UNIVERSITY OF PORTSMOUTH

UoP Research Portal
Rights Retention Cover Sheet

Citation

Seoung Won Choi, Julak Lee and Mark Button (2026). 'Korean-targeted human trafficking for cyber scam operations: how Cambodia-based criminal networks exploit Korean vulnerabilities'. Deviant Behavior. DOI: https://www.doi.org/10.1080/01639625.2026.2685195

Open Access and License

This Author Accepted Manuscript is made available in accordance with the University of Portsmouth's Open Access and Institutional Rights Retention Policy.

The manuscript is distributed under the terms of the Creative Commons Attribution license (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Korean-Targeted Human Trafficking for Cyber Scam Operations: How Cambodia-Based Criminal Networks Exploit Korean Vulnerabilities

Seoung Won Choi[a] Julak Lee[b*] and Mark Button[c]

[a] Department of Public Conflict Intelligence, Chung-Ang University, Seoul, South Korea; [b] Department of Industrial Security, Chung-Ang University, Seoul, South Korea; [c] Centre for Cybercrime and Economic Crime, University of Portsmouth, Portsmouth, United Kingdom

* Correspondence concerning this article should be addressed to Julak Lee, Department of Industrial Security, Chung-Ang University, 84 Heukseok-ro, Dongjak-gu, Seoul, South Korea, 06974, Email: julaklee71@cau.ac.kr

Published 15th June 2026 at https://doi.org/10.1080/01639625.2026.2685195

Author Biographies

Seoung Won Choi, Ph. D., is a Visiting Professor in the Department of Public Conflict Intelligence at Chung-Ang University. His research interests include cybercrime, counter-fraud, and security management.

Julak Lee, Ph.D., is a Professor in the Department of Industrial Security at Chung-Ang University. His research interests include criminal justice, security management, and physical security.

Mark Button, Ph. D., is the Co-Founder and Co-Director of the Centre for Cybercrime and Economic Crime at the University of Portsmouth. His research interests include counter-fraud, cyber fraud, and economic crime.

Korean-Targeted Human Trafficking for Cyber Scam Operations: How Cambodia-Based Criminal Networks Exploit Korean Vulnerabilities

Human trafficking increasingly intersects with cyber scams, yet Korean-specific cases have received limited scholarly attention. This study offers the first in-depth analysis of Korean-targeted recruitment and exploitation pathways within human trafficking for cyber scam operations in Cambodia. Thematic analysis yielded four themes: a Korean-targeted recruitment strategy; multi-layered control and complete subjugation; exploiting Korean nationals' traits to target fellow Koreans; and Korea's financial system exploitation and scam industrialization. The findings reveal that Korea's education-employment mismatch, competitive culture, and financial infrastructure generate structural susceptibility to targeting, while Korean nationals' linguistic fluency, cultural dispositions, and digital proficiency are leveraged for cyber scam operations against fellow Koreans. Unlike earlier forms of human trafficking, this pathway involves induced voluntariness, exploitation of cultural and digital skills rather than physical labor, coercive control through addiction, and a victim-to-perpetrator transition. These findings demonstrate that human trafficking has evolved to exploit nationally specific cultural and societal conditions through digital technology, highlighting the need for country-specific analyses of sociocultural context in prevention and response efforts.

Keywords: Human Trafficking; Korean Victim; Victim-Perpetrator Transition; Industrialization of Cyber Scam

Introduction

Transnational organized crime is becoming more complex and harder to regulate, often moving faster than existing international frameworks (Button et al., 2025; United Nations Office on Drugs and Crime [UNODC], 2024). Human trafficking, once dependent on physical coercion and local exploitation, has now transformed by merging with cyber platforms. In particular, cyber scam organizations based in Southeast Asia have raised growing international concern, with Cambodia emerging as a central hub in this shift (United States Institute of Peace [USIP], 2024).

Historically, international criminal organizations involved in fraud, kidnapping, and murder used China, Laos, and Myanmar as their primary bases (Franceschini et al., 2023; Franceschini et al., 2024; Lee, 2025). However, as crackdowns intensified in these countries, many groups moved their operations to Cambodia, where regulation remains relatively weak (Lee, 2025). Amnesty International (2025) reports that at least 53 scam compounds are active across Cambodia, where human trafficking victims are held captive and forced to take part—either directly or indirectly—in cyber scams. Within these facilities, severe forms of exploitation, including forced labor, child labor, torture, and slavery, occur on a large scale. Furthermore, factors such as authoritarian governance and limited police capacity have fostered a global perception of Cambodia as lenient toward organized crime (Lee, 2025).

Before proceeding, it is necessary to clarify the two core concepts that underpin this study. Human trafficking refers to "the recruitment, transportation, transfer, harbouring or receipt of people through force, fraud or deception, with the aim of exploiting them for profit." (UNODC, n.d.-a). Cyber scams refer to digitally operated fraud, including fake investment scams, romance scams, and impersonation scams designed to deceive victims into transferring money or personal assets (Global Anti-Scam Alliance [GASA],

2025; Han and Button, 2025). In the context of this study, these two phenomena intersect: trafficking victims are coerced into running cyber scams as forced labor, rendering them simultaneously as victims of trafficking and instruments of fraud against others.

Amid the shifting landscape of international crime, Koreans have emerged as a new target group. Cases of forced confinement or abduction of Koreans in Cambodia rose sharply, from 11 in 2022 to 21 in 2023, and surged to 76 in the first half of 2024 alone (Bang, 2025). In 2024, Cambodian police raided the Mango Park complex in Kampong Speu Province—a site associated with one of the most prominent cases of compound-based trafficking in the country—where a large number of foreign nationals were detained, the majority of whom were Chinese and Korean (Narim, 2024). This form of organized human trafficking has emerged as an unprecedented threat and has been elevated to a national priority, culminating in its inclusion on the agenda of the Korea–Cambodia summit (Choi and Won, 2024).

Human trafficking is rapidly evolving and becoming more diverse, with cases involving Koreans representing an unprecedented phenomenon. As of 2025, Korea's GDP (Gross Domestic Product) stands at $1.79 trillion, ranking 13th globally (Cerity Global, 2025). Additionally, a university enrollment rate of 76.2%, among the highest worldwide (Staatssekretariat für Wirtschaft [SECO], 2025), makes Korean victims differ significantly from traditional trafficking targets, as traditional victims were often marginalized or economically vulnerable groups (UNODC, 2008). Despite this, research on organized trafficking targeting specific nationalities remains limited.

To capture the full scope of this phenomenon, this study is organized around two analytical axes. The first axis addresses Korean-specific vulnerability across two dimensions: the societal characteristics of Korea (RQ1) and the traits of Korean

nationals (RQ2). The second axis addresses the distinctiveness of this pathway, analyzing how the recruitment and exploitation processes involved in Korean-targeted trafficking diverge from earlier forms of human trafficking (RQ3). Here, 'earlier forms of human trafficking' refers to conventional trafficking patterns irrespective of geographic location. The following research questions guide the analysis.

RQ1: Which specific societal characteristics of Korea contribute to the occurrence of Korean-targeted human trafficking for cyber scam operations in Cambodia?
RQ2: Which traits of Korean nationals are exploited in cyber scams, and in what ways?
RQ3: How do the processes involved in Korean-targeted human trafficking in Cambodia diverge from earlier forms of human trafficking?

Literature Review and Theoretical Background

The Rise and Industrialization of Cyber Scams

Asia has become a global epicenter of cyber scam activity, and Korea in particular has been so severely affected that observers now describe the situation as a 'scam pandemic' (GASA, 2025; Rogers, 2024). Recent data show that 44% of Korean adults encountered a scam, with 26% suffering actual financial losses (GASA, 2025). Investment and impersonation schemes pose the greatest threat—voice phishing losses alone reached KRW 6.4 trillion (approximately USD 4.9 billion), a 98% increase from the previous year (GASA, 2025). Criminal operations have grown more sophisticated as perpetrators adopt AI (Artificial Intelligence) and deepfake technology (GASA, 2025).
More broadly, the cyber scam industry is rapidly expanding in Southeast and East Asia (Han and Button, 2025; Lazarus et al., 2025). Criminal organizations, which previously operated in a decentralized manner primarily using apartments, villas, and hotel rooms,

have scaled up and moved into large-scale scam compounds where dozens of companies are concentrated (Franceschini et al., 2023). Within these compounds, thousands of people are subjected to forced labor and human trafficking while being mobilized for cyber scams (Franceschini et al., 2024). They are increasingly industrializing their operations through sophisticated recruitment tactics and multifaceted role specialization, turning crime into a structured business (Franceschini et al., 2023; Franceschini et al., 2024). For example, pig butchering scams are hybrid romance-investment scams where criminals build trust with victims online before luring them to fake investment platforms, causing significant financial harm (Burton and Moore, 2024; Han and Button, 2025). Within the scam compounds located in Southeast Asia and elsewhere, roles are systematically divided and coordinated to carry out the scam operations: teams responsible for contacting and gaining victims' trust, teams operating the fake investment platform, teams communicating with customers, and teams handling money laundering (Han and Button, 2025).

The Evolution of Human Trafficking in the Digital Age

Human trafficking is the world's fastest-growing criminal enterprise, a global industry worth approximately $32 billion annually (U.S. Department of Justice, 2025). It has grown to become one of the most profitable criminal businesses globally, alongside drug trafficking, and continues to expand rapidly (Greenberg, 2016).

Traditionally, women and children have been the primary targets of human trafficking (Toney-Butler et al., 2023), but it has now expanded to affect individuals in all communities, and victims can be of any age, race, gender, or nationality (U.S. Department of Homeland Security, 2025). As criminal motives and methods of this crime diversify, more and more individuals are at risk of becoming potential victims.

Victims are coerced into acts against their will, with the most common forms being sexual exploitation and forced labor. Sexual exploitation primarily occurs in street prostitution or massage parlors, while forced labor manifests across various industries such as apparel, computers, agriculture, and coffee production (UNODC, n.d.-b). Recently, beyond these traditional forms of exploitation, cases of forced mobilization into cybercrime have surged, further complicating and expanding the landscape of human trafficking (Interpol, 2025; Lazarus et al., 2025). The Office of the High Commissioner for Human Rights (2023) estimates that approximately 100,000 people are held captive and coerced into working for cyber scams in inhumane conditions. Advancements in communication technology have fundamentally transformed human trafficking. These advancements enable targeted profiling through social networking services (SNS), fake job advertisements, and fraudulent website operations, as well as psychological manipulation through real-time messaging, blackmail using private photos or videos, and real-time control via GPS and apps (Ozer et al., 2025). Furthermore, cryptocurrencies and dark web markets play a key role in facilitating payment and money laundering to help traffickers evade detection, ensure anonymity, and globalize their operations (Ozer et al., 2025).

Cambodia's Criminal Infrastructure and Scam Compounds

The Collapse of the Tourism Industry Post-COVID-19 and Cambodia's Emergence as a Criminal Hub

Prior to the COVID-19 pandemic in 2019, Cambodia's tourism industry contributed approximately 12% of national GDP, generating approximately $5 billion in revenue and supporting around 600,000 direct jobs, making tourism a major pillar of the Cambodian economy (International Trade Administration, 2024). However, the

pandemic led to a severe stagnation in tourism, with empty casinos and nearby infrastructure in Sihanoukville, Poipet, Bavet, and Phnom Penh rapidly turning into heavily fortified scam compounds (USIP, 2024). As a result, Cambodia's cyber scam industry has grown to an estimated $12.5 billion annually, equivalent to half of the country's official GDP, deepening its dependence on the illegal economy (USIP, 2024).

Scam Compounds and the Inadequate Response

Cyber scam operations in Cambodia are highly fluid and adapt to different settings with ease. Some operate out of only a single apartment, while others occupy large multi-story buildings within walled compounds or entire hotels (Global Initiative, 2025). As large compounds became dispersed in Sihanoukville in 2022, thousands of 'boutique' mini-scam compounds proliferated across Cambodia's inland regions (USIP, 2024), reflecting a unique characteristic of contemporary Cambodian organized crime. These remote areas restrict access for journalists and civil society, which in turn hinders monitoring (USIP, 2024).

Cracking down on these scam compounds is difficult due to their ownership by business elites who have close ties to the political establishment (Cheung, 2022; USIP, 2024). For example, Senator Ly Yong Phat, a standing committee member of the Cambodian People's Party, openly advertises ownership of the notorious Osmachi Resort and Casino on his business website—an illustration of the ties between compound ownership and political influence (USIP, 2024). Furthermore, as Chinese capital gains access to and colludes with Cambodia’s authoritarian regime, the entire country has effectively turned into a hotbed for Chinese-linked criminal networks (Lee, 2025). Other factors, such as Cambodia’s removal from the Financial Action Task Force (FATF) 'grey list' in 2023, resulting from significant lobbying (U.S. Department of

State, n.d.-a) and its Tier 3 designation in the 2024 Trafficking in Persons Report (indicating insufficient efforts to meet minimum standards for the elimination of trafficking) (U.S. Department of State, n.d.-b), have further enabled Cambodia's scam industry to flourish (USIP, 2024).

Diversification of Targets

As Cambodian cybercrime organizations continue to evade crackdowns, their targeting strategies have shifted. While crimes targeting Chinese nationals were previously frequent, intensified crackdowns by the Chinese government and increased diplomatic pressure have led these groups to gradually choose targets from other countries (U.S.-China Economic and Security Review Commission [USCC], 2025). Although Chinese nationals are still frequently targeted, criminal groups now see citizens of developed countries like Korea as more profitable and less risky targets, leading to a significant increase in crimes targeting them (Lee, 2025; USCC, 2025).

Analysis of Previous Research

The convergence of human trafficking and cybercrime is a new criminal phenomenon promoted by the development of digital technology, fundamentally redefining the traditional understanding of human trafficking. Sykiotou (2017) conceptualized this as "cyber-trafficking," defining it as the use of cyberspace for the recruitment of victims, advertisement of victims, advertisement of their services or organs, and for attracting clients. Furthermore, Sykiotou (2017) systematized the ways in which this crime appears in various forms, including sexual exploitation, labor exploitation, exploitation through international marriage brokers, illegal adoption, and organ trafficking. Building upon this conceptual foundation, Sarkar and Shukla (2024) proposed a new

concept: "bi-directional exploitation," a cyclical structure where human trafficking victims become both targets and perpetrators of cybercrime. This model explains a chain reaction mechanism where cybercrime facilitates human trafficking, and trafficked individuals are then coerced into cybercrime activities. They highlight that the scope of targets has expanded, particularly since COVID-19, which has led to increased unemployment and internet dependency (Sarkar and Shukla, 2024). While early trafficking targets were primarily uneducated individuals, women, and children, the scope now includes educated people, particularly men proficient in English or other languages and with advanced technical backgrounds (Sarkar and Shukla, 2024; United Nations Human Rights Office of the High Commissioner [OHCHR], 2023). Furthermore, Wang and Topalli (2024) described the industrialization of online fraud through the concept of "Intimacy Manipulated Fraud Industrialization (IMFI)." As online romance scams have become more organized with established business models, chat intermediaries who deceive victims have emerged as both perpetrators and victims of human trafficking, creating a new multilayered structure of exploitation. Previously, victim–perpetrator overlap was linked to shared social or geographic proximity, which increased the likelihood of committing crimes and becoming victims (Lauritsen et al., 1991). In contrast, IMFI represents a deliberately created corporate system that operates entirely in cyberspace (Wang and Topalli, 2024). This shift extends the victim-perpetrator overlap concept into the digital realm, providing a theoretical foundation for a new crime type that combines human trafficking and cybercrime.

Methodology

Data Collection

This study investigates Korean-targeted human trafficking for cyber scam operations in

Cambodia by analyzing publicly available media content. Research on crime and particularly involving organized crime and human trafficking often faces difficulties in recruiting participants, and even when participants are available, they are typically reluctant to share detailed accounts of their experiences. Consequently, many studies rely on single-case analysis (e.g., Carter, 2021; Lazarus, 2025a; Lazarus et al., 2025). However, for crimes that attract significant social and public attention, victim interviews are often featured in investigative programs and news articles, generating publicly available data usable for research. Given the considerable media attention that Korean-targeted human trafficking in Cambodia has received, this study leverages such publicly available data to investigate the characteristics and mechanisms of this crime. The study collected data using BIG KINDS, a news database operated by the Korea Press Foundation, known for its high data reliability and ability to systematically search and classify articles from major Korean media outlets (Na and Oh, 2024). Articles were collected that included the term ‘Cambodia’ along with at least one of the keywords ‘human trafficking’, ‘abduction’, ‘confinement’, or ‘torture’. The collection period was set from September 2024 to September 2025. This period is important, as cases of employment scams and abduction/confinement in Cambodia surged dramatically from 17 and 21 cases in 2023 to 220 and 221 in 2024, with 226 and 212 cases reported in the first half of 2025 alone (Kim, 2025). The search resulted in a total of 382 news articles. After excluding 253 articles that only covered policies, statistics, or lacked incident descriptions or explanations, or were unrelated to the research topic, and removing 46 duplicates, 83 articles were analyzed. This sample size is appropriate for thematic analysis, as the study focuses on the mechanisms and processes underlying Korean-targeted trafficking rather than the statistical scope of the phenomenon.

Data Analysis

This study used Braun and Clarke's (2006) thematic analysis to investigate the mechanisms through which Cambodia-based criminal organizations target and exploit Koreans. As a key qualitative research method (Alhojailan and Ibrahim, 2012), thematic analysis enables a nuanced and detailed exploration and interpretation of diverse themes (Boyatzis, 1998), offering a comprehensive understanding of complex issues (Yardley and Marks, 2003). Braun and Clarke (2019) emphasize that thematic analysis treats researcher subjectivity and reflexivity as key resources, framing coding and theme development as creative and productive endeavors. In other words, themes are derived through the researcher's interpretive engagement; they are not mere domain summaries, but recurrent patterns of shared meaning organized around a central concept (Braun and Clarke, 2019). This flexibility makes thematic analysis particularly well-suited to the exploratory nature of the present study.

The analysis followed the procedures outlined in Table 1, with the derived themes structured according to the four components presented in Table 2. We acknowledge that media-based data can introduce selection bias and limit analytical depth compared to primary data sources such as interviews or court documents (e.g., Lazarus, 2025a). To address this, we distinguished between three content types during coding: (1) officially reported information from law enforcement, government agencies, and NGOs; (2) victim testimony as quoted or paraphrased in media accounts; and (3) journalistic interpretation or editorial framing. Content in the third category was excluded from substantive claims and used only for contextual background.

(Table 1 here)

(Table 2 here)

Each researcher independently analyzed the same data before discussing the results to reconcile differences, thereby reducing bias and enhancing consistency. Themes were allowed to emerge from the data, with existing theoretical concepts (e.g., cyber trafficking, bidirectional exploitation, IMFI) subsequently drawn upon to interpret and situate the findings within broader scholarly conversations. Since the study relied on publicly available media materials, no formal ethical approval was required.

Results

Thematic analysis yielded four major themes (Table 3): (1) Korean-Targeted Recruitment Strategy, (2) Multi-Layered Control and Complete Subjugation, (3) Exploiting Korean Nationals' Traits to Target Fellow Koreans, and (4) Korea's Financial System Exploitation and Scam Industrialization.

(Table 3 here)

Theme 1: Korean-Targeted Recruitment Strategy

Recruitment Messages Targeting Desperate Job Seekers

Criminal organizations' recruitment messages precisely target the psychological vulnerability of young people struggling to find employment. They entice victims with promises of immediate rewards using phrases like 'No experience required, immediate hire,' '10 million won in just 3 months,' and 'Quick financial independence.' During times of prolonged job searches and financial hardship, coupled with anxiety about the future, such offers are seen not as red flags but as escape routes, neutralizing victims' critical judgment. Korea's structural conditions thus function as a pre-recruitment vulnerability, one that criminal organizations exploit before any direct contact occurs.

Utilization of Diverse Digital Platforms

Human trafficking organizations use various anonymous platforms and job sites to attract victims. They run chat rooms disguised as job search or investment information channels on encrypted platforms such as Telegram and Open KakaoTalk. They monitor chat rooms and posts to identify individuals who are in financial difficulties and then evaluate their financial status, psychological urgency, and ability to take risks through conversations. Meanwhile, job sites advertise positions with professional-sounding titles such as "inbound customer service representatives for existing customers," and present simple requirements such as "Korean language skills" and "basic computer utilization skills" to minimize barriers to entry. Preferred qualifications such as "experience of living abroad" or "second language skills" are also included to lend the posting a more legitimate appearance, while being explicitly marked as optional—a deliberate tactic to broaden the applicant pool without raising suspicion.

Theme 2: Multi-layered Control and Complete Subjugation

Immediate Isolation and Identity Control

Upon arrival in Cambodia, victims' passports and mobile phones are immediately confiscated. They are unable to escape from Cambodia because all external communication routes are blocked, and they are also unable to contact family members, friends, or Korean authorities, depriving them of the opportunity to request rescue or publicize their situation. Meanwhile, large-scale complexes such as the Mango Complex are called 'prison cities' and are equipped with military-level security systems. These facilities have 3.5-meter-high steel walls, electric fences, double gates, and barred windows, and more than 15 armed guards prevent any attempts to escape. This compound environment thus functions as a self-contained architecture of control,

severing the social ties and institutional access that might otherwise enable resistance.

Anonymization and Collusion with Local Authorities

Criminal organizations refer to victims within the compound not by their real names but by numbers, and the victims themselves use aliases. This prevents bonding among captives and makes reporting or informing on the criminals difficult if a victim escapes. Furthermore, collusion with local authorities thwarts escape attempts, discouraging and demotivating victims from attempting to escape, creating a stable environment for the criminal organization to operate over extended periods. Even where physical escape remains conceivable, this institutional complicity renders it effectively futile.

Addiction Mechanism

Criminal organizations strategically employ drugs and gambling to deepen victims' psychological and economic bondage. Victims are coerced into drug use, which causes addiction that deteriorates their decision-making capability, compelling them to continue despite objectively needing to escape. Some victims are reported to have refused rescue opportunities due to drug dependence—a response that reflects not genuine volition but the predictable outcome of deliberate and sustained coercion. Victim accounts further indicate that gambling debts bind victims to the organization and compel obedience, while they are pressured to recruit acquaintances or friends to repay those debts. Moreover, legally and socially restricted activities in Korea, such as prostitution, are reported to become readily accessible within these facilities, with some victims developing addictions to these as well. That some victims described the compound as 'paradise' reflects not a willing acceptance, but the profound distortion of reality that prolonged exploitation and isolation produce. Over time, these accumulating

pressures erode the boundary between coerced and voluntary participation, laying the groundwork for victim-to-perpetrator transition.

Theme 3: Exploiting Korean Nationals' Traits to Target Fellow Koreans

Exploiting Linguistic and Cultural Competence

Criminal organizations coerce detained Koreans into committing cyber scams targeting fellow Koreans by exploiting their linguistic and cultural proficiency. They seamlessly weave contemporary Korean societal issues into conversations and meticulously mimic generational language patterns to build trust. Specifically, based on the Korean honorific culture, a polite tone is used for the elderly and a language familiar to the young. Their firsthand understanding of Korean sociocultural dynamics—acquired as native members of that culture—gives them unparalleled precision in targeting fellow Koreans. For example, investment scams exploit Korea's collectivist culture by applying peer pressure through expressions such as 'Many others are doing it too.' Relationship development is accelerated by reflecting the general Korean-style dating process that develops from favorability to interest, confession, and eventually into a romantic relationship. This linguistic and cultural sophistication is a powerful means of converting targets’ suspicion into trust, and this process takes several months to execute.

Exploiting Fellow Koreans' Deference to Public Authority

Detained Koreans' shared cultural background with their targets gives them precise knowledge of how deeply their fellow Koreans defer to public authority—a disposition they systematically exploit through impersonation schemes. Drawing on this insider knowledge, scammers impersonate institutions such as the 'Prosecutor's Office,'

'Financial Supervisory Service,' or 'Police,' deploying authoritative tones, official-sounding titles, and specialized legal terminology to simulate a legitimate government interaction. Targets are typically contacted without warning and informed that their identity has been stolen, that their bank account is under criminal investigation, or that they are implicated in a serious legal case. Detained Koreans know that fellow Koreans will instinctively treat such claims as obligations rather than choices—and exploit this certainty by steering targets toward a solution that typically involves transferring money to a fake investigation account or providing one-time passwords to allow account access. What makes this technique particularly effective is not technological sophistication but the fact that detained Koreans, as native members of Korean society, possess an intimate understanding of this disposition—allowing them to deploy it with a precision that transforms their targets' own cultural values into the instrument of their victimization.

Theme 4: Korea's Financial System Exploitation and Scam Industrialization

Building Criminal Infrastructure Exploiting the Speed of Korea's Financial System

The speed and convenience of the Korean financial system provide an ideal operating environment for criminal organizations. Overseas accounts are immediately suspicious in cyber scams targeting Koreans, so it is important to use a locally registered Korean account to ensure their reliability. Even if the account is frozen, the rapid account opening process allows traffickers to quickly create alternative accounts. A simplified loan screening process also makes it easier to fraudulently secure tens of millions of won in loans in the victim's name.

Criminals collect required documents, including a certified copy of their resident

registration, birth certificate, and seal certificate, before the victim arrives in Cambodia. These documents are requested as part of a legal employment process, but the actual purpose is to open unauthorized bank accounts and receive loans in the victim's name. The secured funds and access to a number of Korean accounts are used as capital for additional criminal activities, expanding cyber scam operations to the industrial scale and transforming victims into more active perpetrators.

Industrialization of Cyber Scams

Scam operations have evolved beyond isolated offenses into industrial-scale enterprises. The physical structure of the scam complex is reminiscent of a factory-style production system, and dozens to hundreds of computers and mobile phones are arranged in a row. Each worker is assigned the personal data of thousands of individuals to execute multiple scams at the same time. Their performance (number of contacts, response rate, success rate of fund transfer) is continuously monitored, and compensation and punishment for achieving the goal are linked to further promote the industrialization of crime.

Discussion

This study investigated a Korean-targeted recruitment and exploitation pathway within trafficking into forced criminality for cyber scams. The findings are discussed along two analytical axes. The first axis addresses Korean-specific vulnerability across two dimensions: the societal characteristics of Korea (RQ1) and the traits of Korean nationals (RQ2). The second axis addresses the distinctiveness of this pathway (RQ3), examining how the recruitment and exploitation processes documented in this study diverge from earlier forms of human trafficking. While all four themes collectively

inform the research questions, their primary correspondences are as follows: Themes 1 and 4 address RQ1 and RQ3, Theme 2 addresses RQ3, and Theme 3 addresses RQ2. The key findings are discussed below in relation to each research question.

Societal Characteristics of Korea Associated with Korean-Targeted Human Trafficking for Cyber Scam Operations in Cambodia

Regarding RQ1, Korea's societal characteristics contribute to the vulnerability of Korean nationals in several ways. Despite having one of the world's highest university enrollment rates, Korea offers relatively few high-quality job opportunities, generating widespread frustration among highly educated individuals in their 20s and 30s (SECO, 2025). The country's competitive, performance-oriented culture and pervasive use and influence of social media further amplify feelings of relative deprivation by constantly showcasing others' achievements (Cho and Lee, 2024; Chun et al., 2019; Nam and Nam, 2022; Seo, 2017). This psychological pressure leads young adults to prioritize short-term, high-income opportunities over sustainable career paths, causing them to openly express their economic desperation on anonymous digital platforms, where prolonged visibility increases their susceptibility to criminal targeting (Paek et al., 2022; Wongmahesak et al., 2025). Furthermore, Korea's 'hurry-hurry culture' (Pratamasari, 2020), often described as 'speed capitalism' (Kang, 2010), extends to the financial system, facilitating rapid account opening and loan approval (Jung, 2017; Kim and Jeong, 2023). While efficient, this convenience inadvertently creates an enabling environment in which criminal organizations can easily exploit financial infrastructure for cyber scams.

The convergence of these factors demonstrates how the 'ladder of success' in a given society can be strategically weaponized as a primary entry point for exploitation. This

phenomenon is not an isolated occurrence; rather, it reflects an emerging global trend where localized aspirations are appropriated for human trafficking. For instance, just as the pursuit of elite professional employment is exploited in Korea, similar patterns can be observed in West Africa, where dreams of athletic stardom are leveraged to recruit youth into fraudulent networks (Lazarus, 2025b). These findings underscore that in high-income or high-aspiration contexts, vulnerability is no longer defined solely by what individuals lack but by what they intensely desire, transforming legitimate sociocultural goals into conduits for transnational crime.

Traits of Korean Nationals Exploited for Cyber Scams Targeting Fellow Koreans

While RQ1 examined the structural conditions in Korean society that generate vulnerability from the outside, RQ2 shifts focus to the capabilities, competencies, and internalized dispositions that Korean nationals carry within themselves. Detained Koreans' shared cultural background with their targets allows criminal organizations to exploit these traits with a precision that would be impossible to achieve through external recruitment alone.

Their native command of the Korean language is perhaps the most immediately exploitable of these traits. By replicating natural speech patterns—including generation-specific and regional linguistic variations—detained Koreans can conduct scams that bypass the suspicion triggered by the unnatural language characteristic of earlier voice phishing schemes (Choi et al., 2017; Do, 2018).

Beyond language, their firsthand familiarity with Korean sociocultural dynamics enables them to deploy culturally calibrated psychological strategies against fellow Koreans with exceptional precision. Their understanding of collectivist norms and relationship progression patterns—dispositions they themselves embody as native

members of Korean society—allows them to anticipate and manipulate targets' responses in ways that outsiders simply could not. This extends to their precise grasp of how deeply Koreans defer to authority figures (Yoon and Han, 2008), which they leverage through impersonation schemes that trigger instinctive compliance rather than critical scrutiny. In the Korean context, IMFI (Wang and Topalli, 2024) is extended through this cultural and linguistic precision—specifically, the use of generation-specific language and Korea-specific sociocultural scripts—suggesting that IMFI operates not only through emotional manipulation but also through culturally calibrated psychological targeting.

Equally significant are Koreans' high educational attainment and digital proficiency (SECO, 2025), characteristics of the digital native generation that enable them to rapidly master complex financial scam operations. Their practiced familiarity with mobile banking and cryptocurrency trading (Korea Consumer Agency, 2016), developed through routine engagement with Korea's advanced financial infrastructure, means they can participate in technical operations such as operating fake investment platforms. These attributes effectively render detained Koreans as highly efficient 'production personnel' in organized cyber scams. This aligns with Sarkar and Shukla's (2024) observation that trafficking targets now include educated, digitally proficient individuals with advanced language skills, reflecting a broader shift toward cyber-enabled exploitation. Such culturally calibrated exploitation stands in contrast to the gendered coercion documented among female survivors in Southeast Asian scam compounds, which operates through sexual violence and reproductive control rather than linguistic and digital extraction (Li et al., 2026). This underscores that the axis of exploitation in Korean-targeted trafficking is cultural capital, not gender.

How Korean-Targeted Trafficking Diverges from Earlier Forms of Human Trafficking

Regarding RQ3, the recruitment process aligns with the deceptive 'soft' tactics documented in Bangladesh (Ullah, 2025), which prioritize the strategic exploitation of trust and promises of high income. However, a critical divergence emerges in both the nature of vulnerability and the trajectory of exploitation. While in many parts of South and Southeast Asia, rapid population growth and underdevelopment heighten these vulnerabilities, especially in rural communities with limited economic opportunities (Ullah, 2025), the Korean case is driven by relative deprivation and an education-employment mismatch, which—as documented in RQ1—facilitates 'induced voluntariness' that erodes victims' critical judgment before any direct contact with traffickers occurs. In this digital-era paradigm, victims are not merely passive objects of physical labor; they are recruited for their intellectual and digital proficiency to sustain industrialized cyber scams. Unlike earlier forms of trafficking that represent a terminal stage of exploitation, this 'Korean-targeted' pathway reflects 'bidirectional exploitation' (Sarkar and Shukla, 2024), where victims themselves produce new victims. These mechanisms are further elaborated by the trajectory of participation itself. According to Lazarus and colleagues (2025), voluntary participation in cybercrime is relatively common in West Africa, whereas forced participation is predominant in Southeast Asia. The Cambodian case targeting Koreans exhibits both of these tendencies simultaneously. Initially, victims are drawn in through 'induced voluntariness'—deceived by false job offers into believing they are pursuing legitimate employment. Upon arrival in Cambodia, however, this apparent voluntariness gives way to explicit coercion, as victims are confined in criminal compounds and subjected to imprisonment, physical abuse, and forced drug administration before being coerced into

conducting cyber scams such as romance scams, fake investment scams, and employment scams (Jeong, 2025; Won and Lee, 2025). Over time, repeated exposure to the criminal environment, economic pressures for survival, and cognitive rationalization through performing roles within the organization combine to erode the boundary between coercion and choice. The cumulative effect of these pressures can be interpreted as transforming coerced participation into voluntary engagement, as victims internalize a criminal identity and transition from objects of exploitation into agents who sustain the industry itself. Taken together, Korean-targeted trafficking appears to diverge from earlier forms in several key ways: victims are drawn in through relative deprivation rather than absolute poverty; they are exploited for their cultural knowledge and digital skills rather than physical labor; the harm does not end with the victim but can extend outward as they are compelled to victimize others; and what begins as coerced participation can gradually become internalized as part of their own identity.

Conclusion

This study examines a Korean-targeted recruitment and exploitation pathway within trafficking into forced criminality for cyber scams. The findings suggest that existing human trafficking frameworks have been adapted to exploit the sociocultural characteristics of specific nationalities through digital technology. In particular, they imply that traditional approaches focused solely on poverty reduction and educational interventions are insufficient, emphasizing the need for country-specific analyses of sociocultural context in prevention and response efforts.

The study makes both theoretical and empirical contributions. While research on scam compounds and forced criminality in Southeast Asia has grown significantly (Lazarus et al., 2026), Korean-specific cases—particularly the exploitation of Korean language

skills, cultural knowledge, and financial systems—have received limited scholarly attention. In line with calls for more victim-centered research that accounts for diverse backgrounds (Johannes et al., 2023; Wang, 2024), this study argues that educated, digitally proficient Koreans are targeted not despite their strengths, but because of them—through Korean-language scripting, impersonation of trusted authorities, and manipulation of Korea's fast and accessible financial infrastructure. In doing so, it extends Sykiotou's (2017) cyber trafficking framework to a Korean-specific context, grounding it in concrete cultural and structural conditions, and contributes to a broader understanding of how transnational criminal networks exploit nationally specific vulnerabilities in the digital age.

Despite these contributions, the study is not without limitations. Due to challenges in accessing individuals involved in illegal activities (Weitzer, 2007), it relied on secondary data such as media reports rather than direct interviews. Furthermore, the possibility of memory distortion in victim accounts due to trauma cannot be ruled out. Although we systematically distinguished between officially reported information, victim testimony, and journalistic interpretation during coding, media-based data inevitably reflect editorial choices in how cases are selected and described. Therefore, future researchers could strengthen these findings by triangulating multiple data sources—law enforcement files, NGO records, and perpetrator testimonies—and by comparing patterns across different geographic locations.

References

Alhojailan, M. I. and Ibrahim, M. 2012. "Thematic Analysis: A Critical Review of its Process and Evaluation." *West east journal of social sciences* 1(1): 39-47.

Amnesty International. 2025. "*I Was Someone Else's Property*" - *Slavery, Human Trafficking and Torture in Cambodia's Scamming Compounds.* Retrieved September 25, 2025. (https://www.amnesty.org/en/documents/asa23/9447/2025/en/).

Bang, B. 2025. "[Exclusive] Man in His 20s Charged with Human Trafficking for Extorting Money through Illegal Loans and Selling Victims to Cambodia." *Newspim*, February 28. Retrieved October 10, 2025. (https://www.newspim.com/news/view/20250228000109).

Boyatzis, R. E. 1998. *Transforming Qualitative Information: Thematic Analysis and Code Development*. Sage.

Braun, V. and Clarke, V. 2006. "Using Thematic Analysis in Psychology." *Qualitative research in psychology* 3(2): 77-101. doi: 10.1191/1478088706qp063oa.

Braun, V. and Clarke, V. 2019. "Reflecting on Reflexive Thematic Analysis." *Qualitative research in sport, exercise and health* 11(4): 589-597. doi: 10.1080/2159676X.2019.1628806.

Burton, S. L. and Moore, P. D. 2024. "Pig Butchering in Cybersecurity: A Modern Social Engineering Threat." *SocioEconomic Challenges* 8(3): 46-60. doi: 10.61093/sec.8(3).46-60.2024.

Button, M., Hock, B., Suh, J. B. and Koh, C. S. 2025. "Policing Cross-Border Fraud 'Above and Below the Surface': Mapping Actions and Developing a More Effective Global Response." *Crime, Law and Social Change* 83(1): 1-27. doi: 10.1007/s10611-024-10186-2.

Carter, E. 2021. "Distort, Extort, Deceive and Exploit: Exploring the Inner Workings of a Romance Fraud." *The British Journal of Criminology* 61(2): 283-302. doi: 10.1093/bjc/azaa072.

Cerity Global. 2025. "Top 15 Countries by GDP in 2025." Retrieved October 10, 2025. (https://www.cerityglobal.com/blogs/top-15-countries-by-gdp-in-2025/)

Cheung, R. 2022. "They Thought Their Human Trafficking Nightmare Was Over. Then Came the Police." *Vice*, October 4. Retrieved October 5, 2025. (https://www.vice.com/en/article/human-trafficking-police-corruption-cambodia/).

Cho, Y. W. and Lee, J. Y. 2024. "Social Comparison on Social Networking Service and Social Isolation among Youth: The Mediating Role of Relative Deprivation and Moderating Effect of Victim Justice Sensitivity." *Journal of Human Understanding and Counseling* 45(1): 153-174. doi: 10.30593/JHUC.45.1.6.

Choi, I. and Won, D. 2024. "[Exclusive] "Don't Even Know the Chinese Mastermind's Identity." Leading Rooms Still Thriving." *KBS News*, August 29. Retrieved September 20, 2025. (https://news.kbs.co.kr/news/pc/view/view.do?ncd=8047292).

Choi, K., Lee, J. L. and Chun, Y. T. 2017. "Voice Phishing Fraud and its Modus Operandi." *Security Journal* 30(2): 454-466. doi: 10.1057/sj.2014.49.

Chun, H., Son, H. and Woo, J. 2019. "Lived Experiences of High School Students for the "Naesin" Grading as a Norm-Referenced Evaluation." *The Korean Journal of School Psychology* 16(3): 401-431. doi: 10.16983/kjsp.2019.16.3.401.

Do, S. H. 2018. "A Study on the Phonetics of Voice Phishing." *Criminal Investigation Studies* 4(1): 67-90.

Franceschini, I., Li, L. and Bo, M. 2023. "Compound Capitalism: A Political Economy of Southeast Asia's Online Scam Operations." *Critical Asian Studies* 55(4): 575-603. doi: 10.1080/14672715.2023.2268104.

Franceschini, I., Li, L., Hu, Y., and Bo, M. 2024. "A New Type of Victim? Profiling Survivors of Modern Slavery in the Online Scam Industry in Southeast Asia." *Trends in Organized Crime*: 1-23. doi: 10.1007/s12117-024-09552-2.

Global Anti-Scam Alliance. 2025. "South Korea Faces a Scam Pandemic: Urgent Need for AI-Based Countermeasures and Centralized Governance." Retrieved October 10, 2025. (https://www.gasa.org/post/state-of-scams-in-south-korea-report-2025).

Global Initiative. 2025. *Compound Crime: Cyber Scam Operations in Southeast Asia*. Retrieved September 25, 2025. (https://globalinitiative.net/analysis/compound-crime-cyber-scam-operations-in-southeast-asia/).

Greenberg, J. 2016. "Yes, Human Trafficking Ranks No. 3 in World Crime." *Politifact*, July 27. Retrieved September 15, 2025. (https://www.politifact.com/factchecks/2016/jul/27/amy-klobuchar/yes-human-trafficking-ranks-3-world-crime/).

Han, B. and Button, M. 2025. "An Anatomy of 'Pig Butchering Scams': Chinese Victims' and Police Officers' Perspectives." *Deviant behavior*: 1-19. doi: 10.1080/01639625.2025.2453821.

International Trade Administration. 2024. "Cambodia Country Commercial Guide." Retrieved October 10, 2025. (https://www.trade.gov/country-commercial-guides/cambodia-travel-and-tourism).

Interpol. 2025. "INTERPOL Releases New Information on Globalization of Scam Centres." Retrieved October 12, 2025. (https://www.interpol.int/News-and-Events/News/2025/INTERPOL-releases-new-information-on-globalization-of-scam-centres).

Jeong, R. 2025. "Cambodia: A Hotbed of International Crime Targeting Koreans." *Sisajournal*, July 13. Retrieved September 14, 2025. (https://www.sisajournal.com/news/articleView.html?idxno=339158).

Johannes, A. E., Kusumasari, B., Hadna, A. H. and Retnandari, N. D. 2023. "Human Trafficking: A Systematic Review and Future Research Agenda." *Jurnal Kebijakan Dan Administrasi Publik* 27(2): 107-129.

Jung, J. 2017. "Open an Account in Just 5 Minutes without Visiting a Bank... The Era of Contactless Banking." *Yeonhap*, January 17. Retrieved September 13, 2025. (https://www.yna.co.kr/view/MYH20170117021200038).

Kang, J. 2010. "The Cultural Politics of 'Ppallippalli': A Study on the 'Speed Communication' in Korea." *Journal of Communication Science* 10(3): 47-80.

Kim, D. 2025. "[Exclusive] Over 200 Koreans Victimized... What Happened at a Cambodian Warehouse?" *Hankyung*, July 30. Retrieved September 13, 2025. (https://www.hankyung.com/article/202507298652i).

Kim, E. B. and Jeong, I. R. 2023. "A Study on the Improvement of User Identification of Non-Face-to-Face Financial Transactions with Messenger Phishing Case." *Journal of The Korea Institute of Information Security and Cryptology* 33(2): 353-362. doi: 10.13089/JKIISC.2023.33.2.353.

Korea Consumer Agency. 2016. *Survey on the Current Status of Mobile Banking Services.* Retrieved September 25, 2025. (https://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE07253944).

Lauritsen, J. L., Sampson, R. J. and Laub, J. H. 1991. "The Link between Offending and Victimization among Adolescents." *Criminology* 29(2): 265–292. doi: 10.1111/j.1745-9125.1991.tb01067.x.

Lazarus, S. 2025a. "Cybercriminal Networks and Operational Dynamics of Business Email Compromise (BEC) Scammers: Insights from the "black Axe"" Confraternity. *Deviant Behavior* 46(4): 456-480. doi: 10.1080/01639625.2024.2352049.

Lazarus, S. 2025b. "The Weaponization of Football Dreams in Human Trafficking Schemes." *Journal of Human Trafficking*: 1-6. doi: 10.1080/23322705.2025.2600272.

Lazarus, S., Chiang, M. and Button, M. 2025. "Assessing Human Trafficking and Cybercrime Intersections through Survivor Narratives." *Deviant Behavior*: 1-18. doi: 10.1080/01639625.2025.2470402.

Lazarus, S., Chiang, M., Dimitrova, R. S., Thu, T. T. and Essien, E. 2026. "What Do We Know About Human Trafficking and Scam Compounds in Southeast Asia (2020–2025)? A Qualitative Meta-Synthesis of Coercive Deviant Enterprises." *Deviant Behavior*: 1-33. doi: 10.1080/01639625.2025.2604138.

Lee, K. 2025. "[Exclusive] Criminals Fleeing to Cambodia over China... Two Reasons it Became the Top Overseas Hideout." *Chosun*, July 3. Retrieved September 14, 2025. (https://www.chosun.com/national/national_general/2025/07/03/OTJXQ2IKWBH4ZD3HXIQG4L47HA/).

Li, L., Liu, C. and Franceschini, I. 2026. "The Gendered Life Cycle of Forced Criminality: Female Victims in Southeast Asia's Online Scam Industry." *Critical Asian Studies* 58(1): 41-61. doi: 10.1080/14672715.2025.2588125.

Na, G. and Oh, S. Y. 2024. "Analysis on 'Short-Form' Trends Using BIG KINDS." *Korean Journal of Leisure, Recreation & Park* 48(2): 113-125.

Nam, Y. and Nam, S. K. 2022. "Consumer Happiness by Generation: Focused on MZ Generation." *The Korean Journal of Consumer and Advertising Psychology* 23(2): 129-152. doi: 10.21074/kjlcap.2022.23.2.129.

Narim, K. 2024. "Cambodia: Police Raid Suspected Scam Compounds and Detain about 1,000 Foreigners, Mostly Chinese and Koreans, Following Media Reports about Alleged Online Scam Operations." *Business & Human Rights Resource Centre*, October 25. Retrieved September 20, 2025. (https://www.business-humanrights.org/en/latest-news/cambodia-police-raid-suspected-scam-compounds-and-detain-about-1000-foreigners-mostly-chinese-and-koreans-following-media-reports-about-alleged-online-scam-operations/).

Office of the High Commissioner for Human Rights. 2023. "Hundreds of Thousands Trafficked to Work as Online Scammers in SE Asia, Says UN Report." Retrieved October 20, 2025. (https://www.ohchr.org/en/press-releases/2023/08/hundreds-thousands-trafficked-work-online-scammers-se-asia-says-un-report).

Ozer, M., Kucukkaya, G., Kose, Y., Mukasheva, A., Ciris, K., and Penumatcha, B.V. 2025. "Mapping Trafficking Networks: A Data-Driven Approach to Disrupt Human Trafficking Post Russia-Ukraine Conflict." *Computational Science and Computational Intelligence. CSCI 2024. Communications in Computer and Information Science* 2509: 201-212. doi: 10.1007/978-3-031-94953-1_17.

Paek, S. Y., Lee, J. and Choi, Y. J. 2022. "The Impact of Parental Monitoring on Cyberbullying Victimization in the COVID-19 Era." *Social Science Quarterly* 103(2): 294-305. doi: 10.1111/ssqu.13134.

Pratamasari, A. 2020. "South Korean Hurry-Hurry (빨리 빨리) COVID-19 Strategy: Privacy Concern, No-Lockdown, and Discriminations." *Jurnal Global & Strategis* 14(2): 29-48. doi: 10.20473/jgs.14.2.2020.203-222.

Rogers, S. 2024. "New GASA Report Estimates $688 Billion in Scam Losses across Asia amid Rising Cyberthreat Worldwide." *Global Anti-Scam Alliance*, October 15. Retrieved October 10, 2025. (https://www.gasa.org/post/2024-asia-scam-report-688-billion-lost).

Sarkar, G. and Shukla, S. K. 2024. "Bi-Directional Exploitation of Human Trafficking Victims: Both Targets and Perpetrators in Cybercrime." *Journal of Human Trafficking,* 1-22. doi: 10.1080/23322705.2024.2353015.

Seo, M. 2017. "Influences of SNS Use on Life Satisfaction via upward Social Comparison, Relative Deprivation and Underestimation of Economic Status." *Korean Journal of Communication & Information* 83(3): 72-95. doi: 10.46407/kjci.2017.06.83.72.

Staatssekretariat für Wirtschaft. 2025. *Economic Report 2025 Republic of Korea*. Retrieved September 25, 2025. (https://www.seco.admin.ch/dam/seco/it/dokumente/Aussenwirtschaft/Wirtschaftsbeziehungen/L%C3%A4nderinformationen/Asien_Ozeanien/wirtschaftsbericht_suedkorea.pdf.download.pdf/Wirtschaftsbericht_S%C3%BCdkorea_2025.pdf).

Sykiotou, A. P. 2017. "Cyber Trafficking: Recruiting Victims of Human Trafficking through the Net." Pp. 1547-1588 in *Europe in Crisis: Crime, Criminal Justice, and the Way Forward*, edited by C. D. Spinellis, N. Theodorakis, E. Billis, G. Papadimitrakopoulos, Athens: Ant. N. Sakkoulas Publishers L. P.

Toney-Butler, T.J., Ladd, M. and Mittel, O. 2023. *Human Trafficking*. StatPearls.

Ullah, A. 2025. "Human trafficking in Bangladesh: the interplay of deception, socio-economic vulnerabilities, and structural challenges." *Global Crime* 26(3-4): 237-258. doi: 10.1080/17440572.2025.2538080.

U.S.-China Economic and Security Review Commission. 2025. *China's Exploitation of Scam Centers in Southeast Asia*. Retrieved September 25, 2025. (https://www.uscc.gov/research/chinas-exploitation-scam-centers-southeast-asia).

U.S. Department of Homeland Security. 2025. "What Is Human Trafficking?" Retreived October 11, 2025. (https://www.dhs.gov/blue-campaign/what-human-trafficking).

U.S. Department of Justice. 2025. "Human Trafficking." Retrieved September 2. (https://www.justice.gov/usao-ri/human-trafficking).

U.S. Department of State. n.d.-a. 2023 "Investment Climate Statements: Cambodia." Retrieved September 2. (https://www.state.gov/reports/2023-investment-climate-statements/cambodia/).

U.S. Department of State. n.d.-b. "2024 Trafficking in Persons Report: Cambodia." Retrieved September 2. (https://www.state.gov/reports/2024-trafficking-in-persons-report/cambodia/).

United Nations Human Rights Office of the High Commissioner. 2023. *Online Scam Operations and Trafficking into Forced Criminality in Southern Asia: Recommendations for a Human Rights Response*. Retrieved October 10, 2025. (https://bangkok.ohchr.org/news/2022/online-scam-operations-and-trafficking-forced-criminality-southeast-asia).

United Nations Office on Drugs and Crime. 2024. *Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape*. Retrieved August 27, 2025. (https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf).

United Nations Office on Drugs and Crime. 2008. *An Introduction to Human Trafficking: Vulnerability, Impact and Action*. Retrieved September 2, 2025. (https://www.unodc.org/documents/human-trafficking/An_Introduction_to_Human_Trafficking_-_Background_Paper.pdf).

United Nations Office on Drugs and Crime. n.d.-a. "Human Trafficking." Retrieved September 5. (https://www.unodc.org/unodc/en/human-Trafficking/Human-Trafficking.html).

United Nations Office on Drugs and Crime. n.d.-b. "8 facts you need to Know about Human Trafficking in the 21st Century." Retrieved September 5. (https://www.unodc.org/unodc/frontpage/2024/May/8-facts-you-need-to-know-about-human-trafficking-in-the-21st-century.html).

United States Institute of Peace. 2024. *Transnational Crime in Southeast Asia: A Growing Threat to Global Peace and Security*. Retrieved September 1, 2025. (https://www.usip.org/publications/2024/05/transnational-crime-southeast-asia-growing-threat-global-peace-and-security).

Wang, F. 2024. "Victim-Offender Overlap: The Identity Transformations Experienced by Trafficked Chinese Workers Escaping from Pig-Butchering Scam Syndicate." *Trends in Organized Crime* (2024): 1-32. doi: 10.1007/s12117-024-09525-5.

Wang, F. and Topalli, V. 2024. "The Cyber-Industrialization of Catfishing and Romance Fraud." *Computers in Human Behavior* 154: 108133. doi: 10.1016/j.chb.2023.108133.

Weitzer, R. 2007. "The Social Construction of Sex Trafficking: Ideology and Institutionalization of a Moral Crusade." *Politics & Society* 35(3): 447-475. doi: 10.1177/0032329207304319.

Won, D. and Lee, W. 2025. "Man in His 20s Dies in Cambodia… Forced to Take Drugs." *KBS News*, September 30. Retrieved October 20, 2025. (https://news.kbs.co.kr/news/pc/view/view.do?ncd=8371413).

Wongmahesak, K., Singh, B. and Kaunert, C. 2025. "The Complex Interplay of Generational Differences, Digital Literacy, and Cybercrime Fear." *Asian Crime and Society Review* 12(1): Article 3. doi: 10.14456/acsr.2025.3.

Yardley, L. and Marks, D. F. 2003. *Research Methods for Clinical and Health Psychology*. Sage.

Yoon, S. and Han, S. 2008. "Differences in Obedience to Authority between Authoritarians and Non-Authoritarians: in Three Authority-level Situations." *Korean Psychological Journal of Culture and Social Issues* 14(3): 41-56.

Table 1. Stages of thematic analysis.

Stage	Description
Data Familiarization	Reading the material repeatedly to grasp the entire content and meaning
Initial Coding	Coding key features across the entire dataset
Theme Development	Grouping similar codes to derive potential themes
Theme Review	Verifying consistency between themes, coded data, and the entire dataset
Theme Definition	Defining and naming themes based on their relevance to the research questions
Final Analysis	Integrating supporting evidence for themes and presenting a consistent interpretation

Table 2. Components of thematic framework.

Component	Description
Theme	A recurring meaning or pattern found throughout the data
Definition	A statement that expresses the core meaning contained within the theme
Subthemes	Secondary categories created by subdividing the theme
Characteristics	The specific attributes and detailed expressions that constitute the theme

Table 3. Thematized summary.

Theme No.	Definition	Subthemes	Characteristics
1	An organized process of deceiving and recruiting people experiencing economic hardship in the digital environment	Recruitment messages targeting desperate job seekers, Utilization of diverse digital platforms	False high-income promises, Leveraging anonymous platforms, Financial status profiling, Legitimacy-disguised job postings
2	A comprehensive control system eliminating escape possibilities through physical, psychological, and chemical mechanisms	Immediate isolation and identity control, Anonymization and collusion with local authorities, Addiction mechanism	Passport and mobile phone confiscation, Military-grade compound facilities, Use of aliases, Forced drug use and gambling, Psychological and economic bondage
3	Sophisticated manipulation leveraging Korean linguistic competence, cultural norms, and authority deference	Exploiting linguistic and cultural competence, Exploiting fellow Koreans' deference to public authority	Using generational language patterns, Exerting group pressure, Mimicking dating processes, Disguising legal authority, Manipulating victims' psychology
4	Korea's fast-paced financial infrastructure and factory-style cyber scam industrialization	Building criminal infrastructure exploiting the speed of Korea's financial system, Industrialization of cyber scams	Necessity of locally registered Korean accounts, Account opening through document collection, Utilization of multiple accounts, Factory-style mass scam execution, Performance-based management