organizations establish operations in special economic zones. Chinese-backed special economic zones (SEZs) have existed for decades to build stronger economic ties between China and its Southeastern neighbors. These SEZs operate with a unique amount of autonomy and multinational involvement. The Chinese government works with local governments to launch various infrastructure, economic, and social projects in these regions. An unfortunate byproduct of this system is that criminal organizations can take advantage of the complexity.

Some government-approved SEZs are developed or managed by private companies. Although these zones remain subject to national law, their private management, multinational funding, and location in areas with limited government oversight can make illegal activity harder to detect. Criminal groups have exploited these conditions in some SEZs by using apparently legitimate businesses and development projects to conceal scam operations. Researchers sometimes describe developments that blur the boundary between legitimate investment and criminal control as "gray SEZs."[41]

This has led to a significant increase in SEZs used to cover up illicit activity across Southeast Asia, particularly in underdeveloped border regions. Some criminal syndicates establish operations in casino developments or take over abandoned casinos, allowing them to combine scam operations with the financial networks used to conceal their profits.[42] Allegedly, there are reportedly over 140 casinos and 128 SEZs across Southeast Asia's Borderlands.[43] In these areas, scam compounds and the organizations who run them can thrive.

Scam-compound networks may also facilitate other forms of exploitation, including sexual exploitation and the trafficking of children. Workers can face discrimination, violence, or sexual abuse based on their gender, nationality, or perceived economic value. Traffickers deliberately separate and pit workers against each other to foster distrust and prevent them from organizing or resisting their captors.[44] Victims are unable to leave the scam compounds and tortured for various reasons. If they try to escape, in some cases, they may be killed and have their organs harvested.[45] On top of human trafficking for labor, these crime syndicates also engage in other forms of trafficking such as child and sex trafficking. As a function of the latter, brothels are set up inside of scam compounds as

well.[46]

Animals and the environment are also targets of these criminal networks. Wildlife trafficking is widespread, in which coveted animal parts such as ivory, pangolin scales, and tiger pelts are sold illegally for significant profit. Exotic meat farms and the sale of live animals are also a part of this animal exploitation infrastructure. Illegal gold and rare earth mineral mining results in river poisoning, mercury contamination, deforestation, air pollution, and wildlife displacement.[47]

In a region with weak rule of law and diminished trust in public institutions, corruption inevitably thrives. Criminal syndicates work with corrupt government officials who turn a blind eye to their various transgressions. Officials can ignore illegal activity, provide fraudulent permits, or protect criminal leaders. This corruption makes it more difficult to arrest organizers, preserve evidence, and rescue trafficked workers. This is especially harmful when it comes to physically shutting down scam compounds and rescuing victims. For instance, corrupt officials may warn compounds when a raid is about to occur, allowing the criminals to escape and bring workers with them, which reduces the number of victims able to be saved.[48] In one instance in 2022, Cambodian officials were thought to be complicit with Chinese nationals running scam compounds. This resulted in the relative failure of a series of raids by the Thai police on scam compounds in Cambodia. The police estimated that they could save 3,000 Thai nationals being forced to work at these compounds, but only 66 people were rescued. Among those saved, some corroborated reports stated government corruption directly aided the scammers.[49]

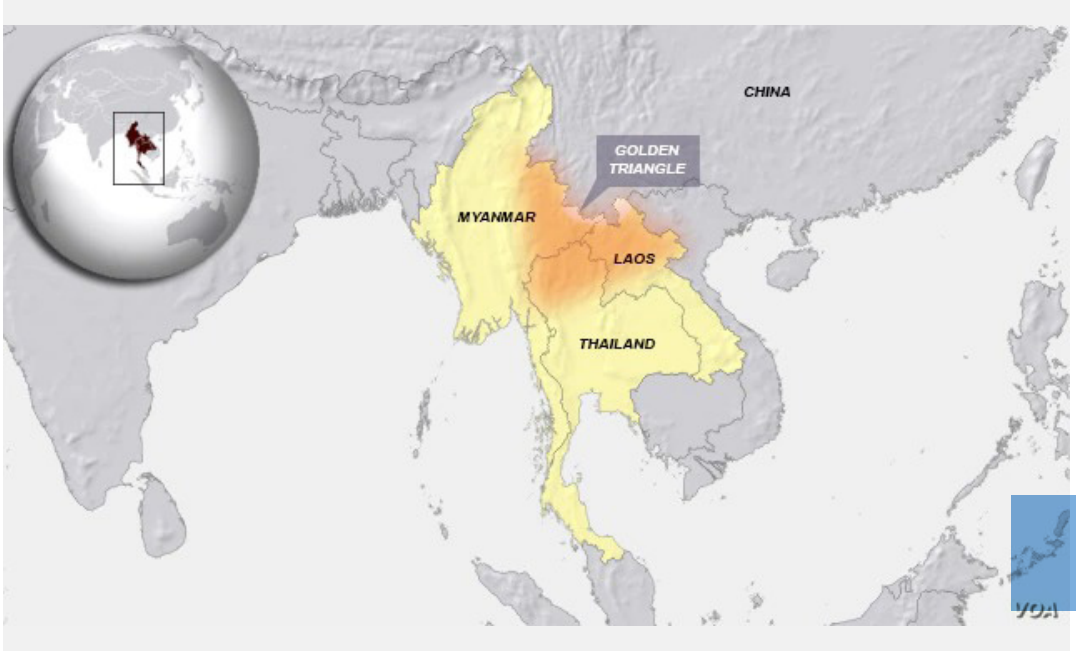
Over time, profits generated by scam compounds can weaken governance in the communities where they operate. Criminal organizations may use those profits to bribe officials, finance armed groups, purchase legitimate businesses, and expand control over local economies. This can reduce public trust in law enforcement, discourage legitimate investment, and make local governments increasingly dependent on or vulnerable to criminal networks.[50]

SOUTHEAST CENTRALIZATION

As a result of crackdowns in China, crime syndicates expanded beyond the country's borders and diversified their approach.[51] Although these operations initially targeted Chinese citizens, they have since evolved into a transnational criminal enterprise. Today, many scam compounds are concentrated in the Golden Triangle, composed of Thailand, Laos, and northern Myanmar. Cambodia is also a major hub. While many of these compounds continue to target Chinese-speaking victims, they increasingly traffic individuals from around the world. Tens of thousands of victims are trafficked into these compounds each year, including victims from South America, East Africa, and Western Europe.[52]

Although forms of organized telecommunications fraud were developed by criminal networks in Taiwan and elsewhere in China, Myanmar has since become a major center for industrial-scale online scam compounds. Beginning in the late 1980s, ceasefire agreements gave some ethnic armed organizations and militias considerable control over territories and economic activity in Myanmar's borderlands. Over time, fragmented government authority and the armed groups' need for revenue allowed casinos, illicit businesses, and trafficking networks to flourish. Criminal syndicates later used this existing infrastructure and armed protection to establish modern scam compounds. These hubs mainly targeted and exploited Chinese citizens.

The number and scale of these trafficking hubs continued to expand, peaking in the early 2020s. However, in 2023, the Three Brotherhood Alliance (3BTA) took action. 3BTA is composed of three Myanmar-based ethnic armed organizations: the Arakan Army, Myanmar National Democratic Alliance Army (MNDAA), and Ta'ang National Liberation Army.



The Golden Triangle of Southeast Asia

Credit: Voice of America

They collaborated on a crackdown called Operation 1027.[53] The offensive primarily targeted Myanmar's military government and its allied forces. However, eliminating scam operations was also one of the alliance's stated objectives.[54] This was because some scam compounds operated under the protection of local militias and officials connected to Myanmar's territorial control. The alliance dismantled some major scam centers, but its regional impact was limited. Many criminal networks relocated elsewhere in Myanmar or Southeast Asia. China supported efforts to close these operations, as many were run by Chinese criminal networks and targeted Chinese citizens.

Cambodia has since developed into one of the region's largest hubs for human trafficking. From there, these operations also spread into Laos and northern Myanmar. Their proximity to China allowed traffickers to more easily target Chinese-speaking victims. Limited law enforcement throughout much of the Golden Triangle has enabled these criminal organizations to establish, expand, and fortify scam compounds with relative impunity.

Although some cases like Rachel Yoong's have received international attention, the cases of thousands more remain unidentified and undocumented.[55] The centralization of these operations within Southeast Asia has made them harder to track and dismantle. Weak state capacity, corruption, and limited government interference in parts of the region allow many compounds to continue operating despite periodic crackdowns. According to INTERPOL data, 74 percent of the trafficking victims represented in that data were taken to scam centers in Southeast Asia.[56] Although law enforcement agencies have made arrests and recovered stolen funds, these efforts have largely disrupted individual operations instead of the broader criminal networks.[57] As a result, greater international cooperation and intelligence sharing remains essential to preventing these organizations from continuing to expand.[58]

Despite increased international attention, many scam compounds have continued to evolve. Criminal organizations utilize AI to create convincing fake identities, translate messages, and conduct sophisticated phishing attempts, allowing them to target victims far

beyond Southeast Asia. At the same time, these networks have expanded their recruitment through social media. They also venture into other illicit markets, including drug trafficking and the illegal arms trade.[59] As such, the threat posed by Southeast Asian scam compounds is no longer confined to the region but has become a global security challenge.

Current Status

ARTIFICIAL INTELLIGENCE

The rise of artificial intelligence (AI) has gravely impacted the operations of the scam industry. AI is incorporated into various parts of the fraud ecosystem, from generating scripts, pictures, and audio deepfakes for scammers to use to helping scammers manage multiple scams at once. Concerningly, AI can generate content that will most psychologically affect potential victims.

Agentic AI refers to systems that can independently plan and complete a series of tasks with limited human direction. In a fraud campaign, these systems could help criminals research potential victims, create personalized messages, maintain conversations, and issue payment or ransom demands.[60] The 2026 INTERPOL Global Financial Fraud Threat Assessment also found that AI-enhanced fraud is approximately 4.5 times more profitable than traditional scamming. This makes it extremely attractive to scam compounds.[61] The rise of generative AI has made it extremely easy for even unskilled individuals to get involved with and start running their own scams, lowering the barrier for entry into the industry.[62]

The AI revolution's economic aftershocks have also gravely impacted the scam ecosystem. Across the world, AI is replacing entry-level tech jobs. This had led to many people being out of work and turning to scamming out of desperation. This is especially true for people with a criminal background who struggle to find work. Sometimes, such people are economically forced into scamming under the illusion of choice.[63]

AI can be used in most romance scams, as workers chat online with victims for a period of time before convincing them to wire over a large sum of money. However, sometimes victims will demand to video call either to meet their supposed love or to confirm for themselves that they are not being conned. The appearance of the scammer is not often suited to these kinds of calls. This could be because someone does not actually look like the person they are pretending to be or because they are visibly suffering from physical abuse. In response to this, scam bosses will at times hire people who have strong interpersonal skills to further charm the victims. AI deepfake software can be layered on top of a hired person's appearances to match the look of whomever the victims believes they have been chatting with. As AI becomes more advanced, visual "tells" and glitches are less likely, making AI harder to detect and thus more dangerous in the hands of scammers.[64]

The risks of deepfake impersonation extend beyond romance scams. In January 2024, a finance employee at a Hong Kong-based company joined what appeared to be a routine video call with the company's chief financial officer and other colleagues.[65] Everyone looked and sounded authentic, but the employee was actually the only real person on the call. Scammers had used deepfake technology to imitate all the other participants. Believing their instructions were legitimate, the employee transferred approximately USD 25 million to accounts controlled by the criminals before discovering the deception.[66] This case demonstrates how AI can strengthen traditional impersonation scams by reproducing the faces and voices of trusted individuals, making common warning signs much harder to recognize.

Deepfakes are only one way AI can strengthen impersonation scams. Another scam type that has become more common due to the rise of AI

involves scammers impersonating companies such as banks, insurance agencies, or airlines. In this scam, the scammers pretend that there has been some kind of problem that requires an urgent fix. Victims are instructed to download software that looks similar to the real software these companies use. Through this process, the victim's data is harvested, whether that be biometric, financial, or something else. With this information, the scammers can then log into the victim's accounts directly and drain funds.[67]

The AI technology necessary to run these AI-powered scams is developed both by the scam compounds themselves and separately by third parties. Scam compounds have been known to develop the AI technology themselves by relying on open access code and AI-centric resources before adapting it to their own nefarious purposes.[68] However, if they lack the experts necessary for this in-house development, scam centers can also turn to outside sources. For instance, many scam centers rely on the company Huione. Huione is unofficially an underground one-stop shop for all of a scam center's financial and technological needs. This includes creating AI-powered tools specifically dedicated to the exact tasks scammers would need them for such as creating fake personas.[69]

However, AI isn't just part of the problem, it is also being leveraged as part of the solution. AI systems can examine large numbers of financial transactions in real time and identify patterns much more quickly than human investigators. For example, these systems can flag unusual changes in the amount, frequency, location, or destination of a person's transactions.[70] They can also map connections among certain accounts. This can help investigators identify money mules and larger criminal networks as a whole, instead of individual suspicious transactions.[71] Some AI models can also learn from previous fraud cases and adapt quickly as criminals change methods. Despite the advantages, AI alone cannot identify fraud. Some unusual behaviors may have legitimate explanations. Bad or biased data can cause AI systems to miss fraud or wrongly restrict innocent users.[72] Effective AI usage to fight scams therefore requires robust data, human review, and privacy protections.

I-GRIP PAYMENT INTERCEPTION TOOL

Operation Shadow Storm was launched in March 2026 as an international task force funded by the United Kingdom's Home Office.[73] It aims to identify the criminal leaders, intermediaries, shell companies, and financial networks operating behind scam compounds. The task force will use INTERPOL's international network and tools such as I-GRIP while examining connections among financial fraud, cybercrime, and human trafficking for forced criminality.[74] The Global Rapid Intervention of Payments, or I-GRIP, is one of INTERPOL's best tools for responding to cross-border financial fraud. Launched in 2022, I-GRIP is a stop-payment mechanism that helps law-enforcement agencies communicate rapidly when stolen money is transferred to another country. Since its inception, I-GRIP has already intercepted upwards of USD 200 million.[75] Its primary advantage is speed. Fraud proceeds may pass through several accounts or jurisdictions

Scam compounds have been known to develop the AI technology themselves by relying on open access code and AI-centric resources

within hours, making recovery more difficult each time the money moves.

I-GRIP does not independently monitor every transaction or automatically decide that an account is fraudulent. Instead, when national authorities identify a suspicious international payment, they can use the mechanism to contact law-enforcement counterparts in the country receiving the funds. Those authorities can then work with relevant banks or financial institutions to determine whether the transaction can legally be blocked, the account frozen, or the money returned. Investigators remain responsible for gathering evidence and determining whether criminal activity occurred.[76]

Its significance lies in its ability to unite financial institutions, law enforcement, cross-border organizations, and much more.[77] This only emphasizes the need for international cooperation. Without an established communication channel, the money may otherwise disappear before the appropriate authorities identify one another and begin cooperating.[78]

I-GRIP may support Operation Shadow Storm by helping participating countries intercept payments connected to the scam compounds under investigation. As a stop-payment mechanism, I-GRIP allows investigators to share and access data quickly. This provides a comprehensive map of information needed to prevent funds from being transferred away and lost. However, investigators still must separately analyze phone numbers, social-media profiles, bank accounts, cryptocurrency wallets, corporate records, and trafficking routes to identify the criminal leaders. Shadow Storm can connect these forms of intelligence, while I-GRIP provides a rapid channel for responding when suspicious payments cross borders.[79] It can also be used to track and work with financial institutions to investigate and gather more detailed information on criminal figureheads.

One of the most common scams are business email compromises (BECs). Recently, a large Singaporean commodity firm fell victim to this very scam.[80] On July 19th, 2024, cybercriminals impersonated a local supplier, tricking the firm into transferring USD 41 million into a fake account in Timor-Leste.[81] After the fraud was discovered, Singaporean authorities contacted INTERPOL. Rapid cooperation through I-GRIP allowed authorities in Timor-Leste to intercept most of the money, returning it back within days of the event. This marks one of the largest ever recoveries INTERPOL has had. USD 39.3 million dollars were returned to the commodity firm, but the rest of the funds had already been transferred to Indonesia.

Operation First Light 2026 provides a broader example of how I-GRIP can contribute to an international anti-fraud operation. Conducted from January through April 2026, the operation involved 97 countries and territories and targeted social-engineering scams and related money laundering.[82] Participating authorities analyzed 152,808 cases, blocked 31,014 bank accounts, solved 23,715 cases, and identified 15,606 suspects.[83] These results came from the operation as a whole, including investigations, raids, account freezes, intelligence sharing, and the use of I-GRIP. It is important to note that the entirety of the operation's success should not be attributed to I-GRIP alone. However, this example shows the potential of this technology, and how useful it is.

I-GRIP is being used today throughout numerous operations. Its versatility, speed, and reliability has supported INTERPOL's operations incredibly well. However, as much as INTERPOL's technology has grown, so has the technology of many crime syndicates. With Artificial Intelligence technologies being readily accessible throughout the world, scam operations have become harder to detect. Additionally, it has become easier to trick victims. I-GRIP proves that new technology can only address crime syndicates for so long.[84] Only with continued innovation and drive to synthesize new approaches can INTERPOL succeed in their operations.

PUBLIC-PRIVATE PARTNERSHIPS

Partnerships are essential to INTERPOL's strategy to counter scam centers through Operation Shadow Storm and beyond. The 2026 Global Fraud Summit underscored this focus point by pointing out that collaboration across borders and industries is essential to stopping the global spread of scamming as an industry. Not only must countries work with each other, but they must work with the private companies that can either enable or inhibit scamming. This coalition must come together to convince for profit companies that the latter is preferable. Private companies must not only condemn fraud with words, but with actions too.[85]

Prior to the 2026 summit on Global Fraud, 11 large, multinational tech and retail companies including Meta, OpenAI, Amazon, Google, and Microsoft signed an agreement committing to developing and deploying AI-powered defenses against scams.[86] The pledge commits various tech and retail companies to working against global fraud. Because scam operations move between social media, dating platforms, online retailers, AI tools, and financial services, action by only one company may simply push criminals onto another service. While no major actions have been taken due to the agreement, it has increased investment on the issue, and helps companies respond more consistently across platforms.

This industry accord has four primary themes: prevention, cooperation and collective learning, resilience, and public awareness. These themes encourage companies to create stronger verification mechanisms, clearer anti-scam terms, stronger enforcement, better internal resourcing and information sharing, collective learning from trends, and higher level of consumer awareness. Together, these measures address scams at several stages: verification can prevent criminals from creating false identities, detection systems can identify suspicious activity, information sharing can reveal networks operating across platforms, and public education can reduce the number of people deceived.

The accord also calls for cooperation with governments. Governments can support these commitments by establishing clearer legal requirements, improving fraud-reporting systems, increasing law-enforcement capacity, and creating lawful procedures through which companies can share relevant information.[87] While only 11 corporations signed this agreement, they are some of the largest and most powerful corporations in their respective industries. As such, by signing the agreement, these companies are challenging the rest of their industries to join the coalition against global fraud. However, the accord is voluntary and does not establish penalties when a company fails to fulfill its commitments. Its ultimate effect will therefore depend on whether signatories publish measurable results, consistently enforce their policies, and continue cooperating after the summit. The accord also calls for cooperation with governments, rather than asking governments to adopt the companies' exact commitments. Governments can support these efforts by establishing clearer legal requirements, improving fraud-reporting systems, increasing law-enforcement capacity, and creating lawful procedures through which companies can share relevant information. This division of responsibility matters because companies can restrict the use of their services, but only governments can conduct arrests, prosecutions, and many forms of asset recovery.

Between publishing the report and the end of the 2026 summit on Global Fraud, numerous other companies have pledged to work with INTERPOL, however, is necessary to counter fraud. These companies include Group-IB (a cybersecurity company), Gherson (a legal firm), and many more companies in many different fields.[88]

As part of the 2026 Global Fraud Summit, INTERPOL and the United Nations Office on Drugs and Crime developed a framework for public-private cooperation. The framework

2026 Global Fraud Summit

Credit: Bangladesh Press Information Department

includes six steps:

1. Acknowledging shared responsibility
2. Taking proactive and coordinated action to counter fraud
3. Sharing information
4. Supporting victims
5. Educating the public and businesses
6. Leveraging innovation and emerging technologies, together

These six steps lay the foundation for a coordinated response to global fraud.[89] The framework recognizes that no participant controls every part of the problem: governments possess investigative and legal authority, while private organizations control many of the platforms, payment systems, technical tools, and information used by scammers.

Companies can also specifically support government actions against fraud by pooling data. This allows INTERPOL and other police forces to act with as much information as possible. Telecom and security companies can work with police forces to gather and relay data such as phone numbers, bank accounts, crypto wallets, social media profiles, and more.[90] However, this can raise security concerns regarding user privacy. The methods in which data is collected and shared must be deeply scrutinized to ensure that data does not fall into the wrong hands and is not abused in any way.

One instance of successful public-private partnerships comes in the form of Operation Red Card 2.0. This Operation ran from December 2025 to January 2026 across 16 African countries. The operation was conducted under the African Joint Operation against Cybercrime (AFJOC). AFJOC is an initiative funded by the UK's Foreign, Commonwealth & Development Office. It was also supported by INTERPOL. The process included working with private partners, including Cybercrime Atlas, Team Cymru, Trend Micro, TRM Labs, and Uppsala Security. These partners provided data and intelligence. In this process, the multinational police force arrested 651 individuals and recovered USD 4.3 million. On top of this, hundreds of mobile phones, laptops, SIM cards, and fraudulent social media accounts were confiscated or shut down. This happened primarily across Nigeria, Kenya, and the Ivory Coast.[91]

Organizations outside law enforcement can also contribute through training and capacity building. In another instance, the Regional Support Office of the Bali Process supported INTERPOL during Operation Storm Makers II.[92] This project, an earlier INTERPOL-coordinated operation addressing trafficking and migrant smuggling, rescued 149 victims of human trafficking from scam centers and arrested the ringleaders of the operations. To support this, the RSO's Operational Capacity Building and Training Program Manager gave a training session on victim identification and support to a group of law enforcement officers from various groups.[93] This illustrates the importance of capacity building. Rather than conducting raids or making arrests itself, the RSO gave officers the skills needed to recognize trafficking, distinguish coerced workers from willing participants, and provide appropriate assistance to rescued victims.

Private organizations can also assist with tracing and recovering stolen assets.[94] Financial institutions and cryptocurrency services may identify suspicious transfers, preserve transaction records, freeze assets when legally authorized, and help return recovered funds to victims. Some governments use a portion of confiscated criminal assets to fund future enforcement or victim services.[95] However, these arrangements require clear legal safeguards. Asset recovery should prioritize victims and not create improper financial incentives for governments or private companies.

Bloc Analysis

POINTS OF DIVISION

INTERPOL has always found it difficult to move its members in a single direction, and this committee will be no exception. The organization cannot make arrests, conduct searches, or enter a member state on its own. It can only coordinate the collection and exchange of information and act with a host government's permission. It must also reconcile the competing priorities of civilian, military, national, and local police forces, which may define success differently.[96]

Despite these challenges, at its core, every delegate in this committee should be aligned about the main objectives. All participants should want to dismantle existing scam compounds, prevent their spread, and free victims. No entity in this committee actively seeks the spread of or acceptance of these scam compounds.

The real disagreements are not about goals but about method, speed, and cost. Three questions will separate the blocs. The first is whether to strike at the source of these scams or at the flow of illicit funds. Some delegates want to locate and physically dismantle compounds, while others believe the easier way to strike the scam compounds is through the money, technology, and infrastructure that keep them running. The second is a disagreement about what is realistic. Historically, the operators of these compounds have proven very adept at evading authorities. When one compound is abandoned, another often reappears across the nearest border within months. For some, every time a compound is closed is a victory. Others may see a waste of resources that do not solve the core problem. The third disagreement concerns authority – how much expanded investigative power, cross-border data-sharing, and regulation of finance and technology the committee should endorse. Every participant will draw a different red line before they start to see threads to national sovereignty, individual privacy, and legitimate businesses.

STAKEHOLDERS FAVORING STRONG, DECISIVE ACTION

This bloc wants to strike the compounds where they stand with every available tool. Its members are willing to endorse coordinated raids, arrests, extraditions, and the expanded authority needed to carry them out, and they are impatient with responses they see as treating symptoms rather

than the disease. The United Kingdom anchors the group: its Home Office funds Operation Shadow Storm and has cast itself as the leader of an international effort to hunt down overseas scammers.[97]

Each member may have their own motivations, but they agree on the urgency of the issue. Thailand, for example, has already shown its appetite for hard measures, mounting cross-border operations to liberate Thai nationals.[98] The bloc's non-governmental members supply the moral case. Human Rights Watch and the International Justice Mission frame the compounds where exploited victims are held in servitude,[99] Although there are many obstacles to maintaining the type of sustained action this bloc seeks, they work to leverage their resources aggressively.

STAKEHOLDERS FAVORING FINANCIAL AND TECHNOLOGICAL CONSTRAINTS

This bloc is skeptical that storming compounds solves anything for long because they have a tendency to reappear. Although the compounds and the people can be moved, this bloc seeks to focus on other, more vulnerable industry lifelines – financial systems, cryptocurrency, shell companies, and communications tools. Its members favor asset freezes, financial-intelligence sharing, platform takedowns, and mechanisms such as INTERPOL's I-GRIP, a stop-payment tool that has intercepted more than USD 200 million and, in one case, helped recover USD 39.3 million of a USD 41 million business-email fraud within days.[100]

The bloc's logic suits its members' positions. Transparency International's mandate is precisely the tracing of illicit financial flows, beneficial ownership, and asset recovery.[101] Meta has already demonstrated the model, disabling more than a million scam-linked accounts in a joint operation with other technology firms and law enforcement.[102] Amnesty International arrives at a similar preference from a different direction: its own research found that most compounds kept operating even after police "rescues," and it warns that raid-first approaches too often leave trafficking victims criminalized rather than protected.[103]

STAKEHOLDERS URGING CAUTION

This bloc does not defend the compounds. It

Victims of a scam center

Credit: GettyImages

distrusts the tools proposed to fight them. Its members will readily support action against clearly identified criminal sites, but they resist broad grants of investigative authority, expanded financial and technological regulation, and standing surveillance powers that could sweep in legitimate businesses. The line between an aggressive-but-lawful call center and a criminal scam operation is not always bright, and hyper-aggressive investigation risks creating tangible economic harm. The cryptocurrency industry, represented by Coinbase, is wary of any expansion of blockchain oversight; Brian Armstrong keeps a hard line against unlawful conduct while arguing that "regulation by enforcement" chills legitimate innovation.[104] Starlink illustrates the same tension from the connectivity side: its terminals have been found powering compounds across the Myanmar border, and while the company has disabled thousands of devices when presented with specific targets, it resists blanket restrictions on where and to whom it may sell.[105]

The states in this bloc make similar arguments. Countries like Laos sit closest to the problem and are the most exposed to it. Its borderlands host the region's grey special economic zones (SEZs) and casino developments – reportedly over 140 casinos and 128 SEZs. The economies here are entangled with the very networks the committee is targeting, making them protective of sovereignty and cautious about external intervention.[106] OpenAI, though a signatory to the 2026 industry accord alongside Meta, favors voluntary and technical safeguards over committee action that would broadly regulate AI tools with legitimate uses.[107]

Committee Mission

As an international police organization made up of member countries, INTERPOL cannot violate the sovereignty of any given nation. This means that INTERPOL cannot make arrests, or do searches and seizures.[108] INTERPOL's primary ability is to coordinate the collection and transmission of data and information. INTERPOL can work with the forces of member states and private companies to create task forces; however, it has no authority on its own and must have permission before acting in any given country. Thus, INTERPOL's strength comes from its collaborative and structured nature. When done properly, INTERPOL can act as a central hub that allows member states to work better and more efficiently. It is imperative that delegates keep all of this in mind throughout the committee.

There are many different avenues this committee can take to accomplish its goals, ranging from relying on modern technology to more traditional police-like forces. However, while doing so, it is imperative that the committee remembers the human aspect of this issue. Human rights must be protected at all times when any actions are taken.[109] This means recognizing that perpetrators can also be victims. Delegates must delicately balance their pursuits of apprehending and punishing criminals with the goal of helping victims. On top of this the social, political, and economic ramifications of actions taken against scam compounds must be considered, as communities can be torn asunder during and after raids.[110] The tradeoffs are numerous, meaning that delegates must fully understand the implications of their decisions, while also acting with haste.

This isn't an easy task. It is recommended that delegates look at frameworks developed by INTERPOL, human rights organizations, private companies, and other nonprofits to synthesize comprehensive plans for how to counter scam compounds. Delegates should consider how successful national or regional anti-scam programs could be adapted for international use. They should also examine previous INTERPOL operations involving financial fraud, cybercrime, human trafficking, and asset recovery to determine which methods could be expanded through Operation Shadow Storm.

Character Biographies

AUSTRALIA: HEAD OF NATIONAL SECURITY HAMISH HANSFORD

Hansford commenced this role in July 2025. He is responsible for integrating national security missions for Home Affairs and is also the National Counter Foreign Interference Coordinator and the Commonwealth CounterTerrorism Coordinator. Hansford has worked across the Australian government in cybersecurity infrastructure, law enforcement policy, COVID-19 response, border protection, transportation, intelligence, etc.[111] He worked in cybersecurity infrastructure for the Australian government from 2020 to 2025 during which he led various cybersecurity related reforms.[112]

CAMBODIA: DEPUTY PRIME MINISTER NETH SAVOEUN

Savoeun has been the deputy prime minister of Cambodia since 2023. Before he started this role, from 2008 to 2023 he was the National Police Chief. In this role, he took steps against foreign criminal activity in the Sihanoukville Province.[113] Savoeun has a deep background in law enforcement, having previously been the police chief of Phnom Penh and the head of the Penal Crimes Division's justice department. He is a longtime member of the Cambodian People's Party, the current ruling party of Cambodia that has been accused of corruption and human rights abuses.[114] Savoeun's cooperation will be essential to stamping out scam compounds in Southeast Asia.

CHINA: DIRECTOR OF THE OFFICE OF THE NATIONAL SECURITY COMMISSION CAI QI

Cai is currently the vice president of the National Security Commission Office, head of the Communist Party's central ideology school, and the chief of staff to Xi Jinping.[115] He is a longtime and committed member of the Chinese Communist Party. He is a close confidant of Xi Jinping and the fifth ranked member of the CCP. He was an executive in the General Office of the National Security Commission from 2014 to 2016. Since then, he has also been chairman of the organizing committee for the 2022 Beijing Olympic Games.[116]

FRANCE: NATIONAL DIRECTOR OF THE DNPJ CHRISTIAN SAINTE

Sainte has held this position since July 2023. Previously, he was the head of the judicial police force of Paris from 2015 to 2023 and, prior to that, he was the head of the judicial police force for Marseille.[117] He is considered particularly knowledgeable regarding organized crime, having worked on cases involving gangs and transnational crime in the past.[118] He is a reformer of police, specifically focused on public safety.[119]

GERMANY: FEDERAL MINISTER OF THE INTERIOR ALEXANDER DOBRINDT

Dobrindt has held this position since May 2025. This role involves managing internal security, public protection, and law enforcement.[120] The Federal Ministry of the Interior ensures that security policies are integrated across society. During his time in this role, Dobrindt has been particularly focused on border security and immigration. Prior to this, he has spent much of his career in various positions within the Christian Social Union political party as well as having been the Federal Minister of Transport and Digital Infrastructure from 2013 to 2017.[121]

INDIA: NATIONAL SECURITY ADVISOR AJIT DOVAL

Doval has been a National Security Advisor for the Modi government since 2019. Previously, he had a long career in law enforcement and intelligence, having worked as an undercover operative. He has been a part of high-profile hostage negotiations and takes strong stances

against militarism and terrorism. He was elected President of the International Association of Chiefs of the Police for Asia and Pacific region in 2004.[122] He founded the Vivekananda International Foundation, a public policy think tank focused on collaborative security in 2009.[123]

LAOS: MINISTER OF PUBLIC SECURITY VANTHONG KONGMANY

Lt. Gen. Vanthong Kongmany is on the forefront of the fight against scam compounds. He has described the problem as a top government priority, and draws on his extensive military background when planning police operations. From 2023 to May 2026, his department has made over 2,800 arrests in connection with scam compounds. He has made frequent visits to neighboring states to shore up diplomatic support and resources, and he has not been shy about supporting strong enforcement actions.[124]

MYANMAR: NATIONAL SECURITY ADVISOR TIN AUNG SAN

U Tin Aung San has been the National Security Advisor since April 22, 2026. His responsibilities lie in analyzing and reviewing national security, then advising the Office of the President.[125] Previously, U Tin Aung San served as the Myanmar Armed Force and the Commander-in-Chief. And in between 2021-2026, he served in senior positions under numerous administrations. He cycled between the State Administration Council, Deputy Prime Minister, Minister for Transport and Communications, Minister of Defense, Union Minister in the Prime Minister's Office, and now the National Security Advisor.[126]

THAILAND: SECRETARY-GENERAL OF THE NATIONAL SECURITY COUNCIL CHATCHAI BANGCHUAD

Bangchuad is currently serving as the Thai Secretary-General of the National Security Council at a Senior Executive Level since November 17, 2024. Bangchuad has also been consistently chosen as chief negotiator for multiple panels and international dialogues along with his numerous other positions.[127] He served from 2011-to the present, serving as directors of numerous Security Bureaus and assistant Secretary General of the National Security Council.[128]

İbrahim Kalın

Credit: Tahirselim2016

TURKEY: DIRECTOR OF THE NATIONAL INTELLIGENCE ORGANIZATION İBRAHIM KALIN

Kalin currently serves as the Director of National Intelligence and advisor to the Turkish Prime Minister. He was previously a professor at the College of the Holy Cross. He also founded the SETA foundation for Political, Economic and Social Research through 2005-2009.[129] His background contains years of experience in numerous Universities. He trained as a scholar of Islamic studies and philosophy, as well as Islamic history and culture.[130] This experience and education is vital to his role as the Director of National Intelligence.

UNITED KINGDOM: HOME SECRETARY SHABANA MAHMOOD

Mahmood has served as the British Home Secretary since September 5, 2025. She was then reappointed as of July 20, 2026. Previously serving as Lord Chancellor and Secretary of State for Justice since 2024, she has consistently been a top advocate for safer environments for British citizens.[131] Notably, she is the United Kingdom's first female Muslim Home Secretary.[132] She also enjoys running, participating in the London Marathon.[133]

VIET NAM: MINISTER OF PUBLIC SECURITY LƯƠNG TAM QUANG

Lương currently serves as Vietnam's Minister of Public Security since June 2024. He also served as a Politburo member for the 13th and 14th tenures. This means that he is part of Vietnam's top political decision-making body.[134] Notably, he served in the Vietnamese military as a general, and was a member of Vietnam's Council for National Defence and Security.[135] He is also very adamant on pushing Vietnam to develop digital databases and digitize the nation. This is shown through his work as the Chairman of the National Data Association.[136]

NGO: HUMAN RIGHTS WATCH EXECUTIVE DIRECTOR PHILIPPE BOLOPION

Formerly a United Nations Director of Human Rights Watch, Bolopion now serves as the Executive Director.[137] His role is to organize advocacy responses to crises such as in Myanmar or Burundi. He, himself, has participated in these crisis responses, traveling into conflict zones.[138] He started his career as a journalist, and was deployed to Kosovo. There, he covered ethnic violence, and the UN's administration action.[139] Through the United Nations, he would then work his way up to his position today.

NGO: GLOBAL ANTI-SCAM ALLIANCE MANAGING DIRECTOR JORIJ ABRAHAM

Abraham serves as the managing director of the Global Anti Scam Alliance.[140] This organization aims to prevent potential victims from scams. He started his career off in eCommerce in 1997, working his way through multiple store chains and organizations.[141] Most notably, he founded two companies, eVentures Europe and vZine. These were companies that supported business development and online publishing respectively.[142] His experience in the eCommerce industry is vital to understanding the digital landscape and preventing scams today.

NGO: TRANSPARENCY INTERNATIONAL CHAIR FRANÇOIS VALÉRIAN

After acting as a member of the International Board, Valérian was elected as a Transparency International Chair in 2023.[143] As a member of the International Board, he tackled 3 central issues. The Board worked on illicit financial flows, where money is illegally earned, transferred, or used across borders. They worked on political integrity to keep the powerful in check. They also worked on strategic litigation, advocating for more legal and social change.[144]

NGO: AMNESTY INTERNATIONAL SECRETARY GENERAL AGNÈS CALLAMARD

Dr. Callamard currently serves as Amnesty International's Secretary-General since 2021. She has had many years of experience in the field of human rights. She served as the United Nations Special Rapporteur in 2016.[145] She also served as the Global Freedom of Expression Director at Columbia University.[146] Throughout her career, she has had numerous publishings in the human rights, women's rights, and refugee movement fields.[147] Dr. Callamard has been a prominent figure in the human rights field for decades.

NGO: INTERNATIONAL JUSTICE MISSION CEO GARY HAUGEN

Haugen founded the International Justice Mission in 1997. Prior to this, he worked at the US Department of Justice as a civil rights attorney and as a Director in the United Nations' investigation into the aftermath of the Rwandan genocide. In addition to his anti-slavery work against human trafficking he is also heavily involved in work aiming to protect the poor from violence.[148] Haugen is very committed to his faith, Christianity and uses the Bible's teaching on justice to fuel his work.[149]

PRIVATE SECTOR: META CTO ANDREW BOSWORTH

Bosworth has held this role since January 2022. Before this, he worked at Facebook from 2006 to 2022 as a Vice President. At Facebook, he worked on multiple virtual reality-centric projects. He has also worked at Microsoft and has a degree in computer science.[150] Outside of work Bosworth is a US Army Reserve Officer as a member of the Executive Innovation Corps. He enjoys creative hobbies such as writing and photography.[151] Bosworth is involved with charity and is the vice chair on the board of directors for the Peninsula Open Space Trust.[152]

PRIVATE SECTOR: COINBASE CEO BRIAN ARMSTRONG

Armstrong co-founded Coinbase in June 2012 and has been CEO since then. Since then, he has also founded NewLimit, an anti-aging startup and ResearchHub, a public research paper repository.[153] He has expressed support for de-regulated economic zones and private companies investing in cities around the world. He believes that a long-term goal of crypto is to support the creation and protection of freedom in physical spaces all over the world.[154] He has a technical academic background in computer science and has worked as a software engineer.

PRIVATE SECTOR: STARLINK SENIOR VP OF ENGINEERING MICHAEL NICOLLS

Nicolls has worked for SpaceX, specifically Starlink, since November 2020. He became the Senior Vice President of Engineering in January 2026. He has a deep background in science, having worked for the Stanford Linear Accelerator Center, Stanford Research Institute Center for Geospace Studies, and having founded an orbital intelligence startup in the past.[155] Nicolls is interested in laying the foundation for space commerce through his work and bringing broadband connectivity to everyone on Earth.[156]

PRIVATE SECTOR: CYBERSECURITY LEAD CLINT GIBLER

Gibler has been a member of OpenAI's technical staff since May 2026. Note: OpenAI uses the title "member of technical staff" for all engineers and technical staff regardless of seniority. As a member of OpenAI's technical staff, Gibler focuses specifically on cybersecurity. Before this, he spent the majority of his career working in cybersecurity as well as spending some time in defense and as an angel investor. Outside of work, Gibler enjoys improv comedy and screenwriting. He also did Model UN in college at Case Western.[157]

Research and Preparation Questions

Your dais has prepared the following research and preparation questions as a means of providing guidance for your research process. These questions should be carefully considered, as they embody some of the main critical thought and learning objectives surrounding your topic.

1 With increased use of Artificial Intelligence leading to more efficient scam operations, what is the best way to protect victims from advanced scamming methods?

2 How responsible are corporations and tech companies in preventing online scams?

3 How can each country actively protect their citizens from human trafficking rings linked to online scam compounds?

4 What role should nonprofits play in a law enforcement-led operation?

5 Considering that I-GRIP is one of INTERPOL's strongest current resources, how accurate is it, and can its algorithm be taken advantage of?

6 How can INTERPOL and law-enforcement agencies prevent scam compound operations from moving to other under-developed countries after having been shut down?

7 How can INTERPOL support member states and organizations in successfully shutting down scam compounds in Southeast Asia for good?

Important Documents

Google et al., Industry Accord Against Online Scams & Fraud (2026), https://services.google.com/fh/files/newsletters/industryaccord.pdf.

INTERPOL, Crime Trend Update: Human Trafficking-Fueled Scam Centres (Lyon: INTERPOL, June 2025).

INTERPOL, Global Financial Fraud Threat Assessment, 2nd ed. (Lyon: INTERPOL, March 2026).

United Nations Human Rights, OHCHR Regional Office for Southeast Asia, Online Scam Operations and Their Impact on Human Rights in Southeast Asia (Bangkok: OHCHR, 2023), https://bangkok.ohchr.org/sites/default/files/documents/2025-01/online-scam-operations-2582023.pdf.

UNODC and INTERPOL, Global Fraud Summit 2026: Outcome Documents (Vienna: UNODC, March 2026), https://www.unodc.org/res/organized-crime/GFS/Global-Fraud-Summit-Outcome-Documents-English.pdf.

UNODC Regional Office for Southeast Asia and the Pacific, Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia (Bangkok: UNODC, April 2025), https://www.unodc.org/roseap/uploads/documents/Publications/2025/Inflection_Point_2025.pdf.

About the Authors

TOPIC A: TEDDY NGUYEN

Teddy Nguyen is an undergraduate at De Anza College where he studies general Chemistry to pursue a career in Dentistry. He has been involved with Model United Nations since 2021, competing as a delegate throughout his high school career. He has primarily been a crisis delegate, as well as the trainer for his team in his Junior and Senior years. Since then, he has staffed for four conferences ranging from local high school conferences to committees hosted in Honolulu, Hawai'i, as well as, of course, NHSMUN. He will also be returning to many of these conferences within the next year.

TOPIC A: PRIYANKA PATEL

Priyanka Patel is an undergraduate at Stanford University where she studies the interdisciplinary intersection of society, technology, and sustainable development. She has been involved in Model United Nations since 2019 having competed and staffed at the middle school, high school, and college levels. In high school, she founded her high school's Model UN club and interned at BestDelegate for 1.5 years. At Stanford, she is the co-captain of the competitive Stanford Model UN team and the Deputy Secretary-General of the Stanford Model United Nations Conference XXX.

Additional writing by Chris Talamo

Edited by Adam Allibhoy, Armen Bagdassarian, Ashley Block, Ana Margarita Gil, Marlon Hoffrogge, Sabeeh Mirza, Althea Turley, and Olivia Woodard

Endnotes

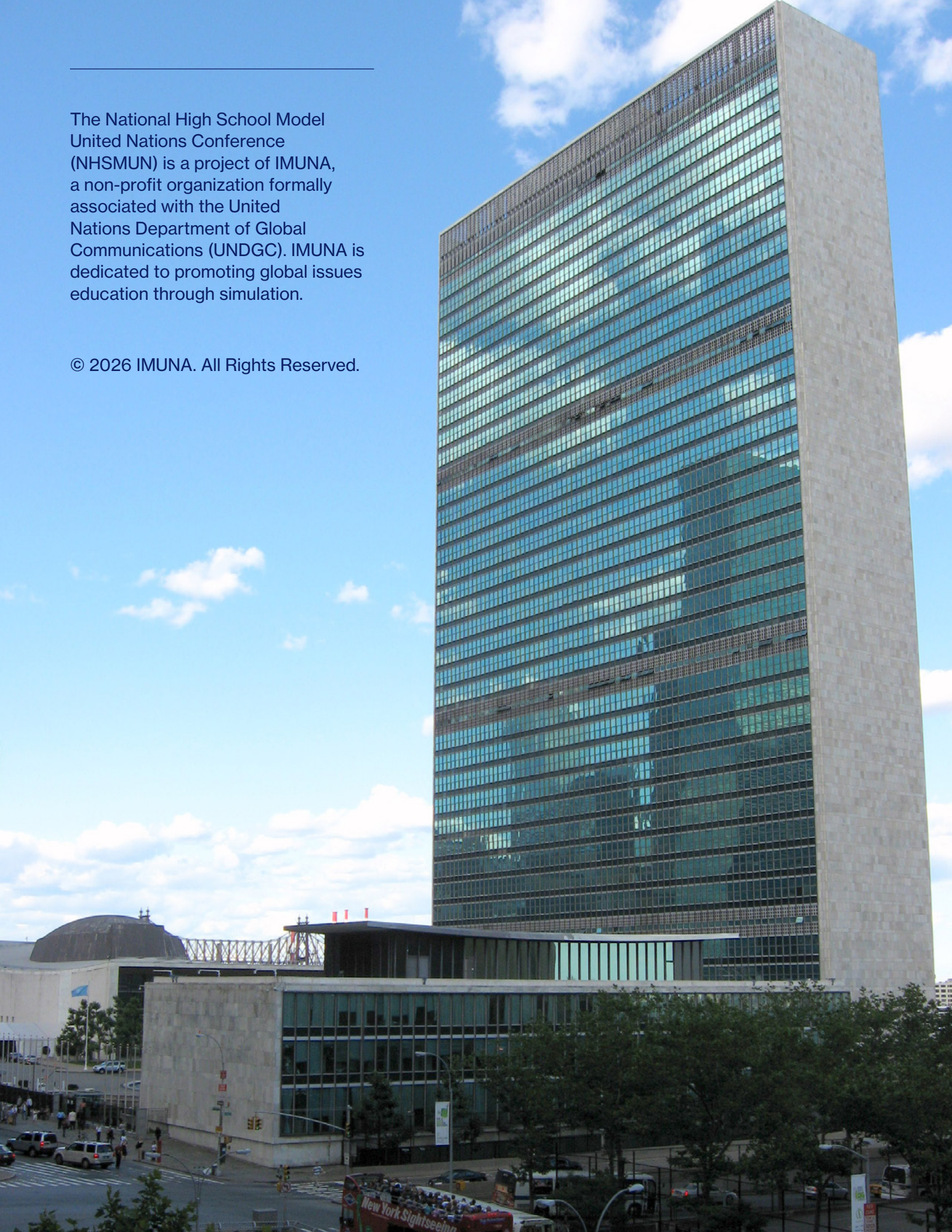
1 "What Is INTERPOL?" INTERPOL, accessed July 29, 2026, www.interpol.int/en/Who-we-are/What-is-INTERPOL.
2 Jerome L. Neapolitan, "Interpol," EBSCO Research Starters: Social Sciences and Humanities, EBSCO Information Services, 2024, www.ebsco.com/research-starters/social-sciences-and-humanities/interpol.
3 Dmytro Konovalenko, "History of Interpol and Its Main Purpose," Human Rights Lawyers, December 21, 2023,
4 INTERPOL, "INTERPOL Report Warns of Increasingly Sophisticated Global Financial Fraud Threat," news release, March 16, 2026, www.interpol.int/en/News-and-Events/News/2026/INTERPOL-report-warns-of-increasingly-sophisticated-global-financial-fraud-threat.
5 Poppy McPherson, "Crime Gangs Snare More Than $88 Billion in Scams in Asia-Pacific, UN Says," Reuters, July 21, 2026, www.reuters.com/legal/government/crime-gangs-snare-more-than-88-billion-scams-asia-pacific-un-says-2026-07-21/.
6 "Golden Triangle Special Economic Zone (GTSEZ) & Zhao Wei: Gray Zone Case Study," Not For Sale, November 25, 2025, wearenotforsale.org/human-trafficking/golden-triangle-special-economic-zone-case-study/.
7 Not For Sale, "Crypto and Human Trafficking: How Corruption Helps Scam Compounds Scale Modern-Day Slavery," July 13, 2026, https://wearenotforsale.org/human-trafficking/crypto-human-trafficking-corruption-scam-compounds/.
8 INTERPOL, "INTERPOL Report Warns of Increasingly Sophisticated Global Financial Fraud Threat," news release, March 16, 2026, https://www.interpol.int/News-and-Events/News/2026/INTERPOL-report-warns-of-increasingly-sophisticated-global-financial-fraud-threat.
9 Washington State Office of the Attorney General, "AG's Office 'Pulls Plug' on Illegal Telemarketing of Canadian Lottery," news release, January 31, 1996, www.atg.wa.gov/news/news-releases/ags-office-pulls-plug-illegal-telemarketing-canadian-lottery.
10 Marcus Moo, "Confronting Human Trafficking in the Golden Triangle," All the World, The Salvation Army International Headquarters, December 10, 2025, alltheworld.salvationarmy.org/confronting-human-trafficking/.
11 Marcus Moo, "Confronting Human Trafficking in the Golden Triangle."
12 United Nations Development Programme, Anti-Scam Handbook v1.0: Collective Response and Tools to Safeguard Development (Singapore: UNDP Policy Centre, 2024), https://www.undp.org/sites/g/files/zskgke326/files/2024-10/undp_anti-scam_handbook_v1.0.pdf.
13 UNDP, Anti-Scam Handbook v1.0.
14 Kuldeep Singh Chauhan, "Unmasking Cyber Slavery: The Hidden Truth Behind Southeast Asia's Scam Compounds," Free the Slaves, July 23, 2025, freetheslaves.net/unmasking-cyber-slavery-the-hidden-truth-behind-southeast-asias-scam-compounds/.
15 Caixin Global, "China's War on Rampant Telecom Scams," Sixth Tone, September 22, 2022, www.sixthtone.com/news/1011271.
16 Koh Ewe, "Thousands of Chinese lured abroad and forced to be scammers - now Beijing is cracking down," BBC, November 8, 2025 www.bbc.com/news/articles/c1lq95j1yp9o
17 "Cross-strait Joint-action against Crimes and Judicial Cooperation," Investigation Bureau, Ministry of Justice (Taiwan), December 12, 2016, www.mjib.gov.tw/EditPage/?PageID=90a48af8-0348-449b-bbfa-46ce0352041c.
18 Ivan Franceschini, "Sihanoukville: Rise and Fall of a Frontier City," Global China Pulse, September 16, 2024, globalchinapulse.net/sihanoukville-rise-and-fall-of-a-frontier-city/
19 US. Department of the Treasury, "Treasury Sanctions Southeast Asian Networks Targeting Americans with Cyber Scams," news release, September 8, 2025, home.treasury.gov/news/press-releases/sb0237.
20 Jing Jing Luo, "The Grey Zone of Chinese Capital: Online Gambling in Cambodia's Sihanoukville," Contemporary Southeast Asia 45, no. 3 (December 2023): 414-441, www.jstor.org/stable/27278481.
21 Childline, "Debt Bondage," June 2026, www.childline.org.uk/info-advice/bullying-abuse-safety/crime-law/debt-bondage/.
22 Associated Press, "Why Southeast Asia's Online Scam Industry Is So Hard to Shut Down," PBS NewsHour, January 8, 2026, www.pbs.org/newshour/world/why-southeast-asias-online-scam-industry-is-so-hard-to-shut-down.
23 Jason G. Tower, "Crime, Corruption, and Power: The Rise of CCP-linked Scam Networks Targeting Americans and Threatening US. Security" (testimony before the House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party, Washington, DC, May 19, 2026), docs.house.gov/meetings/ZS/ZS00/20260519/119290/HHRG-119-ZS00-Wstate-TowerJ-20260519.pdf.
24 INTERPOL, "INTERPOL Report Warns of Increasingly Sophisticated Global Financial Fraud Threat," news release, March 16, 2026, www.interpol.int/en/News-and-Events/News/2026/INTERPOL-report-warns-of-increasingly-sophisticated-global-financial-fraud-threat
25 INTERPOL, "INTERPOL Report Warns of Increasingly Sophisticated Global Financial Fraud Threat," news release, March 16, 2026, www.interpol.int/en/News-and-Events/News/2026/INTERPOL-report-warns-of-increasingly-sophisticated-global-financial-fraud-threat.
26 INTERPOL, "INTERPOL Releases New Information on Globalization of Scam Centres," news release, June 30, 2025, https://www.interpol.int/News-and-Events/News/2025/INTERPOL-releases-new-information-on-globalization-of-scam-centres.
27 INTERPOL, "INTERPOL Operation Reveals Further Insights into 'Globalization' of Cyber Scam Centres," news release, December 8, 2023, www.interpol.int/en/News-and-Events/News/2023/INTERPOL-operation-reveals-further-insights-into-globalization-of-cyber-scam-centres.
28 "Crushing Scam Farms, Southeast Asia's 'Criminal Service Providers'," United Nations Office on Drugs and Crime, July 2024, www.unodc.org/unodc/frontpage/2024/July/crushing-scam-farms—southeast-asias-criminal-service-providers.html.
29 INTERPOL, "INTERPOL Operation Reveals Further Insights into 'Globalization' of Cyber Scam Centres," news release, December 8, 2023, www.interpol.int/en/News-and-Events/News/2023/INTERPOL-operation-reveals-further-insights-into-globalization-of-cyber-scam-centres.
30 INTERPOL, "INTERPOL Operation Reveals Further Insights."
31 Charlie Campbell, "Poppies to Pig-Butchering: Inside the Golden Triangle's Criminal Reboot," TIME, March 21, 2024, time.com/6899646/scams-trafficking-drugs-southeast-asia-golden-triangle/.
32 Charlie Campbell, "Poppies to Pig-Butchering: Inside the Golden Triangle's Criminal Reboot," TIME, March 21, 2024, time.com/6899646/scams-trafficking-drugs-southeast-asia-golden-triangle/.
33 Office of the United Nations High Commissioner for Human Rights, "Victims of Trafficking Should Be Protected, Not Punished—UN Expert," news release, June 29, 2021, https://www.ohchr.org/en/press-releases/2021/06/victims-trafficking-should-be-protected-not-punished-un-expert.
34 INTERPOL, "INTERPOL Releases New Information on Globalization of Scam Centres," June 30, 2025, www.interpol.int/News-and-Events/News/2025/INTERPOL-releases-new-information-on-globalization-of-scam-centres.
35 INTERPOL, "Global Financial Fraud Threat."
36 Anran Sun, Eray Arda Akartuna, and Matthew Manning, "Employment Scams: A Crime Script and Scoping Review of Prevailing Methods, Trends and Future Directions," Trends in Organized Crime (May 26, 2026), https://doi.org/10.1007/s12117-026-09598-4
37 Not For Sale, "Crypto and Human Trafficking."
38 Sun, Akartuna, and Manning, "Employment Scams."
39 United Nations Office on Drugs and Crime, Casinos, Cyber Fraud, and Trafficking in Persons for Forced Criminality in Southeast Asia (Bangkok: UNODC Regional Office for Southeast Asia and the Pacific, September 2023), https://www.unodc.org/roseap/uploads/documents/Publications/2023/TiP_for_FC_Policy_Report.pdf

40 UNODC, Casinos, Cyber Fraud, and Trafficking in Persons.
41 Selina Ho, Xue Gong, and Carla P. Freeman, "China's Interventions in 'Gray Special Economic Zones' in Southeast Asia's Borderlands," Journal of Contemporary China, published online March 30, 2025, doi.org/10.1080/10670564.2025.2484205.
42 Not For Sale, "Golden Triangle Special Economic Zone (GTSEZ) & Zhao Wei: Gray Zone Case Study," Not For Sale, November 25, 2025, wearenotforsale.org/human-trafficking/golden-triangle-special-economic-zone-case-study/.
43 Selina Ho, Xue Gong, and Carla P. Freeman, "China's Interventions in 'Gray Special Economic Zones' in Southeast Asia's Borderlands," Journal of Contemporary China, published online March 30, 2025, doi.org/10.1080/10670564.2025.2484205.
44 Kristina Amerhauser and Audrey Thill, Compound Crime: Cyber Scam Operations in Southeast Asia (Geneva: Global Initiative Against Transnational Organized Crime, May 2025), 24, globalinitiative.net/wp-content/uploads/2025/05/GI-TOC-Compound-crime-Cyber-scam-operations-in-Southeast-Asia-May-2025.pdf.
45 Alastair McCready and Allegra Mendelson, "Survivors of Myanmar's Scam Mills Talk 'Torture,' Death, Organ Harvesting—and the Battle to Escape," Pulitzer Center, July 22, 2023, https://pulitzercenter.org/stories/survivors-myanmars-scam-mills-talk-torture-death-organ-harvesting-and-battle-escape
46 Not For Sale, "Golden Triangle Special Economic Zone (GTSEZ) & Zhao Wei: Gray Zone Case Study," Not For Sale, November 25, 2025, wearenotforsale.org/human-trafficking/golden-triangle-special-economic-zone-case-study/.
47 Not For Sale, "Golden Triangle Special Economic Zone (GTSEZ) & Zhao Wei: Gray Zone Case Study," Not For Sale, November 25, 2025, wearenotforsale.org/human-trafficking/golden-triangle-special-economic-zone-case-study/.
48 Kristina Amerhauser and Audrey Thill, Compound Crime: Cyber Scam Operations in Southeast Asia (Geneva: Global Initiative Against Transnational Organized Crime, May 2025), 24, globalinitiative.net/wp-content/uploads/2025/05/GI-TOC-Compound-crime-Cyber-scam-operations-in-Southeast-Asia-May-2025.pdf.
49 Danielle Keeton-Olsen, "Thai Police Visit Concludes With 66 Rescued, Other Victims Moved," VOD, April 12, 2022, vodenglish.news/thai-police-visit-concludes-with-66-rescued-other-victims-moved/.
50 Kristina Amerhauser and Audrey Thill, Compound Crime: Cyber Scam Operations in Southeast Asia (Geneva: Global Initiative Against Transnational Organized Crime, May 2025), 24, globalinitiative.net/wp-content/uploads/2025/05/GI-TOC-Compound-crime-Cyber-scam-operations-in-Southeast-Asia-May-2025.pdf.
51 Ivan Franceschini and Roun Ry, "Sihanoukville: Rise and Fall of a Frontier City," Global China Pulse 3, no. 1 (September 16, 2024), doi.org/10.69131/GCP.03.01.2024.03.
52 INTERPOL, "INTERPOL Issues Global Warning on Human Trafficking-Fueled Fraud," news release, June 7, 2023, www.interpol.int/en/News-and-Events/News/2023/INTERPOL-issues-global-warning-on-human-trafficking-fueled-fraud.
53 International Institute for Strategic Studies, "The Geopolitics of Southeast Asia's Cyber-scamming Crisis," in Armed Conflict Survey 2025 (London: IISS, 2025), www.iiss.org/publications/armed-conflict-survey/2025/armed-conflict-survey-2025/regional-spotlight-asia/.
54 Yun Sun, "Operation 1027: Changing the Tides of the Myanmar Civil War?" Brookings Institution, January 16, 2024, www.brookings.edu/articles/operation-1027-changing-the-tides-of-the-myanmar-civil-war/.
55 Campbell, "Poppies to Pig-Butchering."
56 Eric Priezkalns, "INTERPOL Warns of Scam Compounds Spreading to Middle East, West Africa and Central America," Commsrisk, July 2, 2025, commsrisk.com/interpol-warns-of-scam-compounds-spreading-to-middle-east-west-africa-and-central-america/.
57 Priezkalns, "INTERPOL Warns of Scam Compounds Spreading."
58 INTERPOL, "Growing Threat of Transnational Scam Centres Highlighted at INTERPOL General Assembly," news release, November 26, 2025, www.interpol.int/en/News-and-Events/News/2025/Growing-threat-of-transnational-scam-centres-highlighted-at-INTERPOL-General-Assembly.
59 INTERPOL, "Growing Threat of Transnational Scam Centres."
60 Syedur Rahman, "Interpol Issues Stark Warning About Increasingly Sophisticated Global Fraud," Rahman Ravelli, March 24, 2026, www.rahmanravelli.co.uk/expertise/multi-agency-and-multi-jurisdictional-investigations/articles/interpol-issues-stark-warning-about-increasingly-sophisticated-global-fraud/.
61 INTERPOL, "INTERPOL Report Warns of Increasingly Sophisticated Global Financial Fraud Threat," March 16, 2026, www.interpol.int/en/News-and-Events/News/2026/INTERPOL-report-warns-of-increasingly-sophisticated-global-financial-fraud-threat.
62 Press Trust of India, "Financial Fraud Siphoned $442 bn from Global Economy in 2025: Interpol," Business Standard, March 16, 2026, www.business-standard.com/world-news/financial-fraud-siphoned-usd-442-bn-from-global-economy-in-2025-interpol-126031601089_1.html.
63 Charlie Campbell, "'A Perfect Storm': How AI Is Transforming the Global Scam Industry," Time, April 7, 2026, time.com/article/2026/04/07/-a-perfect-storm-how-ai-is-transforming-the-global-scam-industry/.
64 Danny Bradbury, "Scam Compounds Hiring 'AI Models' to Seal the Deal in Deepfake Video Calls," Malwarebytes (blog), March 24, 2026, www.malwarebytes.com/blog/news/2026/03/scam-compounds-hiring-ai-models-to-seal-deal-in-deepfake-video-calls.
65 "AI: The Double-Edged Sword in Financial Crime and Fraud," LexisNexis Risk Solutions, accessed August 13, 2026, https://risk.lexisnexis.com/insights-resources/article/ai-double-edged-sword-financial-crime-fraud.
66 "AI: The Double-Edged Sword in Financial Crime and Fraud," LexisNexis Risk Solutions.
67 Charlie Campbell, "'A Perfect Storm': How AI Is Transforming the Global Scam Industry," Time, April 7, 2026, time.com/article/2026/04/07/-a-perfect-storm-how-ai-is-transforming-the-global-scam-industry/.
68 Campbell, "'A Perfect Storm': How AI Is Transforming the Global Scam Industry."
69 Chainalysis Team, "U.S. Launches New Strike Force to Combat $10 Billion Southeast Asian Scam Industry; OFAC Targets Burma-Based Cyber Scam Network," Chainalysis (blog), November 12, 2025, www.chainalysis.com/blog/ofac-targets-pig-butchering-scams-november-2025/.
70 Nasir Uddin, "Role of AI in Preventing Financial Crime: A Comprehensive Analytical Review," Journal of Economic Criminology 13 (September 2026): 100200, https://doi.org/10.1016/j.jeconc.2025.100200.
71 Uddin, "Role of AI in Preventing Financial Crime," 100200.
72 Uddin, "Role of AI in Preventing Financial Crime," 100200.
73 INTERPOL, "INTERPOL Report Warns of Increasingly Sophisticated Global Financial Fraud Threat," news release, March 16, 2026, www.interpol.int/en/News-and-Events/News/2026/INTERPOL-report-warns-of-increasingly-sophisticated-global-financial-fraud-threat.
74 INTERPOL, "INTERPOL Report Warns of Increasingly Sophisticated Global Financial Fraud Threat," news release, March 16, 2026, www.interpol.int/en/News-and-Events/News/2026/INTERPOL-report-warns-of-increasingly-sophisticated-global-financial-fraud-threat.
75 Financial Action Task Force, "FATF-INTERPOL Global Roundtable on Asset Recovery Concludes with Call for Major Mindset Shift," news release, September 20, 2023, www.fatf-gafi.org/en/publications/Methodsandtrends/FATF-Interpol-partnership.html.
76 "Interpol's Global Rapid Intervention of Payments (I-GRIP) Mechanism," Swiss Security Solutions, August 8, 2024, www.swiss-security-solutions.com/post/interpol-s-global-rapid-intervention-of-payments-i-grip-mechanism.
77 INTERPOL, "Over 5,800 Arrests, USD 293 Million Intercepted in Global Fraud Bust," news release, July 9, 2026, www.interpol.int/en/News-and-Events/News/2026/Over-5-800-arrests-USD-293-million-intercepted-in-global-fraud-bust.

78 "INTERPOL's Global Rapid Intervention of Payments (I-GRIP): A New Era in Asset Recovery," Synametrics Technologies, October 10, 2024, web.synametrics.com/interpol-s-global-rapid-intervention-of-payments-i-grip-a-new-era-in-asset-recovery-00000000161_1728573725230-arya.blog.
79 UK Home Office, "Global Taskforce Launched to Hunt Down Overseas Scammers," news release, March 17, 2026, www.gov.uk/government/news/global-taskforce-launched-to-hunt-down-overseas-scammers.
80 Kristian McCann, "I-GRIP: INTERPOL's Mechanism that Stopped a $42m BEC Fraud," Cyber Magazine, August 11, 2024, cybermagazine.com/articles/i-grip-interpols-mechanism-that-stopped-a-42m-bec-fraud.
81 INTERPOL, "INTERPOL Financial Crime Operation Makes Record 5,500 Arrests, Seizures Worth over USD 400 Million," news release, November 27, 2024, www.interpol.int/en/News-and-Events/News/2024/INTERPOL-financial-crime-operation-makes-record-5-500-arrests-seizures-worth-over-USD-400-million.
82 Paul O'Donoghue, "INTERPOL Launches Operation Shadow Storm to Fight Scam Centres," AML Intelligence, March 16, 2026, www.amlintelligence.com/2026/03/news-interpol-launches-operation-shadow-storm-to-fight-scam-centres/.
83 INTERPOL, "Over 5,800 Arrests, USD 293 Million Intercepted in Global Fraud Bust," news release, July 9, 2026, www.interpol.int/en/News-and-Events/News/2026/Over-5-800-arrests-USD-293-million-intercepted-in-global-fraud-bust.
84 "Global Fraud Summit 2026: From Fragmented Efforts to a Global Fraud Response," Chainalysis, March 19, 2026, www.chainalysis.com/blog/global-fraud-summit-2026/.
85 Reuben Vandercruyssen, "The Global Fraud Summit and the UK's Push to Lead the Anti-Fraud Agenda," Hogan Lovells Cadwalader, March 26, 2026, www.hlc.com/en/publications/the-global-fraud-summit-and-the-uks-push-to-lead-the-antifraud-agenda.
86 Chainalysis Team, "Global Fraud Summit 2026: From Fragmented Efforts to a Global Fraud Response," Chainalysis (blog), March 19, 2026, www.chainalysis.com/blog/global-fraud-summit-2026/.
87 Reuben Vandercruyssen, "The Global Fraud Summit and the UK's Push to Lead the Anti-Fraud Agenda," Hogan Lovells Cadwalader, March 26, 2026, www.hlc.com/en/publications/the-global-fraud-summit-and-the-uks-push-to-lead-the-antifraud-agenda.
88 Thomas Cattee, "INTERPOL Fraud Update – Operation Shadow Storm to Hunt Down Fraudsters," Gherson LLP (blog), March 26, 2026, www.gherson.com/blog/interpol-fraud-update-operation-shadow-storm-to-hunt-down-fraudsters/; Group-IB, "Group-IB Supports INTERPOL's Operation Synergia III, Contributing Intelligence to Global Cybercrime Takedown," press release, March 13, 2026, www.group-ib.com/media-center/press-releases/interpol-operation-synergia-3/.
89 UNODC and INTERPOL, Global Fraud Summit 2026: Outcome Documents (Vienna: UNODC, March 2026), www.unodc.org/res/organized-crime/GFS/Global-Fraud-Summit-Outcome-Documents-English.pdf.
90 Reuben Vandercruyssen, "The Global Fraud Summit and the UK's Push to Lead the Anti-Fraud Agenda," Hogan Lovells Cadwalader, March 26, 2026, www.hlc.com/en/publications/the-global-fraud-summit-and-the-uks-push-to-lead-the-antifraud-agenda.
91 INTERPOL, "Major Operation in Africa Targeting Online Scams Nets 651 Arrests, Recovers USD 4.3 Million," February 18, 2026, www.interpol.int/en/News-and-Events/News/2026/Major-operation-in-Africa-targeting-online-scams-nets-651-arrests-recovers-USD-4.3-million.
92 Regional Support Office of the Bali Process, "RSO Partnership with INTERPOL in Support of Operation Storm Makers II Sees 149 Trafficking Victims Rescued, 281 Arrested," December 21, 2023, https://rso.baliprocess.net/rso-partnership-with-interpol-in-support-of-operation-storm-makers-ii-sees-149-trafficking-victims-rescued-281-arrested/.
93 Regional Support Office of the Bali Process, "Operation Storm Makers II."
94 Regional Support Office of the Bali Process, "RSO Partnership with INTERPOL in Support of Operation Storm Makers II Sees 149 Trafficking Victims Rescued, 281 Arrested," December 21, 2023, rso.baliprocess.net/rso-partnership-with-interpol-in-support-of-operation-storm-makers-ii-sees-149-trafficking-victims-rescued-281-arrested/.
95 Hugo Plowman, Gareth Minty, and Philippa Rees, "Fraud Victims Need More: Why the Government's Global Fraud Strategy Is Missing a Trick," Mishcon de Reya, May 6, 2026, www.mishcon.com/news/fraud-victims-need-more-why-the-governments-global-fraud-strategy-is-missing-a-trick.
96 Tomasz Safjański, "Crucial Problems in the Functioning of Interpol on the Threshold of the 21st Century," Internal Security 9 (2017), doi.org/10.5604/01.3001.0010.7426.
97 UK Home Office, "Global Taskforce Launched to Hunt Down Overseas Scammers," news release, March 17, 2026, www.gov.uk/government/news/global-taskforce-launched-to-hunt-down-overseas-scammers.
98 Danielle Keeton-Olsen, "Thai Police Visit Concludes With 66 Rescued, Other Victims Moved," VOD, April 12, 2022, vodenglish.news/thai-police-visit-concludes-with-66-rescued-other-victims-moved/.
99 Kristina Amerhauser and Audrey Thill, Compound Crime: Cyber Scam Operations in Southeast Asia, Geneva: Global Initiative Against Transnational Organized Crime, May 2025, globalinitiative.net/wp-content/uploads/2025/05/GI-TOC-Compound-crime-Cyber-scam-operations-in-Southeast-Asia-May-2025.pdf.
100 Financial Action Task Force, "FATF-INTERPOL Partnership: Igniting Global Change to Take the Profit Out of Crime," September 20, 2023, www.fatf-gafi.org/en/publications/Methodsandtrends/FATF-Interpol-partnership.html.
101 "Illicit Financial Flows," Transparency International EU, accessed August 2026, transparency.eu/priority/financial-flow-crime/.
102 Meta, "Leading Tech Companies and Law Enforcement Join Forces to Disrupt Criminal Scam Networks in Southeast Asia," June 3, 2026, about.fb.com/news/2026/06/disrupting-southeast-asia-criminal-scam-networks/; Mariella Moon, "Meta Took Down over a Million Scam Accounts in Joint Operation with Microsoft, SpaceX and DOJ," Engadget, June 3, 2026.
103 Amnesty International, "Cambodia: Government allows slavery and torture to flourish inside hellish scamming compounds," June 26, 2025, www.amnesty.org/en/latest/news/2025/06/cambodia-government-allows-slavery-torture-flourish-inside-scamming-compounds/.
104 "Coinbase CEO Brian Armstrong Criticizes Regulatory Overreach," Benzinga, November 5, 2024, https://www.benzinga.com/markets/cryptocurrency/24/11/41735471/coinbase-ceo-brian-armstrong-criticizes-regulatory-overreach-nothing-to-capture-in-small-g.
105 "SpaceX Disables Thousands of Starlink Devices Being Used by Myanmar Scam Centers," CNN, October 23, 2025, www.cnn.com/2025/10/23/asia/myanmar-starlink-scam-centers-spacex-intl-hnk.
106 Selina Ho, Xue Gong, and Carla P. Freeman, "China's Interventions in 'Gray Special Economic Zones' in Southeast Asia's Borderlands," Journal of Contemporary China, published online March 30, 2025, doi.org/10.1080/10670564.2025.2484205.
107 Chainalysis Team, "Global Fraud Summit 2026: From Fragmented Efforts to a Global Fraud Response," Chainalysis (blog), March 19, 2026, www.chainalysis.com/blog/global-fraud-summit-2026/.
108 United States Government Manual, "International Criminal Police Organization (INTERPOL)–Washington," Department of Justice, last updated August 2021, www.usgovernmentmanual.gov/Agency?EntityId=BBWD6v6U+RY=&ParentEId=3jAPUb4n5pE=&EType=F2blCKa+e1g=.
109 United Nations Human Rights, OHCHR Regional Office for Southeast Asia, Online Scam Operations and Their Impact on Human Rights in Southeast Asia (Bangkok: OHCHR, 2023), bangkok.ohchr.org/sites/default/files/documents/2025-01/online-scam-operations-2582023.pdf.
110 Tess McClure, "Age of the 'Scam State': How an Illicit, Multibillion-Dollar Industry Has Taken Root in South-East Asia," The Guardian, December 2, 2025, www.theguardian.com/technology/2025/dec/02/scam-state-multi-billion-dollar-industry-south-east-asia.
111 Australian Department of Home Affairs, "Hamish Hansford," last modified May 14, 2026, https://www.homeaffairs.gov.au/about-us/who-we-

are/our-senior-staff/hamish-hansford.
112 Australian Institute of Company Directors, "Hamish Hansford," accessed August 3, 2026, https://www.aicd.com.au/about-aicd/authors-speakers/h-m/hamish-hansford.html.
113 Post Staff, "Mafia 'Not Welcome,'" Phnom Penh Post, March 16, 2015, https://phnompenhpost.com/national/mafia-not-welcome/.
114 VOA Khmer, Hun Sen Relative Tapped as Police Chief, VOA Khmer, November 11, 2008, https://khmer.voanews.com/a/a-40-2008-11-11-voa2-90166922/1359485.html.
115 Reuters Beijing Newsroom, "China Appoints Senior Official Cai Qi as Head of National Academy of Governance," Reuters, June 18, 2026, https://www.reuters.com/world/asia-pacific/china-appoints-senior-official-cai-qi-head-national-academy-governance-2026-06-18/.
116 Cheng Li and Brookings Staff, "Cai Qi ," Brookings Institution, October 2022, https://www.brookings.edu/wp-content/uploads/2022/10/20th partycongress_cai_qi.pdf.
117 AFP, "Top Paris Crime Investigator Charged with Leaks," The Guardian Nigeria, February 6, 2015, https://guardian.ng/news/world/top-paris-crime-investigator-charged-with-leaks/.
118 Chloé Triomphe, "Christian Sainte Quitte la PJ Paris et Devient Directeur National de la Police Judiciaire," Le Figaro, July 13, 2023, https://www.lefigaro.fr/actualite-france/christian-sainte-quitte-la-pj-paris-et-devient-directeur-national-de-la-police-judiciaire-20230713.
119 Lyes Si Zoubir, "Réforme de la Police: Le Patron du '36' Transféré à la Tête de la Nouvelle Direction Nationale de la PJ," Le Parisien, July 13, 2023, https://www.leparisien.fr/faits-divers/reforme-de-la-police-le-patron-du-36-transfere-a-la-tete-de-la-nouvelle-direction-nationale-de-la-pj-13-07-2023-QFB6A7HOQND75A7QLGW5ABDDBA.php.
120 Federal Ministry of the Interior and Community (Germany), "The Ministry," accessed August 3, 2026, https://www.bmi.bund.de/EN/ministry/ministry-node.html.
121 Federal Ministry of the Interior and Community (Germany), "The Federal Minister of the Interior," accessed August 3, 2026, https://www.bmi.bund.de/EN/ministry/minister/minister.html.
122 Ajit Doval, Chinese Intelligence: From a Party Outfit to Cyber Warriors, Occasional Paper (New Delhi: Vivekananda International Foundation, July 2013), https://www.vifindia.org/sites/default/files/chinese-intelligence-from-a-party-outfit-to-cyber-warriors.pdf.
123 Business Standard, "Who Is Ajit Doval," accessed August 3, 2026, https://www.business-standard.com/about/who-is-ajit-doval.
124 Phoudasack Vongsay, "Lao Security Minister Visits Golden Triangle SEZ Amid Fraud Crackdown," Laotian Times, May 4, 2026, https://laotiantimes.com/2026/05/04/lao-security-minister-visits-golden-triangle-sez-amid-fraud-crackdown/.
125 "Appointment of NSA: President Appointed U Tin Aung San as NSA," Myanmar International TV, April 23, 2026, https://www.myanmaritv.com/news/appointment-nsa-president-appointed-u-tin-aung-san-nsa.
126 "Union Minister U Tin Aung San Appointed as National Security Advisor," Eleven Myanmar, April 23, 2026, https://elevenmyanmar.com/news/union-minister-u-tin-aung-san-appointed-as-national-security-advisor-0.
127 "Chatchai Bangchuad Is Thailand's New Head of Peace Dialogue Panel," The Sun, November 27, 2023, https://thesun.my/news/world-news/chatchai-bangchuad-is-thailand-s-new-head-of-peace-dialogue-panel-di11801165/.
128 "Mr. Chatchai Bangchuad," Office of the National Economic and Social Development Council, last modified March 20, 2025, https://www.nesdc.go.th/en/about-nesdc/organizational-structure/nesdc_board/mr-chatchai-bangchuad/.
129 "Ibrahim Kalin," Building Bridges Seminar, Georgetown University, accessed August 3, 2026, https://buildingbridges.georgetown.edu/people/ibrahim-kalin.
130 "İbrahim Kalın," Middle East Institute, accessed August 3, 2026, https://mei.edu/person/ibrahim-kalin/.
131 "Shabana Mahmood," Shabana Mahmood MP, accessed August 3, 2026, https://shabanamahmood.org/.
132 "Who Is Shabana Mahmood? Pak-Origin Woman Chosen as UK's Home Secretary," NDTV, July 5, 2024, https://www.ndtv.com/world-news/who-is-shabana-mahmood-pak-origin-woman-chosen-as-uks-home-secretary-9235942.
133 William Mata, "Who Is Shabana Mahmood? Labour's Home Secretary and Potential Next Leader," LBC, March 6, 2026, https://www.lbc.co.uk/article/who-shabana-mahmood-labour-5HjdDt6_2/.
134 "Luong Tam Quang," 14th National Party Congress Website, Vietnam News Agency, accessed August 3, 2026, https://en.daihoidang.vn/nhan-su/luong-tam-quang-1257.html.
135 Dinh Truong, "General Luong Tam Quang Elected as National Assembly Deputy of the 16th Term," Cong Doan Viet Nam, March 22, 2026, https://en.congdoanvietnam.vn/thoi-su/dai-tuong-luong-tam-quang-trung-cu-dai-bieu-quoc-hoi-khoa-xvi-28840.tld.
136 "Gov't Proposes Special Legal Framework for Economic Violations without Corruption," Voice of Vietnam, August 3, 2026, https://english.vov.vn/en/politics/domestic/govt-proposes-special-legal-framework-for-economic-violations-without-corruption-post1320753.vov.
137 "Philippe Bolopion," Inter-American Dialogue, accessed August 3, 2026, https://thedialogue.org/expert/philippe-bolopion.
138 "Philippe Bolopion," Human Rights Watch, last modified June 1, 2026, https://www.hrw.org/about/people/philippe-bolopion.
139 Human Rights Watch, "Philippe Bolopion to Lead Human Rights Watch," news release, November 24, 2025, https://www.hrw.org/news/2025/11/24/philippe-bolopion-to-lead-human-rights-watch.
140 "Jorij Abraham, GASA," HardenStance Events, accessed August 3, 2026, https://events.hardenstance.com/telco-strategies-2026/jorij-abraham-gasa/.
141 "Jorij Abraham," Global Anti-Scam Summit (GASS) Asia 2025, Global Anti-Scam Alliance, accessed August 3, 2026, https://events.gasa.org/gass-asia2025/speaker/1770827/jorij-abraham.
142 "Speaker – Prof Jorij Abraham," Singapore International Cyber Week, Cyber Security Agency of Singapore, last modified December 19, 2025, https://www.sicw.gov.sg/speakers/mr-jorij-abraham/.
143 "François Valérian," Transparency International School on Integrity, last modified October 7, 2025, https://transparencyschool.org/lecturer/francois-valerian/.
144 "Board of Directors," Transparency International, accessed August 3, 2026, https://www.transparency.org/en/the-organisation/board-of-directors.
145 "Our Leadership," Amnesty International, last modified June 22, 2026, https://www.amnesty.org/en/about-us/our-leadership/.
146 "Agnès Callamard," Nobel Peace Prize, November 7, 2023, https://www.nobelpeaceprize.org/iran-burning-for-democracy-1/agnes-callamard.
147 "Agnès S. Callamard," Knight First Amendment Institute at Columbia University, accessed August 3, 2026, https://knightcolumbia.org/bios/view/agnes-callamard.
148 International Justice Mission, "Gary A. Haugen," accessed August 3, 2026, https://www.ijm.org/people/gary-a-haugen.
149 National Association of Evangelicals, "Gary Haugen: IJM, Justice, Violence, Hope, Joy," accessed August 3, 2026, https://www.nae.org/gary-haugen-ijm-justice-violence-hope-joy/.
150 Bosworth, Andrew. "Andrew Bosworth." LinkedIn. Accessed August 3, 2026. https://www.linkedin.com/in/andrew-bosworth-8247a01.
151 Bosworth, Andrew. "About." Boz.com. Accessed August 3, 2026. https://boz.com/about.
152 Open Space Trust. "Staff." Accessed August 3, 2026. https://openspacetrust.org/staff/.
153 Armstrong, Bill. "Bill Armstrong." LinkedIn. Accessed August 3, 2026. https://www.linkedin.com/in/barmstrong.

154 Gil Duran, “The Most Powerful Crypto Bro in Washington Has Very Weird Beliefs,” The New Republic, October 1, 2024, https://newrepublic.com/article/185738/coinbase-brian-armstrong-crypto-lobbying-washington-politicians.
155 Michael Nicolls, “Michael Nicolls,” LinkedIn, accessed August 3, 2026, https://www.linkedin.com/in/michael-nicolls-84989a50.
156 Office of Space Commerce, “Michael Nicolls,” Advisory Committee on Excellence in Space (ACES), accessed August 3, 2026, https://space.commerce.gov/advisory-committee-on-excellence-in-space-aces/aces-membership/michael-nicolls/.
157 Clint Gibler, “Clint Gibler,” LinkedIn, accessed August 3, 2026, https://www.linkedin.com/in/clintgibler.

The National High School Model United Nations Conference (NHSMUN) is a project of IMUNA, a non-profit organization formally associated with the United Nations Department of Global Communications (UNDGC). IMUNA is dedicated to promoting global issues education through simulation.

© 2026 IMUNA. All Rights Reserved.