Southeast Asia
Public Policy Institute

Policy State of Play – Online fraud in Southeast Asia

20 March 2024

Introduction

Southeast Asia plays an unfortunate but significant role in the global scam industrial complex. Several countries in the region are host to criminal operations targeting victims in the region and beyond. While the number of victims of scams grows, many of those working in the scam centres are themselves victims of human trafficking operations that lock people into working in the industry often in areas located beyond the reach of local law enforcement.

The online nature of many of the scams, as well as the movement of the illicit gains makes this a truly transnational challenge in need of global cooperation and solutions. Attempts by governments to tackle scams at home will not be sufficient as long as enforcement remains weak in other jurisdictions and international cooperation is lacking.

Over the last decade, the region has earned a reputation for being a hub of online fraud and scam operations. According to a report by the UN Office on Drugs and Crimes (UNODC), profits from the scam industry in just one Mekong nation in 2021 was estimated to be between US$7.5 and US$12.5 billion.[1]

Recognizing the significance of the issue, ASEAN leaders pledged to crackdown on online fraud operations, especially those run by human traffickers during the 42nd ASEAN Summit in May 2023.[2] In a bid to do so, ASEAN has established several mechanisms to facilitate high-level discussions, enhance information and knowledge exchange, build capacity for law enforcement officials, and promote cooperation with external partners. ASEAN is also cooperating with other organizations such as INTERPOL and the UNODC.

For many international and government organisations, online fraud and scams fall under the broader rubric of 'cybercrime'. Cybercrime can be defined as any type of criminal activity that involves a computer, networks or devices connected to the internet. In contrast to other areas of cybercrime such as malware attacks, scams do not necessarily target devices themselves, though computers and online devices are exploited to facilitate offenses. Though the landscape is constantly changing, popular scams include online purchase and e-commerce scams, phishing scams, and investment scams. More recently, the rapid development and increasing sophistication of generative artificial intelligence (AI) technologies, are also being exploited by scammers to facilitate impersonation scams, for example.[3]

Across the Southeast Asia region, fake jobs, fake investment, and e-commerce scams in particular, have emerged as some of the most common form of scams. However, there is some variation across the region in terms of which is the most predominant form. For example, job scams and e-commerce scams are the most popular scam type in Singapore, with close to 10,000 cases recorded for both types in 2023.[4] Meanwhile, e-commerce scams are by far the most popular in Thailand, with other types following far behind in terms of cases recorded.[5] The prevalence of these types of scams clearly demonstrates the increasing importance of cooperation between authorities and industry players in both the technology and financial services sectors.

From a legislative standpoint, most countries in Southeast Asia have already passed, or are moving towards introducing new legislation to combat scams. However, in jurisdictions such as Cambodia and Myanmar, which are home to much of the region's online fraud and scam operations, weak regulation and poor law enforcement remains a significant obstacle.

This briefing provides a snapshot of policy developments across the region to combat online fraud, scams, and related issues.

Singapore

Over the last few years, combatting online fraud and scams has become a major priority for the Singapore government, with losses to fraud reaching SG$652 million in 2023 (US$489 million).

To this end, the government is operationalizing the Online Criminal Harms Act (OCHA), which came into effect in February 2024.[6] OCHA will empower the relevant authorities to issue directions to restrict the exposure of Singapore users on online platforms as well as codes of practice to strengthen partnerships with online services to combat scams and malicious cyber activities.

The government has also recently introduced a slew of new measures to enhance anti-scam efforts following a parliamentary motion on digital safety and inclusion tabled in January 2024. Measures include a new 'Safe App Standard' which provides recommendations to build in malware detection capabilities in apps.

In 2022, the government set up the Anti-Scam Command (ASCom) in a bid to consolidate expertise in combating scams across the police force and enhance their abilities to disrupt scam operations and recover fraudulently gained funds. A key feature that makes ASCom unique is its co-location with staff from major retail banks, which helped to facilitate swift information sharing, fund tracing as well as the freezing of bank accounts suspected of being used for scam operations. This initiative was recently expanded, with the co-location of staff from Carousell, a popular online marketplace platform, which has significantly reduced response times.[7]

The government is also currently looking into the implementation of the Shared Responsibility Framework (SRF), which aims to reduce the risk of phishing scams. Under this framework, financial institutions and telecommunication companies are assigned anti-scam obligations, such as sending consumers outgoing transaction notifications and implementing a scam filter for SMS communications. Failure to discharge these duties adequately may result in banks and operators bearing liability. Conversely, if their duties are adequately carried out, the consumer would bear the full loss.

Beyond legislation, the government and authorities have sought to work with industry to tackle the issue. In collaboration with the Cyber Security Agency of Singapore (CSA), Google has started a new program to prevent users from sideloading applications that abuse certain Android permissions. However, such actions are ultimately voluntary.[8] Notably, the Singapore government has been increasing public pressure on industry players – most recently and publicly Meta – to increase safeguards on platforms.[9]

Malaysia

In 2023, Malaysia recorded a total of RM 1.3 billion (US$277.4 million) lost through online scams, with over 32,000 cases being reported. This marked a significant increase from the figure of RM 804 million (US$171.6 million) lost to scams in 2022.

The bulk of the losses were attributed to fake investment scams, which accounted for a record RM 421 million (US$89.8 million) out of the total lost.[10] To tackle the issue, the Malaysian government is currently reviewing the Communications and Multimedia Act to better address cybercrime. Amendments to the bill are expected to be tabled during 2024. According to the Deputy Minister for Communications, Teo Nie Ching, the amended bill will be amended to address the risks associated with artificial intelligence as well as increasing the responsibilities of service providers.[11]

The Malaysian government also recently announced in March 2023 that it is currently in the process of drafting new legislation to safeguard digital security, with provisions to hold financial institutions liable if they are found to be negligent in cases of online fraud. The proposed act shares some similarities with Singapore's SRF in that financial institutions that do not take appropriate measures to mitigate online fraud will be found liable for scams that occur and become subject to penalties.[12]

In line with Singapore, the Malaysian government has set up the National Scam Response Centre (NSRC) in 2022 to respond to scam cases and take enforcement action against scammers.[13] The center is jointly managed by the police force, Bank Negara Malaysia (the central bank of Malaysia), the Malaysia Communications and Multimedia Commission (MCMC) and the National Anti-Financial Crime Centre. The management of the centre also involves cooperation from various financial institutions.

Thailand

Between January 2022 and September 2023, the Thai police reported a total of 326,992 fraud and scam cases, with total losses amounting to THB 45 billion (US$1.25 billion). These figures are likely to be less than the actual levels of fraud.

To suppress the growth of online fraud and scams, the Thai government passed a Royal Decree on Measures for Protection and Suppression of Technology Crimes to combat cybercrime and scams in March 2023.[14] Measures introduced in the legislation include requiring financial institutions to temporarily freeze any transactions upon receiving an alert from the account holder that they might be a victim of fraud, as well as imposing information-sharing obligations on financial institutions, telcos, and other service providers. According to the Ministry of Digital Economy and Society (MDES), while losses to fraud continued to rise, the number of victims has declined thanks to the new law.[15]

MDES has also collaborated with other relevant agencies such as the Cyber Crime Investigation Bureau (CCIB) and the Bank of Thailand (BOT) to establish the Anti-Online Scam Operation Centre (AOC) in November 2023.[16] The center provides one-stop service that helps people protect their bank accounts when a security breach is suspected. The center is also empowered to freeze and track down proxy accounts that scammers have opened to lure their victims, as well as cancel the latest transactions to minimize damage.

MDES also recently announced that it was carefully considering a parliamentary proposal that recommends banks delay transfers between accounts with no prior transaction history to prevent scams. The ministry is also exploring practices in other countries such as having banks conduct call verification for such transfers. With regards, to tackling account fraud, MDES is in discussion with the BOT and Thai Bankers' Association (TBA) to freeze both first- and second-tier mule accounts suspected of fraudulent activities.[17]

Vietnam

According to figures from the Vietnamese Ministry of Information and Communications (MIC), the number of online fraud and scam cases increased by 65 percent in the first six months of 2023, compared to the same period in 2022.

In response, the government has moved to improve data security through the implementation of Decree No. 13 on Personal Data Protection. Notably Vietnam users are among the most prolific uploaders of personal data to social media platforms.[18]

The decree aims to mitigate the risk of personal data being exploited by cyber criminals by introducing technical and legal requirements for entities that process personal data.[19] Measures include obtaining an individual's consent to process their data and mechanisms for said consent to be withdrawn.

Most recently, the government has also been making progress with its plans to wind down and eventually completely phaseout its 2G network, not just because maintenance of such legacy networks is costly, but because they pose a security risk to its users as well.[20] 2G networks are often easily exploited by malicious actors to distribute spam and/or fraudulent messages about bank accounts, for example. By eliminating this vulnerability and securing personal data, the government hopes to mitigate scam risk.

The State Bank of Vietnam (SBV) is also moving to protect bank accounts from increasing fraud risk by introducing more secure authentication requirements in the banking sector through Decision No. 2345, which enters effect in July 2024.[21] To deter unauthorized transactions, the decision will introduce biometric authentication for first-time mobile banking transactions (including on new or different devices) and on transactions exceeding VND 10 million (US$405) or daily transactions exceeding VND 20 million (US$810).

Philippines

Philippine police data show that in the first nine months of 2023, Filipinos collectively lost more than P155.2 million (US$2.8 million) to online fraud and scams.

While the Philippines has legislation in place to deal with scams, such as the cybercrime law and Financial Consumer Protection Act, they are not equipped to deal with the types of fraud consumers encounter today. To address present regulatory gaps, the Senate sponsored a House Bill that aims to protect citizens from financial cybercrime. Named the Anti-Financial Scamming Act (AFASA), the bill will provide the legal

basis for authorities to penalize scammers and provide legislative support to Philippine financial institutions to combat the proliferation of scammers.[22] The bill will penalize offenses such as acting as a money mule, committing social engineering schemes, and economic sabotage.

In addition, the act will also impose some obligations on financial institutions to protect their clients' bank accounts. These obligations include introducing multi-factor authentication, fraud management systems, and strengthening verification processes.

Indonesia

In 2020, Indonesia's Ministry of Communication and Information Technology (KOMINFO) recorded over 100,000 reports of online scam and fraud cases, with most cases having taken place on e-commerce and social media platforms.[23]

As a result of rapid digitalization and growing incomes, Indonesian appetite for investing has grown – a trend that is accompanied by the increasing prevalence of fake investment scams.[24] In one such case, a total of US$585 million were defrauded from 25,000 people.[25] In response to this, the government is actively working to block illegal trading websites.

In 2023, Indonesia's Commodity Futures Trading Regulatory Agency (Bappebti) blocked 1,855 websites, an increase from 2022, and 2021.[26] Meanwhile, industry players like the Indonesia Commodity & Derivatives Exchange (ICDX) are also complementing these efforts by implementing financial literacy programs to equip consumers with the information and tools to better identify fraudulent trading investment schemes.[27]

Separately, to combat online scams, especially those transmitted through telephone and SMS, KOMNINFO launched an online public whistleblowing channel for members of the public to make complaints and reports against numbers that have been used for fraud, or for the spreading of scam content such as online gambling offers and spam advertisements.[28] Following a report, officers will verify reports within 24 hours and have the telecommunications operator block the reported number.

In addition, the exploitation of generative AI technologies by scammers, such as the creation of deepfakes to run impersonation scams or gain unauthorized access to financial services continues to rise.[29]

In a bid to counter this growing digital threat, financial services are introducing more stringent identification requirements such as electronic Know Your Customer (e-KYC) measures to boost security. These requirements typically employ some additional form of biometric verification like face recognition to digitally authenticate customers before they can do things like open a bank account.

Cambodia

Unlike some Southeast Asian countries such as Singapore, Malaysia and Thailand which are primarily on the receiving end of online fraud and scams, Cambodia has emerged as a major source and host of the online fraud and scam operations that target people across Southeast Asia and beyond. That is not to say that Cambodians are not also victims of fraud.

In particular, the country has come under international spotlight for the link between scams and human trafficking, whereby unsuspecting victims are lured in and forced to work in scam compounds. Many of these illegal operations are based in Sihanoukville and Phnom Penh. According to the UN Office of the High Commissioner for Human Rights (UNOHCHR), it was estimated that about 100,000 people, with many from neighboring China, Vietnam, Thailand, and Malaysia are currently trapped in such compounds.[30]

In the case of Cambodia, effective law enforcement remains a significant challenge in the way of a meaningful local and regional solution to the issue of online fraud and scams. While the government has launched crackdowns on such operations, scam operations are still operating at scale, according to observations made by civil society groups.[31] These groups also argued that the massive 2022 crackdown did not lead to the complete elimination of scam operations and networks as they simply relocated elsewhere in Cambodia, or even to neighboring Laos and Myanmar.

Law enforcement efforts are also further complicated by corruption. According to a New York Times report, efforts by law enforcement agencies from countries such as China, Vietnam, and Indonesia to rescue their citizens who are caught up in such operations have been "stymied" by tip-offs.[32] In one such episode, the

conclusion of an operation saw Thailand's deputy national police chief accusing Cambodian counterparts of sabotaging an operation to rescue more that 3,000 Thais across the country.

Laos

Like Cambodia, Laos has also emerged as a major hub for scam operations. In particular, the Chinese-run Golden Triangle SEZ has earned itself a notorious reputation for being a hub of illegal activity including human trafficking and scamming operations. According to a UNODC report, scam compounds have been identified to be operating in casinos located within the SEZ.[33] In addition, the government is increasingly concerned over the recent intensified crackdowns on scam compounds in Myanmar, fearing that they will simply relocate to Laos.[34]

In an attempt to address the issue, the Lao government has increased its cooperation with Chinese law enforcement authorities to arrest and deport Chinese nationals who are involved in the running of the scam rings.[35] Separately, to bolster local oversight and law enforcement capabilities so that illegal activities taking place in the Golden Triangle SEZ can be reined in, the People's Supreme Court of Laos is also working on establishing a special court in the SEZ.[36] When set up, this special court could allow for the quicker processing of criminal cases in the SEZ, where Lao authorities currently do not possess the right to enter and conduct investigations.

However, observers have expressed concerns that corruption may inhibit the effectiveness of the special court.[37] According to them, having officials located within the SEZ may make them more susceptible to bribery from those suspected of running the criminal activities within the zone.

Myanmar

As the experience of Cambodia and Laos suggest, fraud and scam operations thrive best in areas where the rule of law and governance is weak. Myanmar takes this to the extreme. Embroiled in a civil conflict since the 2021 military coup, the rule of law and reach of the government has broken down in many parts across the country. This has created fertile conditions for scam operations to take root and operate with little disruption.

According to a UNOHCHR report, it is estimated that at least 120,000 people across Myanmar may be trapped in situations where they are being forced to carry out online scams and defraud people.[38] Many of these operations are physically located in weakly regulated and porous border regions along China and Thailand with limited formal law enforcement structures, oversight, and accountability – a state of affairs that is being worsened by the civil conflict.[39]

Much of these scam operations are targeting Chinese citizens, a problem which has increasingly frustrated China's government as their attempts at pressuring Myanmar's military government to address the issue has met little success.[40] However, this changed in the wake of a major offensive launched by an alliance of ethnic rebel groups in October 2023. Following the capture of towns and military posts in northern Shan state by the rebels, a crackdown on the scam compounds was launched, leading to the repatriation of thousands of trafficking victims, and the arrests of suspected ringleaders.

The Chinese government did not hesitate to leverage rebel advances to increase pressure on the national military government.[41] Overall, joint crackdowns between September and November resulted in a total of over 31,000 suspects being transferred from Myanmar to China.[42] More recently, during a meeting in Myanmar in January 2024, both governments agreed to work together to rein in the scam operations and increase security along the border.[43]

Conclusion

Online fraud and scams are yet another area where the diversity of Southeast Asia's economies creates a wide range of challenges. High income markets, such as Singapore, are primarily targets for scammers, while areas with security challenges and limited enforcement capacity host scam operations, with a different set of victims implicated.

However, the issue is front of mind for governments in the region, given its direct impact on citizens, links to organized crime, and international attention. Hence, it has become an area of significant legislative activity for almost every government in the region.

It is imperative that legislative developments create an effective landscape for addressing online fraud, and also that Southeast Asia has a seat at the table for global discussions aimed at cooperation to combat the global scam industry.

About the Southeast Asia Public Policy Institute

The Southeast Asia Public Policy Institute is a research institute based in Bangkok and Singapore, working across the region. Our mission is to support the development of solutions to the most pressing public policy challenges facing Southeast Asia in the 21st century.

The Institute works on a range of issues across sustainability, technology, public health, trade, and governance.

We convene dialogues with stakeholders and decisionmakers to drive discussion on the challenges and opportunities facing markets in the region. The Institute draws on a network of in-market researchers, advisors, and partners to provide insights and recommendations for governments, policymakers, and businesses.

We work with partners on projects to explore and drive discussion on policy challenges through:

- **Research and policy development** – in-depth research providing insights and actionable policy solutions aimed at policymakers looking to move the needle on key issues.
- **Policy dialogues and roundtables** – to present policy ideas and start a dialogue with the most relevant stakeholders holding the pen on policy development in markets across the region.

The Institute is founded on the premise that direct connection and candid, informed dialogue is crucial for both policymakers and business leaders operating in the region's changing economic and public policy landscape.

Disclaimer

This is a policy note developed by the Southeast Asia Public Policy Institute exploring policy developments in markets in Southeast Asia. It aims to provide an overview or highlight activity in the region relevant to a specific policy area and is based on public information and the insights of Institute officers that may be gathered from stakeholders working in the relevant policy space. It does not contain any confidential or business sensitive information. It is not an exhaustive study of policy, legislation or regulation and should not be used to inform investment or other business decisions.

References

[1] The exact country was not named, though many speculated that it was Cambodia.
"Casinos, cyber fraud, and trafficking in persons forced criminality in Southeast Asia," *UNODC*, September 2023, https://www.unodc.org/roseap/uploads/documents/Publications/2023/TiP_for_FC_Policy_Report.pdf.
[2] "ASEAN Leaders' Declaration on Combating Trafficking in Persons Caused by the Abuse of Technology," *ASEAN Secretariat*, May 10, 2023, https://asean2023.id/storage/news/ASEAN%20Leaders%20Declaration%20on%20Combating%20TIP%20Caused%20by%20Abuse%20of%20Technology.pdf.
[3] Chua, Nadine, "Scammers use deepfakes to create voice recordings and videos to trick victims' family, friends," *The Straits Times*, June 15, 2023, https://www.straitstimes.com/singapore/scammers-use-deepfakes-to-create-voice-recordings-and-videos-of-victims-family-friends-to-trick-them.
[4] Tang, Louisa, "Scam cases in Singapore jumped almost 50% in 2023; most victims fell for job, e-commerce cons," *CNA*, February 18, 2024, https://www.channelnewsasia.com/singapore/scams-2023-increase-50-percent-job-e-commerce-measures-4128051.
[5] Leesa-Nguansuk, Suchit, "Authorities ramp up awareness of scams," *Bangkok Post*, August 30, 2023, https://www.bangkokpost.com/business/general/2638367/authorities-ramp-up-awareness-of-scams.
[6] "Commencement of the Online Criminal Harms Act (OCHA) on 1 February 2024," *Ministry of Home Affairs Singapore*, January 30, 2024, https://www.mha.gov.sg/mediaroom/press-releases/commencement-of-the-online-criminal-harms-act-ocha-on-1-february-2024/.
[7] "Advancing the Fight against Scams," *Ministry of Home Affairs Singapore*, February 29, 2024, https://www.mha.gov.sg/mediaroom/parliamentary/committee-of-supply-debate-2024-on-advancing-the-fight-against-scams.
[8] Yong, Jun Yuan, "CSA works with Google to block sideloading of potentially risky Android apps," *The Business Times*, February 7, 2024, https://www.businesstimes.com.sg/companies-markets/csa-works-google-block-sideloading-potentially-risky-android-apps.
[9] Chua, Nadine, "Sun Xueling calls out Meta for not working with MHA to fight e-commerce scams on its platforms," *The Straits Times*, March 5, 2024, https://www.straitstimes.com/singapore/politics/sun-xueling-calls-out-meta-for-not-working-with-mha-to-fight-e-commerce-scams-on-its-platforms.
[10] Aziz, Adam, "Azalina: Govt mulls kill switch on all platforms to halt scams, reviewing laws to allow return of stolen funds to victims," *The Edge Malaysia*, February 27, 2024, https://theedgemalaysia.com/node/702506.
[11] Bernama, "Communications and Multimedia Act amendment bill to be tabled by early 2024," *Free Malaysia Today*, September 17, 2023, https://www.freemalaysiatoday.com/category/nation/2023/09/17/communications-and-multimedia-act-amendment-bill-to-be-tabled-by-early-2024/.
[12] Mahari, Hakim and Amalia Azmin, "Kulasegaran: New digital security Act to hold banks accountable for online fraud," *New Straits Times*, March 4, 2024, https://www.nst.com.my/news/nation/2024/03/1020974/kulasegaran-new-digital-security-act-hold-banks-accountable-online-fraud.
[13] Bernama, "National anti-scam centre to open this month," *Free Malaysia Today*, October 7, 2022, https://www.freemalaysiatoday.com/category/nation/2022/10/07/national-anti-scam-centre-to-open-this-month/.
[14] Somwaiya, Kowit and Usa Ua-areetham, "Thailand issues law to combat technology crimes," *LawPlus Ltd.*, 2023, https://www.lawplusltd.com/2023/04/thailand-issues-law-to-combat-technology-crimes/.
[15] Tortermvasana, Komsan, "Online fraud law sees incidents fall," *Bangkok Post*, September 26, 2023, https://www.bangkokpost.com/business/general/2652782/online-fraud-law-sees-incidents-fall.
[16] "Anti-online Scam Centre gets off the ground," *The Nation*, November 2, 2023, https://www.nationthailand.com/thailand/general/40032467.
[17] (Translated from Thai to English) "DES expedites discussion with banks on transfers to suspicious accounts," *Springnews*, March 11, 2024, https://www.springnews.co.th/news/politics/848529.
[18] "Measures to keep online scams in check," *Viet Nam News*, October 3, 2023, https://vietnamnews.vn/economy/1594625/measures-to-keep-online-scams-in-check.html.
[19] "Legal Alert on Decree 13 on Personal Data Protection," *KPMG*, 2023 https://kpmg.com/vn/en/home/insights/2023/04/legal-alert-on-decree-13.html.
[20] "Measures to keep online scams in check," *Viet Nam News*, October 3, 2023, https://vietnamnews.vn/economy/1594625/measures-to-keep-online-scams-in-check.html.
[21] "Ensuring safe and sound online payments and bankcard payments," The State Bank of Vietnam, December 22, 2023, https://www.sbv.gov.vn/webcenter/portal/en/home/sbv/news/Latestnews/Latestnews_chitiet?centerWidth=80%25&dDocName=SBV585456&leftWidth=20%25&rightWidth=0%25&showFooter=false&showHeader=false&_adf.ctrl-state=11vlqvmj31_199&_afrLoop=46831809809113466#%40%3F_afrLoop%3D46831809809113466%26centerWidth%3D80%2525%26dDocName%3DSBV585456%26leftWidth%3D20%2525%26rightWidth%3D0%2525%26showFooter%3Dfalse%26showHeader%3Dfalse%26_adf.ctrl-state%3D150iu8ojvq_4.
[22] Gonzales, Anna Leah, "BSP backs immediate passage of AFASA bill," *Philippine News Agency*, January 22, 2024, https://www.pna.gov.ph/articles/1217383.
[23] (Translated from Bahasa Indonesia to English) "Kominfo Records the Most Online Fraud Cases: Online Sales," *CNN Indonesia*, October 15, 2021, https://www.cnnindonesia.com/teknologi/20211015085350-185-708099/kominfo-catat-kasus-penipuan-online-terbanyak-jualan-online.
[24] Maulia, Erwida and Ismi Damayanti, "Indonesia's rising appetite for online investment attracts scams," *Nikkei Asia*, August 15, 2022, https://asia.nikkei.com/Spotlight/Market-Spotlight/Indonesia-s-rising-appetite-for-online-investment-attracts-scams.
[25] Nugroho, Johannes, "Arrest of Indonesia's 'Crazy Rich Surabayan' spotlights risk of robot-trading investment scams," *SCMP*, March 26, 2023, https://www.scmp.com/week-asia/article/3214725/arrest-indonesias-crazy-rich-surabayan-spotlights-risk-robot-trading-investment-scams?module=perpetual_scroll_0&pgtype=article&campaign=3214725.

[26] Kurnia, Erika, "Illegal Futures Exchange Sites Are Increasing, Investors Need to Be Careful," *Kompas*, February 20, 2024, https://www.kompas.id/baca/english/2024/02/19/en-pemblokiran-situs-ilegal-bursa-berjangka-meningkat-investor-perlu-berhati-hati.
[27] Ibid.
[28] (Translated from Bahasa Indonesia to English) "Press Online Fraud Case, Kominfo Opens ComplaintNomor.id," *KOMINFO*, November 15, 2023, https://www.kominfo.go.id/content/detail/52935/siaran-pers-no-466hmkominfo112023-tentang-tekan-kasus-penipuan-online-kominfo-buka-aduannomorid/0/siaran_pers.
[29] Molenaar, Ronald, "Unmasking fraudsters: Combating the emerging threat of deepfake fraud," *Jakarta Post*, November 21, 2023, https://www.thejakartapost.com/opinion/2023/11/21/unmasking-fraudsters-combating-the-emerging-threat-of-deepfake-fraud.html.
[30] "Hundreds of thousands trafficked to work as online scammers in SE Asia, says UN report," *UNOHCHR*, August 29, 2023 https://www.ohchr.org/en/press-releases/2023/08/hundreds-thousands-trafficked-work-online-scammers-se-asia-says-un-report.
[31] Kelliher, Fiona and Mech Dara, "Scam Victims Say Human Trafficking Still a Problem in Cambodia," *VOA News*, March 9, 2024, https://www.voanews.com/a/scam-victims-say-human-trafficking-still-a-problem-in-cambodia/7520511.html#.
[32] Wee, Sui-Lee, "They're Forced to Run Online Scams. Their Captors Are Untouchable.," *New York Times*, August 28, 2023, https://www.nytimes.com/2023/08/28/world/asia/cambodia-cyber-scam.html.
[33] "Casinos, cyber fraud, and trafficking in persons forced criminality in Southeast Asia," *UNODC*, September 2023, https://www.unodc.org/roseap/uploads/documents/Publications/2023/TiP_for_FC_Policy_Report.pdf.
[34] "Laos concerned over scam ring influx amid China's Myanmar crackdown," *Radio Free Asia*, January 12, 2024, https://www.rfa.org/english/news/laos/laos-golden-triangle-01122024024000.html.
[35] "Laos deports 462 Chinese nationals with alleged ties to Bokeo scam rings," *Radio Free Asia*, December 5, 2023, https://www.rfa.org/english/news/laos/deportation-12052023164152.html.
[36] "Laos' highest court aims for special court in lawless Golden Triangle," *Radio Free Asia*, March 12, 2024, https://www.rfa.org/english/news/laos/special-court-golden-triangle-03122024153411.html.
[37] Ibid.
[38] "Hundreds of thousands trafficked to work as online scammers in SE Asia, says UN report," *UNOHCHR*, August 29, 2023, https://www.ohchr.org/en/press-releases/2023/08/hundreds-thousands-trafficked-work-online-scammers-se-asia-says-un-report.
[39] "Online Scam Operations and Trafficking into Forced Criminality in Southeast Asia: Recommendations for a Human Rights Response," *UNOHCHR*, August 26, 2023, https://bangkok.ohchr.org/wp-content/uploads/2023/08/ONLINE-SCAM-OPERATIONS-2582023.pdf.
[40] Gan, Nectar, "How online scam warlords have made China start to lose patience with Myanmar's junta," *CNN*, December 19, 2023, https://edition.cnn.com/2023/12/19/china/myanmar-conflict-china-scam-centers-analysis-intl-hnk/index.html.
[41] Ibid.
[42] Zhang, Albee and Ryan Woo, "Myanmar hands over to China thousands of telecom fraud suspects," *Reuters*, November 22, 2023, https://www.reuters.com/world/asia-pacific/myanmar-hands-over-china-thousands-telecom-fraud-suspects-2023-11-21/.
[43] (Translated from Chinese to English) "Vice Minister Sun Weidong visits Myanmar," *Ministry of Foreign Affairs of the People's Republic of China*, January 6, 2024, https://www.mfa.gov.cn/wjbxw_new/202401/t20240106_11219372.shtml.