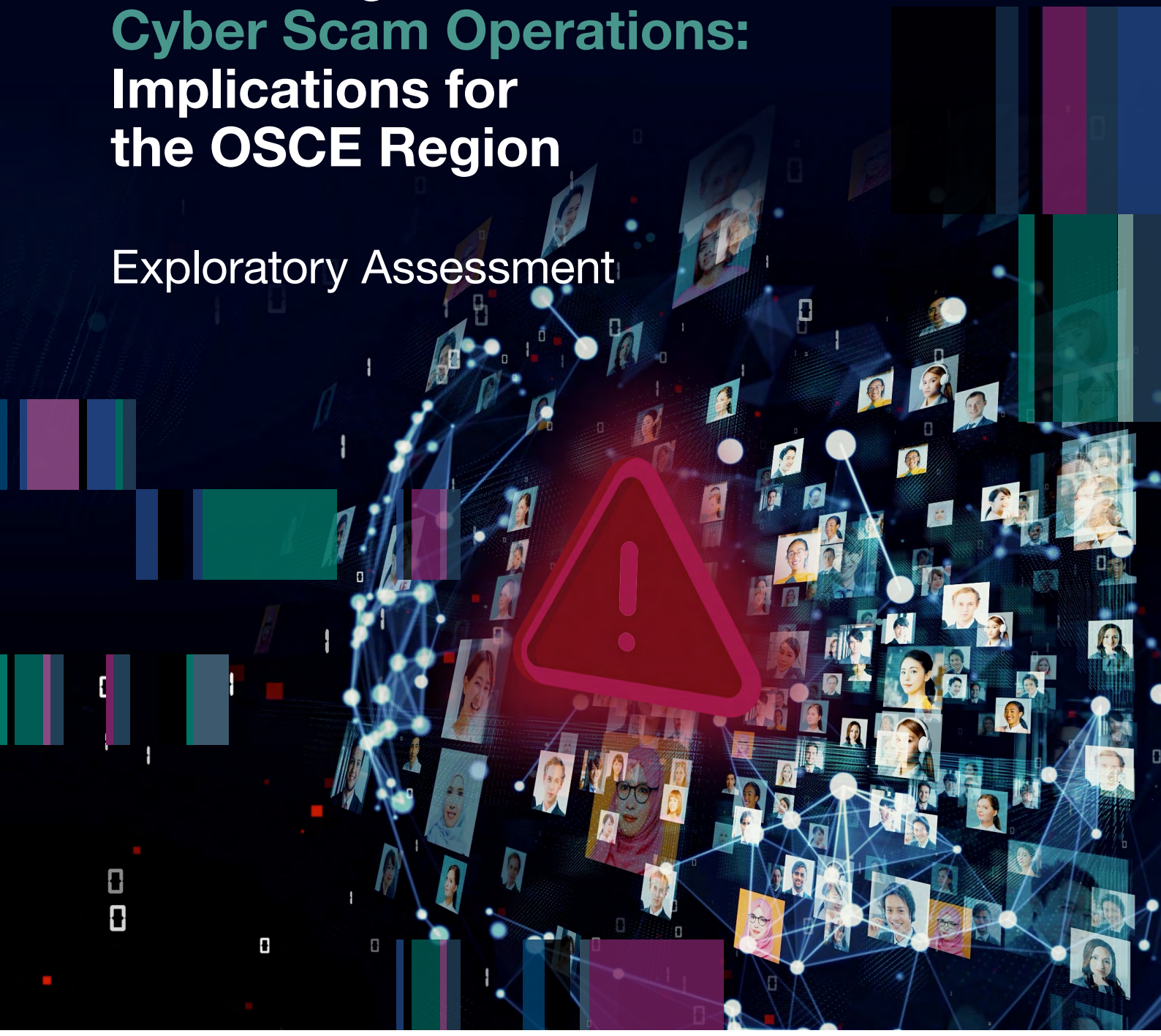
Office of the Special Representative and Co-ordinator
for Combating Trafficking in Human Beings

Trafficking into Cyber Scam Operations: Implications for the OSCE Region

Exploratory Assessment



OSCE Organization for Security and Co-operation in Europe

ISBN: 978-92-9271-666-0

Published by the OSCE Office of the Special Representative and
Co-ordinator for Combating Trafficking in Human Beings

Wallnerstr. 6, 1010 Vienna, Austria
Tel: + 43 1 51436 6664
Fax: + 43 1 51436 6299
email: info-cthb@osce.org

Design: Tina Feiertag, Vienna
Image: Shutterstock

Cite as: Office of the OSCE Special Representative and Co-ordinator for Combating Trafficking in Human Beings,
Indications of Cyber Scam Centres in the Balkans, Central Asia and the United Kingdom
Exploratory Assessment Based on Open-Source Intelligence and Survivor-Informed Insights (Vienna, April 2026)

The Organization for Security and Co-operation in Europe (OSCE) is a pan-European security body whose 57 participating States span the geographical area from Vancouver to Vladivostok. Recognized as a regional arrangement under Chapter VIII of the United Nations Charter, the OSCE is a primary instrument for early warning, conflict prevention, crisis management and post-conflict rehabilitation in its area. Its approach to security is unique in being both comprehensive and co-operative: comprehensive in that it deals with three dimensions of security – the human, the politico-military and the economic/environmental. It therefore addresses a wide range of security-related concerns, including human rights, arms control, confidence- and security-building measures, national minorities, democratization, policing strategies, counter-terrorism and economic and environmental activities.

PARTICIPATING STATES: Albania | Andorra | Armenia | Austria | Azerbaijan | Belarus | Belgium | Bosnia and Herzegovina | Bulgaria | Canada Croatia | Cyprus | Czechia | Denmark | Estonia | Finland | France | Georgia | Germany | Greece | Holy See | Hungary | Iceland | Ireland | Italy Kazakhstan | Kyrgyzstan | Latvia | Liechtenstein | Lithuania | Luxembourg | Malta | Moldova | Monaco | Mongolia | Montenegro | Netherlands North Macedonia | Norway | Poland | Portugal | Romania | Russian Federation | San Marino | Serbia | Slovakia | Slovenia | Spain | Sweden Switzerland | Tajikistan | Türkiye | Turkmenistan | Ukraine | United Kingdom | United States of America | Uzbekistan

ASIAN PARTNERS FOR CO-OPERATION : Afghanistan | Australia | Japan | Republic of Korea | Thailand
MEDITERRANEAN PARTNERS FOR CO-OPERATION: Algeria | Egypt | Israel | Jordan | Morocco | Tunisia

Disclaimer
This report was prepared by the Office of the Special Representative and Co-ordinator for Combating Trafficking in Human Beings (OSR/CTHB) of the Organization for Security and Co-operation in Europe (OSCE). The findings, interpretations, and conclusions expressed herein are based on open-source research and insights from lived experienced experts, and do not necessarily reflect the official views or positions of the OSCE, its participating States, or its institutions. The designations employed and the presentation of material in this publication do not imply the expression of any opinion whatsoever on the part of the OSCE concerning the legal status of any country, territory, city, or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries. The contents of this report, including the analysis, assessments, and any references to specific platforms, entities, or jurisdictions, are intended solely for informational and policy development purposes. They should not be construed as constituting legal determinations or formal accusations against any individual, organisation, or State.

This material has been funded by UK International Development from the UK government; however, the views expressed do not necessarily reflect the UK government's official policies.

Office of the Special Representative and Co-ordinator
for Combating Trafficking in Human Beings

Trafficking into Cyber Scam Operations: Implications for the OSCE Region

Exploratory Assessment

OSCE Organization for Security and Co-operation in Europe

Table of Contents

List of Abbreviations

AI	Artificial Intelligence
CSIS	Center for Strategic and International Studies
GASA	Global Anti-Scam Alliance
GPS	Global Positioning System
GRETA	Group of Experts on Action against Trafficking in Human Beings
IJM	International Justice Mission
IOM	International Organization for Migration
INTERPOL	International Criminal Police Organization
MLA	Mutual Legal Assistance
OCCRP	Organized Crime and Corruption Reporting Project
OHCHR	Office of the High Commissioner for Human Rights
OSCE	Organization for Security and Co-operation in Europe
OSINT	Open-Source Intelligence
SEA	Southeast Asia
THB	Trafficking in Human Beings
UK	United Kingdom
UN	United Nations
UNODC	United Nations Office on Drugs and Crime
USDT	Tether (Cryptocurrency)
USIP	United States Institute of Peace
VoIP	Voice over Internet Protocol

Foreword

The evolution of trafficking for forced criminality has resulted in a highly sophisticated global menace, human trafficking into cyber scam operations. Widely regarded as a phenomenon that was once largely confined to Southeast Asia, this phenomenon continues to spread to other regions, including to the OSCE.

As the OSCE Special Representative and Co-ordinator for Combating Trafficking in Human Beings, I have observed with increasing concern during my mandate the growing indications of this phenomenon, including those raised by participating States. In recent years, several OSCE participating States have launched investigations into cases of trafficking of third country nationals into cyber scam compounds in their territories. Similarly, nationals of OSCE participating State have been trafficked into such compounds outside the region. Our citizens are no longer only economic targets - they are human trafficking victims, and our region is becoming a hub for this criminal practice. This report indicates that approximately 40 per cent of OSCE participating States are now affected, and this number continues to grow.

Such developments led my Office to launch an assessment to explore the impact of this exploitative form on our region. The findings of this assessment highlight a striking reality: forced cyber scam operations are no longer geographically distant. Our data now points to the emergence of similar patterns within the OSCE region. These findings are grounded in both structured analysis of online recruitment content and digital communications and informed by lived experience experts. These perspectives are essential. They remind us that behind every fraudulent message or online advertisement lies the very real risk of exploitation, coercion, and human suffering. The accounts of these experts confirm, yet again, that criminal networks actively use social media and private communication platforms to target individuals for trafficking into cyber scam operations.

The convergence of trafficking in human beings and cybercrime challenges us to rethink our traditional approaches of victim outreach, identification, and protection. It requires stronger co-operation across sectors – including law enforcement, financial actors, and technology platforms – and across borders. It also demands that our structures and systems place victims at the centre of their response, ensuring identification, protection, and access to assistance without prejudice.

As the OSCE region is emerging as a hub for this criminal cyber activity, it presents an important window for early intervention and to get ahead of its expansion. My Office remains committed to supporting participating States in addressing this growing threat and protecting victims. It is my hope that this report will serve as a useful tool in understanding emerging risks posed by expansion of cyber-scam operations and imminent risks associated with vulnerabilities, and that it will help develop targeted and timely responses to prevent further exploitation. This report provides tools and recommendations on how to do so. The time to act is now.

Acknowledgements

This report has been developed under the lead of Tarana Baghirova, Programme Officer, and Valentina López-Yanes, Assistant Project Officer. I thank them for their leadership and vision in conducting this research and preparing this report.

I would like to express my sincere gratitude to Ms. Lynn Dudenhöfer, Senior Intelligence and Technology Expert, who served as the primary researcher and drafter of this report and my profound appreciation to Mr. Abdus Salam, Survivor Advisor of Human Trafficking, and Mr. Saken Kabibulla, Lived Experience Expert, for their invaluable contribution of their lived expertise and analytic insights, which enriched and verified the data presented in this report.I also thanks the United Kingdom for funding the development of this important exploratory assessment.

Dr. Kari Johnstone
OSCE Special Representative and
Co-ordinator for Combating Human Trafficking

Executive Summery

The findings of this assessment suggest that human trafficking into cyber scam centres is transitioning from a Southeast Asian region-specific phenomenon to a replicable operational model. OSCE participating States will likely face the prospect of scam centre expansion unless prevention, protection, and disruption efforts are implemented at scale. The Consolidated Indicator Taxonomy developed in this report provides international and national authorities, as well as platform moderators, with convergence-based assessment criteria enabling early-stage identification of high-risk recruitment content.

Key Findings

This report provides an exploratory assessment of cyber scam operations recruitment infrastructure operational in OSCE participating States, with particular focus on how criminals recruit and entrap victims of human trafficking via fraudulent job offers and compel them to scam others (financial victims of fraud). The assessment is grounded in analysis of 82 coded recruitment advertisements from open-source platforms, (e.g., Facebook, Telegram, LinkedIn, VKontakte), the examination of 750 unique Telegram messages, key testimony from survivors trafficked into cyber scam operations, and publicly available data reported by individual reporting from OSCE participating States.

The assessment yields the following core findings:

1. Recruitment linked to cyber scam centres follows similar patterns across jurisdictions, suggesting a broadly standardised operating model.

2. Recruitment is structured to blend into legitimate labour-market infrastructure, meaning concern arises more often through convergence of multiple indicators than through isolated red flags.

3. The Eastern Europe and South-Eastern Europe region accounts for the highest portion of elevated-risk indicators in the dataset, pointing to a notable concentration of potential cyber-scam activity.

4. Central Asia presents lower cross-border risk profiles, while still showing signs of substantial domestic fraud activity.

5. The South Caucasus features prominently as a recruitment destination, with activity predominantly associated with retention, conversion, and call centre roles.

6. Messaging platforms, including Facebook, Telegram, LinkedIn, WhatsApp and Viber, are the most common contact pathways across all categories, indicating a shift towards private messaging platforms.

7. Gender-based targeting appears in 12 per cent of advertisements, particularly in iGaming and hospitality roles, and in the majority of cases is reflected in relocation, employer-provided housing, or messaging-app routing as the sole point of contact, conditions that may increase vulnerability to exploitation.

8. OSCE-based recruitment often targets citizens of participating States in native-languages, with English language used as the main language, followed by Russian language, and smaller but still analytically relevant advertisements were also found in Turkish, Romanian, and Italian.

Introduction

1

1.1 Background and Rationale

Cyber scam centres have been fertile ground for human trafficking and fraud for at least the past five years. The primary context for major cyber scam hubs has been Southeast Asia, where thousands of victims from OSCE participating States, inter alia, have been trafficked into and committed fraud generating billions in illicit proceeds. The scale of financial losses and human trafficking associated with scam centres is unprecedented: UNODC estimates that scam centres in East and Southeast Asia generated between USD 18-37 billion in 2023 alone, while more recent Global Anti-Scam Alliance data suggests that scams globally caused over 1 trillion in losses in 2024.[1]

The documented scale of this phenomenon is considerable. The United Nations Office of the High Commissioner for Human Rights (OHCHR) has documented grave abuses against trafficking victims, including systematic violence, sexual exploitation, torture, debt bondage, and forced criminality.[2] UNODC reporting indicates that the convergence of cyber fraud with trafficking is emerging as a significant trafficking typology.[3] INTERPOL has established a dedicated scam centre taskforce and assesses the overall global risk related to financial fraud as high, expecting the scale of offending to escalate significantly over the next three to five years.[4] The trajectory suggests that without sustained intervention, the phenomenon could transition from a region-specific to a globally distributed model - a shift that INTERPOL confirms is already underway, with new scam centres discovered in the MENA, Central American, and West African regions.

Human trafficking victims originate from a broad geographic range: as of March 2025, individuals from 80 countries have been trafficked into online scam centres across Southeast Asia, with an estimated 300,000 or more people currently held in scam operations.[5] This constitutes both an unprecedented trafficking crisis and a destabilizing transnational criminal enterprise generating substantial illicit financial flows.

Reports show that, as of April 2026, at least 22 OSCE participating States have been affected by cyber-scam operations. Participating States whose nationals have been reportedly trafficked into cyber scam operations include Bosnia and Herzegovina[6], Croatia[7], Czechia[8], Georgia[9], Kazakhstan[10], Kyrgyzstan[11], Mongolia[12], Netherlands[13], Romania[14], the Russian Federation[15], Tajikistan[16], Türkiye[17], Turkmenistan[18], Ukraine[19], United Kingdom[20], United States[21] and Uzbekistan[22]. Forced cyber scam operations have been identified in Austria[23], Belarus[24], Croatia[25], Georgia[26], Montenegro[27], North Macedonia[28], Poland[29] and Türkiye.

In September 2025, the United States Department of State[30] and the United Kingdom[31] imposed targeted sanctions on criminals implicated in online scam centres in Southeast Asia, recognizing the severity of the threat and the need for co-ordinated international response. In 2026, participating States have continued to step up their efforts, with the United Kingdom imposing sanctions targeting illicit cryptocurrency networks facilitating scam centre activity[32] In March 2026, the FBI, U.S. Department of Justice's Scam Center Strike Force, UK's National Crime Agency, and Canada supported an international crackdown, led by Thailand's Royal Thai Police Anti-Cyber Scam Centre, on Southeast Asian criminal scam centres.[33]

This report reveals an emerging threat: the operationalization of the scam centre recruitment model within the OSCE region. It responds to concerns raised by participating States, including during the OSCE Special Representative and Co-ordinator for Combatting Trafficking in Human Beings (hereinafter "the OSR/CTHB") 2025 annual report to the Permanent Council, and the OSCE Conference of the Alliance against Trafficking in Persons (2025) , where participating States highlighted the growing relevance of this phenomenon in the region.

The findings of the assessment suggest that criminal networks are now actively recruiting on online platforms across the OSCE region, particularly in Eastern Europe and South-Eastern Europe, Central Asia, and the South Caucasus. This assessment provides an empirical base to inform urgent, co-ordinated action to mobilize prevention efforts, advance protection mechanisms to ensure victims forced into scamming operations are identified and protected as such and support prosecution of criminals who compel trafficking victims to defraud financial victims through cyber scams in the OSCE region.

1.2 The Emerging Threat in the OSCE Region

The recruitment pathway from OSCE participating States to Southeast Asian scam centres has been well-documented. OHCHR reporting indicates that perpetrators deliberately target nationals of OSCE participating States, particularly individuals with multilingual capacity, using Facebook, Instagram, LinkedIn, Telegram, and other platforms for recruitment.[35] Trafficking victims are recruited through deceptive job advertisements promising legitimate employment, often offering visa assistance and relocation allowances. Upon arrival at the destination country, victims experience confinement, document confiscation, violence, and forced into criminality conducting fraud via romance or investment scams, task-based fraud, and call-centre operations.

Against this backdrop, two observations led the OSR/CTHB to initiate this assessment. First, investigative and news outlets have documented sophisticated fraud operations now appearing in the OSCE region.[36] These operations exhibit structural parallels to Southeast Asian compounds: call centre infrastructure, multilingual victim workforces, sophisticated fraud typologies, and transnational money-laundering networks. The operations are generating substantial proceeds (estimated at tens to hundreds of millions of euros annually, based on law enforcement seizure data) and appear to be expanding. The expansion into the OSCE region appears to form part of a broader global phenomenon, with increasing activity emerging in the Middle East, West Africa and Central America.[307]

To illustrate the criminal activity, several cases have been sought from selected participating States, which are described below:

Taken together, these findings indicate that the recruitment and exploitation model associated with cyber scam operations is increasingly visible within the OSCE region, with cases across Eastern and Southeastern Europe in the last 6 years. It must be noted that in several cases examined for the purpose of this assessment, the victims were formally identified as victims of human trafficking for forced labour as opposed to victims of forced criminality. This should be understood in the context of domestic legislation, which in many OSCE participating States does not include forced criminality as a distinct form of trafficking and qualifies such cases as forced labour.

In addition to documented sophisticated fraud operations in the OSCE region, open-source monitoring of recruitment platforms and information provided by lived experience experts over the course of a six-month period suggests that a certain portion of recruitment content for these operations originates from within the OSCE region. Unlike Southeast Asian recruitment, which is often conducted in English targeting Western audiences, OSCE-based recruitment frequently targets citizens of participating States in native-language spaces, which may represent a shift in operational geography - rather than recruiting individuals for movement to Southeast Asia, perpetrators now appear to also be recruiting for operations situated in neighbouring or regional countries within or adjacent to the OSCE area.

CASE 1 | **Cyber Scam Operation in Poland Recruited Ukrainian Victims[38]**

In January 2026, Polish law enforcement dismantled a criminal network operating in Warsaw involved in both human trafficking and drug trafficking. The police operation was initiated following the escape of a 22-year-old Ukrainian man who had been recruited through a fraudulent "call centre" job advertisement. After fleeing exploitative conditions, the victim alerted authorities, triggering a police investigation.

The operation was conducted jointly by Warsaw's Mokotów Police Station, Ursynów and Wilanów precincts, the Capital Police Prevention Unit, the Traffic Department, the Counter-Terrorism Unit, and the Central Bureau for Cybercrime. It resulted in the arrest of 22 individuals aged between 18 and 34, and the identification of nine Ukrainian nationals (six men and three women) as victims of human trafficking for forced labour. Investigations indicated that victims were recruited under false promises of employment and subsequently subjected to coercive and exploitative conditions. The criminal network was also found to be involved in drug-related criminal activity.

The victims received assistance from the La Strada Foundation, operating through Poland's National Centre for Victims of Human Trafficking.

CASE 2 — Taiwanese victims forced into cyber scam operations in the Republic of North Macedonia[39]

In May 2021, North Macedonia carried out an operation following a request for international legal assistance from Taiwan through the European Union. The individuals were being investigated in Taiwan for fraud, money laundering, and human trafficking. The North Macedonian police searched several “call centres,” and found 48 people from Taiwan, 7 of whom were organizers of a criminal group, and 41 were identified as potential victims of human trafficking.

In the pre-investigation procedure, two locations with buildings (houses) in the area of Skopje had been identified, where "call centres" were set up, as well as three hotel locations nearby where some of the organizers of the organized crime group temporarily stayed, who were responsible for prior mapping and renting the houses. Based on the measures and activities taken, it emerged that the members of the organized criminal group were responsible for recruiting, receiving, and accommodating individuals from Taiwan on the territory of the Republic of North Macedonia, as well as providing working conditions (technical equipment such as tablets, laptops, telephones, and other technical equipment necessary for the smooth functioning of the call centre), for them to be employed to commit cyber fraud through the "call centres" of individuals in China and Taiwan.

The victims' task was to establish contacts with potential victims of financial fraud via high-speed internet.

They were divided into three groups as telephone operators operating on three levels:

1. The human trafficking victims in the first level, worked as "operators" posed as clerks at a bank, postal service, or insurance company.
2. In the second level, in order to obtain full personal data, the human trafficking victims posed as police officers and demanded proof from economic victims of payment of a fictitious punishment on the basis of which they stole the victims' personal data.
3. The third-tier operators, posing as prosecutors and judges, assured the targeted economic victims that they would face serious charges if they did not cooperate and transfer a certain amount of money to accounts.

This organized crime group, the so-called "Trade Unions," recruited people to Taiwan, promising them better jobs and a better quality of life. Under the pretext of complying with administrative travel procedures, the victims' travel documents were confiscated, and after the human trafficking victims were brought to their destination, their mobile phones were also confiscated. The victims were placed in houses and were constantly accompanied by one of the organizers to control them and prevent them from contacting outsiders. Based on the data provided for entry into the territory of the Republic of North Macedonia, it emerged that all individuals had legal entry, within the legally prescribed period of tourist stay.

This operation was carried out by the North Macedonian Public Prosecutor's Office for Combating Organized Crime and Corruption in co-operation with the National Unit for the Suppression of Migrant Trafficking and Human Trafficking, the Investigation Bureau of the Ministry of Justice of Taiwan, and the Public Prosecutor's Office in the Kaohsiung District in Taiwan.

After the operation, all individuals were temporarily housed in the Reception Center for Foreigners of the Ministry of Interior of North Macedonia and were later transferred to Taiwan for further proceedings.

CASE 3 | **Taiwanese nationals trafficked into a call-centre in Montenegro to commit fraud[40/41]**

In January 2020, the Montenegrin Police identified a call centre where Taiwanese victims were being forced to defraud Chinese citizens. The Police arrested 8 suspects and found 84 persons (including 12 women), who were presumed to be victims of THB, 37 of whom were formally identified as victims and the other 47 were treated as potential victims and returned to Taiwan.

The trafficking victims had been recruited from Taiwan and entered Montenegro on a 90-day tourist visa. In Podgorica, they were accommodated at three different locations, their travel documents were confiscated, and they were trained to use different web-based applications to call Chinese citizens, pretending to be police officers, prosecutors or judges, to request their bank data and withdraw money.

The identification of this modus operandi was carried out by Montenegro, in co-operation with INTERPOL and Europol. A financial investigation was carried out and assets found in Montenegro were seized. The prosecution was handed over to the competent prosecutor's office in Taiwan.

Figure 1:
Recruitment-to-Exploitation Pipeline

Source: OSINT analysis and survivor-informed testimony

Figure 1 illustrates that recruitment linked to scam-centre activity often follows a structured progression rather than a single deceptive act. The process typically begins with seemingly ordinary job discovery through social media, job boards, or messaging channels, followed by direct contact with recruiter personas on private apps. It then moves into onboarding, where travel, visas, accommodation, and document handling are presented as routine support measures, helping the opportunity appear credible and lowering initial suspicion.

The latter stages show how this recruitment process can shift into exploitation. Individuals may be deployed into roles described as iGaming, forex, crypto, or call-centre work, before more serious indicators emerge, such as document confiscation, debt bondage, restricted movement, surveillance, forced labour, and, in some cases, physical abuse.

1.3 Purpose and Scope

This report seeks to document the presence and threat of human trafficking into cyber scam operations in the OSCE region[42] and inform a set of actions for policy and practice for early detection, prevention, and prosecution of human trafficking related to cyber-scam operations and to protect victims. This assessment does not aim to provide comprehensive law-enforcement intelligence; rather, its purpose is to identify open-source indicators that can lead anti trafficking front-line responders (including law enforcement, labour inspectors, immigration authorities, and platform moderators) to identify high-risk recruitment content. The assessment is scoped to publicly available, ethically sourced information.

The analysis contained in this report is informed by insights of lived experience consultants with direct experience of trafficking to Southeast Asian scam compounds. These contributions have also formed an integral part of the research process, including the review and validation of findings. This survivor-centred approach ensures that the assessment reflects not only indicators and data patterns, but also the experiential reality of deceptive recruitment, operational conditions and means of control, and victim exploitation.

Methodology

2

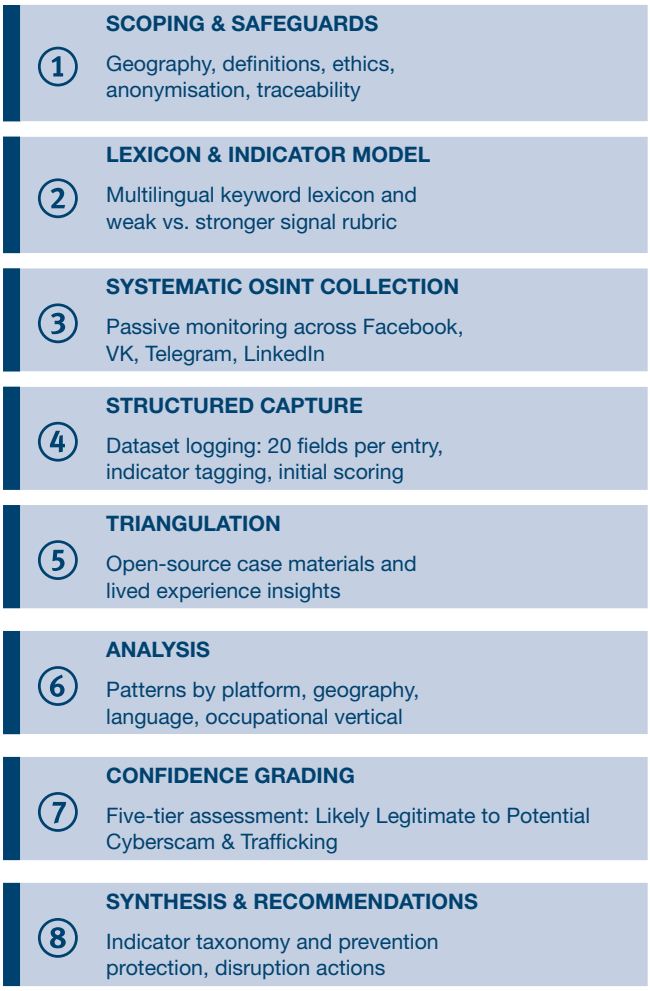
2.1 Analytical Scope and Sources

This assessment draws on three primary data streams: first, a curated dataset of public-facing recruitment advertisements collected from Facebook, VK, LinkedIn, Telegram, and Instagram; second, a targeted review of publicly accessible Telegram recruitment channels; and third, a curated questionnaire completed by experts with lived experience, designed to capture qualitative insights on recruitment pathways, conditions of exploitation, and methods of control. These materials were analysed alongside open-source contextual reporting, including investigative journalism, law enforcement releases, and relevant public reporting, to support interpretation and triangulation.

The analytical workflow underpinning this report followed an eight-stage process, beginning with the definition of scope, ethical safeguards, and a multilingual keyword lexicon, followed by systematic open-source collection across Facebook, VK, Telegram, and LinkedIn. Each entry was recorded using a standard set of 20 fields and tagged based on key indicators. The data was cross-checked with known cases and insights from experts with lived experience, and then analysed to identify patterns across platforms, locations, languages, and job types. Finally, each entry was given a confidence rating, ranging from "Likely Legitimate" to "Potential Cyber-scam and Trafficking."

Risk was assessed by looking at a combination of indicators, rather than relying on any single sign. Content showing several indicators linked to known scam recruitment patterns was classified as higher risk. Content with fewer or unclear indicators was considered a grey area, while content that appeared similar to normal job advertisements was classified as low risk. This approach reflects the fact that deceptive recruitment is often designed to look like legitimate job offers and is therefore easier to identify when multiple indicators appear together.

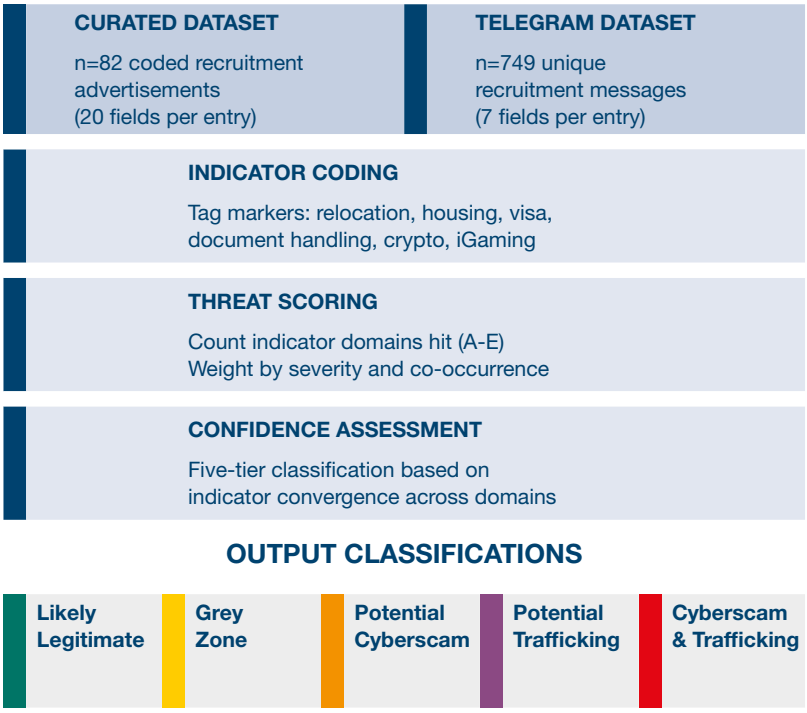
Figure 2:
Analytical Workflow



2.2 Collection and Coding Logic

Recruitment advertisements were coded against 33 indicators across five analytical categories. Geographic entries were tagged to recruitment location, destination, and perpetrator origin where determinable.[44] Advertisements were classified using a five-tier confidence assessment based on indicator convergence across categories: Likely Legitimate (consistent with standard labour recruitment practices), Grey Zone (informal and potentially exploitative, but lacking sufficient indicator convergence to be conclusively linked to trafficking), Potential Cyber-scam (exhibiting indicators consistent with online fraud operations), Potential Trafficking (exhibiting indicators consistent with labour trafficking), and Cyber-scam and Trafficking (exhibiting multiple converging indicators across both domains, suggesting a high likelihood of deceptive recruitment and potential exploitation).

Figure 3:
Collection and Coding Logic Indicator Assessment Framework



The figure above shows how the data was collected and analysed. Two primary datasets were compiled: one with 82 recruitment advertisements collected from Facebook, VK, Telegram, and LinkedIn, each coded across 20 structured fields, and another with 750 recruitment messages from Telegram job channels, captured across 7 fields. Each entry was tagged based on key indicators, which were grouped into five areas, to identify patterns consistent with documented scam centre recruitment.

Each entry was then assessed based on how many indicators were present and how they appeared together. Based on this, entries were placed into one of five categories: Likely Legitimate, Grey Zone, Potential Cyber-scam, Potential Trafficking, or Cyber-scam and Trafficking. This approach reflects the fact that no single sign is enough on its own, it is rather the combination of multiple warning signs that helps distinguish suspicious recruitment from legitimate job offers.

2.3 Survivor-Informed Triangulation

The assessment was informed by two experts with lived experience of trafficking for forced criminality in Southeast Asian scam compounds. The experts provided primary qualitative input, reviewed preliminary findings, and provided narrative context on recruitment deception, operational structure, victim experiences, and perpetrator decision-making. The experts' insights have been integrated throughout this report to provide authentic context for interpretation of indicators and policy recommendations.

2.4 Limitations

The assessment presented in this report should be viewed in light of the following methodological and contextual limitations: (1) As with any open-source assessment, the availability of publicly accessible data provides an illustrative rather than comprehensive picture of the full scale of cyber scam centre recruitment operations; (2) indicator-based classification is designed to flag elevated risk and support prioritisation, but cannot in itself confirm trafficking in any individual case; (3) the assessment covers a defined collection period and may not fully reflect the latest ongoing evolution of recruitment tactics; (4) the research draws exclusively on open-source material and has not been cross-validated against law enforcement case data, which may offer additional context; (5) geographic coverage focuses on OSCE participating States and primary destination countries identified through the data, and recruitment activity in other regions may warrant further examination.

Cyber Scam Centres: The Phenomenon

3

3.1 Origins in Southeast Asia

The first large-scale cyber scam centre operations emerged in Southeast Asia between 2015-2018. These compounds are centralized sites where trafficked victims conduct fraud under coercive control methods. Operations typically employ 50-500 workers per site, operating in long hour shifts conducting various scams, such as romance scams, investment fraud, task-based scams, and call-centre fraud targeting mostly Western and Chinese audiences. Compounds are typically established in countries with weakened governance and geographic proximity to source regions for human trafficking victim recruitment.

Amnesty International's June 2025 investigation documented 53 scam compounds in a single Southeast Asian country, interviewing 58 survivors from 8 nationalities. The investigation detailed the systematic use of "dark rooms" for physical and psychological torture of victims who failed to meet daily fraud targets, as well as comprehensive documentation of severe human rights abuses including systematic violence, sexual torture, and debt bondage.

3.2 Scam Typologies

Primary fraud typologies conducted at scam compounds include, but are not necessarily limited to: romance scams (investment romance frauds, often framed as opportunity for relationship and financial partnership); task-based scams (victims are recruited for microtasks, only to discover tasks involve unlawful activity); call-centre fraud (inbound/outbound fraud via VoIP or traditional phone systems); and deepfake extortion (use of AI-generated video to create blackmail material).[47] Fraud is often polyglot: the same compound may conduct romance fraud in English, task scams in Russian, and investment schemes in Mandarin, targeting different victim demographics.

The lived experience experts provided detailed accounts of three primary scam typologies witnessed across compounds visited: romance scams,[48] where scam centre "workers" build prolonged online relationships before directing victims to fraudulent investment platforms; cryptocurrency task scams, where victims are lured into performing small tasks for payment before being asked to deposit increasing amounts; and call-centre fraud targeting, often elderly, victims with impersonation schemes.

Romance scams alone have cost victims globally an estimated $75 billion over four years, and the latest data indicates that crypto-enabled scams alone generated approximately $17 billion in 2025[49], making this a criminal enterprise of a scale comparable to traditional transnational organized crime.[50]

3.3 Compound Operational Structure

The testimonies of lived experience experts evince a highly hierarchical structure within Southeast Asian compounds: at the apex, owners connected to local security forces and political elites; below them, operations managers; then supervisors who oversee work of the teams, control large investment transactions and are often responsible for punishing and abusing trafficking victims who are assigned as team leaders. Team leaders then oversee groups of 10-15 "workers;" and at the base, the individuals recruited into these operations. Compounds reportedly operate as self-contained ecosystems with canteens, dormitories, and comprehensive surveillance systems. Workers are mostly prohibited from leaving the premises, or, if they could walk in the yard, they were solely allowed at designated areas. Any deviation would trigger punishment. The lived experience experts confirmed that digital control mechanisms include facial recognition at compound entrances and surveillance cameras in all work areas.

A similar structure was identified in Case 2 (North Macedonia)[51], where trafficking victims were housed in controlled premises and organised into a three-tier scam hierarchy: (1) frontline "operators" posing as workers at banks, postal services, or insurance companies; (2) intermediary actors posing as police officers to escalate deception; and (3) operators impersonating prosecutors or judges to pressure victims into transferring funds. Victims were closely supervised, subject to document confiscation and movement restrictions, and monitored continuously to ensure compliance with the fraud operation.

Compounds typically deploy sophisticated digital infrastructure, including specific software tools including "Hello World" for managing multiple social media accounts simultaneously and for auto-translated messages in multiple languages. They also use "i4.cn" for GPS location spoofing to make it appear that operatives are located in the target country rather than the compound location.[52]

Payments are processed exclusively through cryptocurrency (USDT/Tether), enabling rapid, hard to track financial flows. As documented by the OSCE[53], in many cases financial victims are first tricked into sending money from

their normal bank accounts to a crypto exchange (a VASP), which is often a legitimate and sometimes regulated platform. Once the money is deposited, it is converted into cryptocurrencies such as stablecoins and then sent to fake investment platforms controlled by criminals.

Working conditions in cyber scam compounds in Southeast Asia are characterised by severe and systematic abuse. The lived experience experts described 12-18-hour days without any weekly or monthly leave, electric shocks for non-compliance, confinement in dark rooms, and systematic debt bondage where workers owe $5,000-$30,000 for their "purchase price." Victims are "sold" between compounds for $5,000-$30,000 depending on language skills.

3.4 Human Trafficking Victim Profiles

Human trafficking victims in scam compounds originate from diverse geographic regions. According to lived experience experts, many known trafficking victims brought to Southeast Asia for scam centre operations are from OSCE participating States as well as other developing economies.[54] Victims are predominantly aged 18-40, with significant proportions possessing university-level education, IT skills, and multilingual capacity. The lived experience experts confirmed this profile, noting that victims typically held language skills and some professional background prior to recruitment. These findings are consistent with global analyses. INTERPOL reports that 61 per cent of suspected human trafficking facilitators are aged 20–39[55], while OHCHR finds that most victims fall within a similar young-adult age range, with 61 per cent aged 19–30, followed by 31–36 (22 per cent), 37–40 (11 per cent), and 41+ (6 per cent).[56]

3.5 Structural Parallels: From Southeast Asia to OSCE Area

Reporting from OCCRP, INTERPOL, Europol, and national authorities suggests that the operational architecture of cyber-scam centres is being replicated in the OSCE region. The reported structural parallels include: (1) recruitment targeting of multilingual professionals, aged 18-40, with computer skills; (2) deceptive job framing (e.g., iGaming, forex, customer service) concealing fraud roles; (3) relocation packages and housing provisions; (4) messaging-app routing to private contact; (5) rapid onboarding cycles; (6) hierarchical management structures between victim floor workers and managerial staff; and (7) use of cryptocurrency and money-mule networks for laundering of illicit proceeds.[57]

The "Four Families" - criminal organizations in Southeast Asia with alleged state protection - controlled vast scam empires generating billions in annual revenues.[58] However, 2025 brought significant disruptions to these networks through co-ordinated international action and internal conflicts, suggesting that law-enforcement intervention can reduce operational capacity.

Figure 4 highlights the operational replication of scam centre models from established hubs in Southeast Asia and the Gulf to emerging zones within the OSCE area. It identifies five primary source hubs and four OSCE regions where similar operational patterns are now being observed, connected by shared characteristics including deceptive social media recruitment, iGaming and crypto role framing, messaging-app routing, and relocation packages designed to facilitate victim movement across borders. The convergence of these operational characteristics across geographically distinct regions may indicate that scam centre models are being replicated rather than independently emerging.

3.6 Conditions for Operational Replication

Such a replication point to the potential risk of further expansion of cyber-scam operations in the OSCE region wherever three enabling conditions converge: (1) supply of vulnerable workforce (unemployed, linguistically skilled, seeking international mobility); (2) supply-side enabling factors (regulatory gaps in labour oversight, weakened immigration controls, porous borders, weak law enforcement, corruption); and (3) existing potentially criminal infrastructure (money-laundering networks, illicit telecommunications infrastructure, unregulated cryptocurrency exchanges, weak content moderation of social media platforms and emerging technologies).[59] The regions of Eastern Europe, South-Eastern Europe, South Caucasus, and Central Asia exhibit these conditions.

Figure 4:
Global Scam Centre Ecosystem - Established Hubs and Emerging Operational Zones

Data Analysis and Findings

4

This section presents the principal findings of the analysis, structured across three interrelated dimensions: first, the platforms and channels through which recruitment content is disseminated (Section 4.1); second, the geographic and linguistic characteristics of the identified material (Section 4.2); and third, platform-specific patterns, with particular attention to Telegram as a recruitment channel (Section 4.3).

4.1 Overview: Curated Dataset

The curated dataset consists of 82 recruitment advertisements collected from public-facing recruitment platforms between October 2025 and March 2026. It is complemented by a separate analysis of dedicated Telegram recruitment channels, which is addressed in a subsequent section. It must be noted that the dataset was developed through targeted collection focused on higher-risk geographic areas and should therefore be understood as an analytical sample designed to identify indicative recruitment patterns, rather than as a comprehensive representation of recruitment content across platforms.

Figure 6 presents the language distribution across the curated dataset. English accounts for the largest share of advertisements, followed by Russian, while Turkish, Romanian, and Italian form smaller but analytically relevant groupings. The remaining languages, including Kazakh, Bengali, Bulgarian, and Ukrainian, appear only in a limited number of entries. One advertisement was published in both English and Turkish. Taken together, this distribution aligns with the geographic focus of the dataset and offers an initial indication of the linguistic reach of the recruitment activity captured across the OSCE region.

4.2 Threat Assessment Classification

Building on the dataset overview presented above, the threat assessment classification of the curated sample provides a more granular indication of the level of concern associated with the advertisements collected. The elevated-risk classification of approximately one-third of all entries suggests that public-facing recruitment platforms may be hosting significant volumes of content exhibiting patterns consistent with documented scam centre recruitment practices. This proportion underscores the potential value of platform-level intervention, whether through automated content moderation informed by the indicator framework developed in this assessment, or through structured escalation pathways to law enforcement authorities.

Figure 6:
Threat Assessment Classification

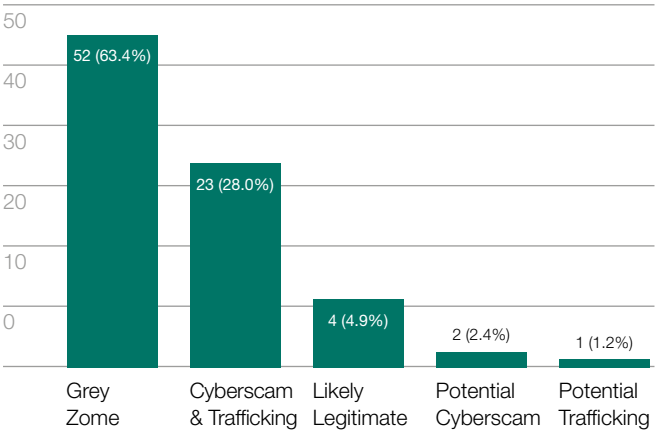
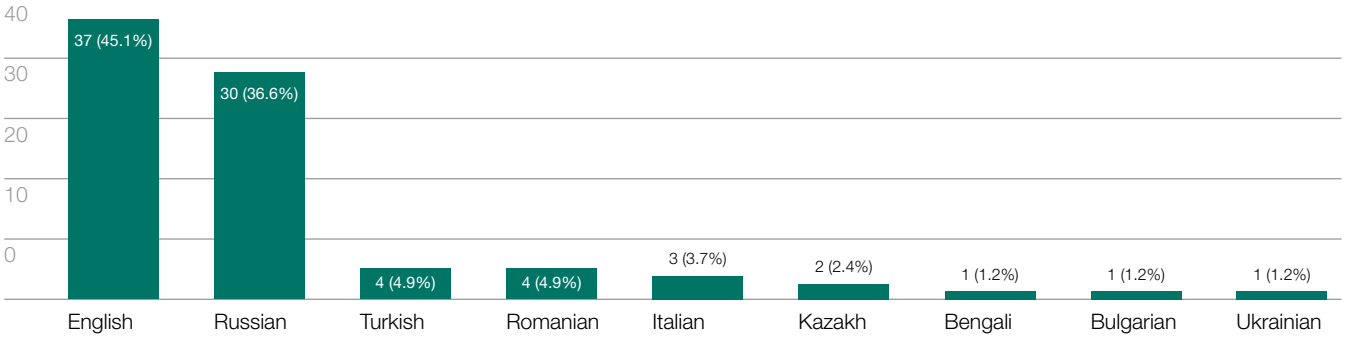


Figure 5:
Language Distribution of Advertisements as part of the curated qualitative dataset.



4.3 Geographic and Platform-Specific Findings

4.3.1 Regional Distribution: Curated Dataset

South-Eastern Europe accounts for the largest regional cluster in the curated dataset, followed by Central Asia, the South Caucasus, and Eastern Europe. Multi-destination advertisements - listing roles across several countries simultaneously - are common, particularly among entries referencing South-Eastern European and South Caucasus destinations. Elevated-risk classification rates vary considerably across regions, with a concentration of indicators associated with iGaming, cryptocurrency, and call centre roles in the two European clusters.[60] Geographic destination patterns reveal a concerning concentration: entries referencing Eastern Europe and South-Eastern Europe account for the highest shares of elevated-risk classifications, a pattern broadly consistent with international law enforcement operations targeting call centres and fraud networks in these areas, and with continuing reporting of ongoing fraud operations.[61]

Figure 7:
Geographic Distribution by Assessment Category

Country	Entries	Elevated-Risk	Elevated %	Risk Level
South-Eastern Europe	51	22	43%	Medium
Central Asia	25	3	12%	Low-Med
South Caucasus	16	5	31%	Low-Med
Eastern Europe	10	5	50%	Medium

Note: Multi destination advertisements may appear in more than one regional category.

The regional distribution of elevated-risk recruitment suggests that Eastern Europe and South-Eastern Europe show the highest concentrations of indicators consistent with scam centre-linked recruitment. The South Caucasus shows a comparable, though somewhat lower, pattern. By contrast, Central Asia, despite a substantial number of entries, records a markedly lower elevated-risk share, which may point to a different operational profile, potentially involving more domestic or grey-zone recruitment activity.[62] While law enforcement data corroborates substantial operational activity in the region, including the shutdown of numerous call centres and the blocking of millions of fraudulent calls in 2024-2025,[63] the Grey Zone classification suggests that these operations may differ structurally from those observed in other regions. Whether this lower elevated-risk share reflects a genuinely lower incidence of forced labour and trafficking within these operations, or whether it reflects different recruitment methods that are less visible through open-source monitoring, remains an open question that warrants further dedicated investigation.

These findings should be read as illustrative rather than definitive, as they are drawn from an exploratory open-source dataset of advertisements linked to potentially suspicious recruitment activity. Individual advertisements frequently reference multiple destination countries or regions, meaning that regional entry totals exceed the number of unique advertisements in the dataset. This reflects the multi-destination character of recruitment targeting and provides a useful basis for identifying patterns, concentrations, and areas of concern, while not constituting an exhaustive representation of the wider phenomenon.

4.3.1 Telegram as a Recruitment Platform

In addition to the curated dataset of 82 advertisements, a separate Telegram dataset was collected from dedicated Telegram recruitment channels, yielding 750 unique messages after deduplication. This platform was selected for further exploration following a preliminary analysis of recruitment channels, which identified Telegram, WhatsApp, and Viber as the main platforms of interest. Telegram was prioritised in this phase due to the open nature of its channels, survivor reports indicating its use in recruitment processes, and documented concerns about its misuse in Southeast Asian scam centre operations. This dataset provides a substantially larger indicator base and is indicative of the operational depth of Telegram-based recruitment infrastructure within the OSCE area.

The analysis shows that geographic targeting in Telegram is extensive and co-ordinated across multiple OSCE regions, with Eastern and South-Eastern Europe featuring prominently in recruitment messaging. This geographic breadth is highly suggestive that Telegram recruitment channels function as centralized, multi-country placement platforms and appear to serve as the public-facing entry point of a broader recruitment pipeline.

The Telegram dataset also reveals the specific operational functions that recruits are expected to perform within scam centre structures. Role terminology clusters tightly around fraud-specific tasks, such as retention, recovery, conversion, and crypto - terms that do not correspond to legitimate financial services positions. In the context of documented scam centre operations, "retention" typically refers to maintaining victim engagement in ongoing schemes, while "conversion," originally a marketing term for turning leads into customers, may refer to persuading victims to invest additional sums. The prevalence of this fraud-specific terminology across the dataset suggests that these Telegram channels function as specialised fraud recruitment infrastructure rather than generalist employment platforms.

Recruiter concentration analysis reveals significant organizational structure within the Telegram ecosystem: the top recruiter accounts collectively generate a high percentage of all recruitment messages. This distribution pattern is far more consistent with centralized professional recruitment networks and franchise models than with ad-hoc individual postings. For law enforcement and platform operators, this concentration suggests that disrupting a small number of key recruitment accounts may have substantial disruptive effect on broader operations and lead to high-impact law enforcement actions via investigations and prosecutions of key transnational criminal actors.

Recruitment indicators in the Telegram dataset parallel those observed in the curated dataset with notable consistency: relocation packages are referenced in approximately 28 per cent of messages, commission-based pay structures feature in approximately 5 per cent, and visa or work permit facilitation appears in 9 per cent. This indicator replication across independent datasets is highly indicative of a standardized recruitment model that operates consistently across platforms; the combination of relocation assistance, commission-based compensation, and direct messaging contact channels constitutes a possible connection to trafficking-linked recruitment activity.

4.3.2.1 Geographic Destinations Referenced in Telegram Recruitment Messages

Analysis of destination references across the 750 unique messages reveals a geographic distribution that broadly mirrors, but does not replicate, the patterns observed in the curated dataset.

Figure 8 presents destination references identified in the monitored Telegram recruitment channels, mapped to the four OSCE regions. Eastern Europe appears as the most frequently referenced destination, followed by the South Caucasus and South-Eastern Europe. A smaller number of references to non-OSCE destinations, may suggest linkages with established scam centre ecosystems beyond the OSCE area. Percentages reflect unique messages and may sum to over 100 per cent, as individual messages frequently reference multiple destinations.

While Figure 08 highlights where recruitment activity appears to be directed, Figure 10 provides additional insight into how these opportunities are framed at the level of advertised roles. Figure 09 presents the most frequently occurring role terms in the deduplicated Telegram dataset, showing that recruitment advertisements are concentrated around a relatively narrow set of operational functions. The most prominent terms are Retention, Crypto/Forex, Recovery, and Conversion, which appear substantially more often than more generic labels such as Sales, Manager, or Recruiter. This distribution suggests that the Telegram recruitment environment is not centred primarily on conventional corporate recruitment language, but instead on role categories associated with customer handling, financial persuasion, and transaction-linked operations. As such, the figure provides useful insight into the functional framing of advertised positions and the types of roles most commonly promoted across the dataset. Taken together, the two figures suggest a recruitment environment shaped both by identifiable regional targeting patterns and by a relatively consistent set of operational role functions.

Figure 8:
Telegram Dataset
Top Destination Regional References

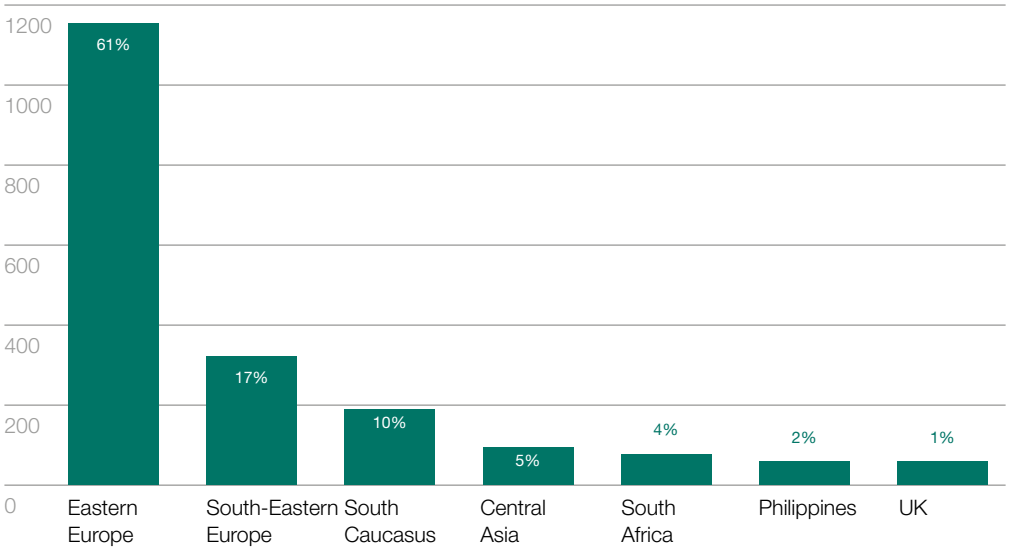


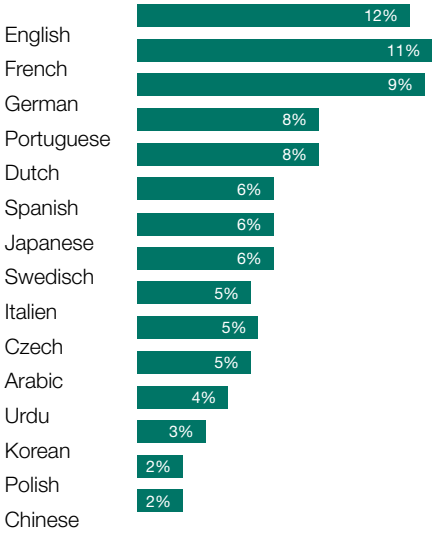
Figure 9:
Telegram Dataset - Key Role Terms

4.3.2.2 Language Requirements in Telegram-Based Recruitment

Language requirements in recruitment messages can provide a useful indication of the operational orientation and intended geographical reach of the roles being advertised. In this case, the monitored Telegram channels point to a notably broad linguistic range across the sampled recruitment environment.

Figure 10 provides an overview of the language requirements identified in the monitored Telegram recruitment messages. The deduplicated Telegram dataset therefore provides insight into the language skills sought by recruiters. Unlike the curated dataset, which is predominantly composed of advertisements written in English and Russian, the Telegram messages specify a wide range of target languages as job requirements. The most frequently referenced languages include English, French, German, Portuguese, and Dutch. These references appear to relate to the languages recruits are expected to use in their prospective roles, rather than the language of the advertisements themselves, which are written predominantly in English. This suggests that while English and Russian serve as the lingua franca of the recruitment channels themselves, the operational roles being advertised are designed to target victims across a diverse set of linguistic markets, predominantly in Western Europe.

Figure 10:
Telegram Dataset -Language Requirements



Synthesis of Telegram-Based Findings

In combination, the Telegram analysis complements the curated dataset by providing a distinct analytical perspective. Whereas the curated dataset captures the visible recruitment interface across platforms and languages, the Telegram data offers additional insight into the operational demand side, including the destinations, role functions, and linguistic capabilities for which personnel appear to be actively sought. The prominence of Western European languages among stated job requirements, combined with destination references concentrated in Eastern Europe and the South Caucasus, is broadly consistent with a model in which individuals may be recruited to support operations directed at higher-income, non-local victim populations. As such, the pattern may merit further examination in relation to the cross-border dimensions of these recruitment networks.

Furthermore, Telegram's architectural features - minimal content moderation, direct messaging architecture, rapid message deletion, and encryption options - appear to make it operationally preferable to Facebook, LinkedIn, or VK for traffickers, given the platform's capacity to facilitate rapid, largely unmonitored communication with prospective victims. This suggests that disruption strategies could specifically address the Telegram ecosystem, potentially through law-enforcement partnerships with Telegram's parent company and collaborative monitoring arrangements with OSINT specialists.

4.4 Recruitment Verticals

Occupational clustering within the dataset reveals a concentration in four primary sectors of jobs advertised for recruitment:

- **iGaming and online casino roles, primarily game presenter and live dealer positions, account for approximately 40 per cent of entries.**
- **Customer service, call-centre, and sales support roles account for approximately 34 per cent.**
- **Forex, cryptocurrency, and trading-related roles, including retention and conversion positions, account for approximately 21 per cent.**
- **The remaining 5 per cent comprises miscellaneous or unspecified roles.**

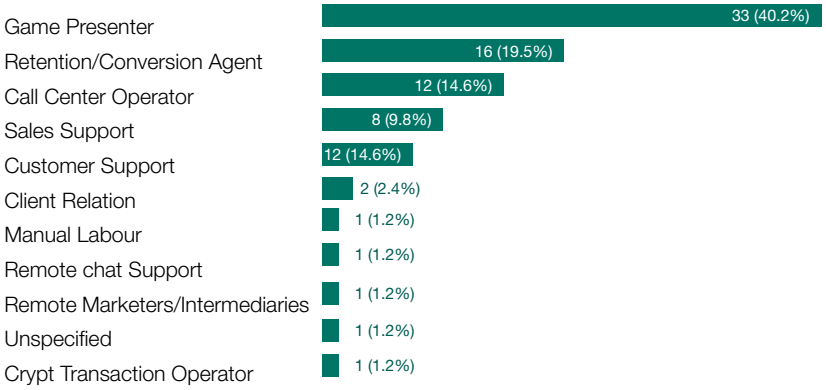
These occupational categories are not incidental; they reflect specific fraud typologies aligned with scam compound operations. iGaming roles enable the operation of fraudulent gambling and betting platforms targeting vulnerable victims; forex roles facilitate investment fraud schemes and victim retention through fake trading psychology; call-centre roles provide the infrastructure for voice-based fraud delivery and victim manipulation. For OSCE area employment authorities, labour inspectorates, and online platform operators, this pattern is indicative of a standardised recruitment playbook: job advertisements in these sectors, particularly those combining relocation offers, accommodation provisions, and above-market compensation, should be treated as potential trafficking indicators pending verification. The consistent clustering of these occupational framings with elevated-risk signals suggests deliberate targeting of vulnerable populations rather than isolated employment anomalies.

Occupational Risk Stratification

The distribution of elevated-risk classifications varies considerably across occupational categories. iGaming and casino roles, as well as forex, cryptocurrency, and trading-related roles, are substantially more likely to be assessed as elevated-risk than other categories in the dataset. These sectors more frequently exhibit the convergence of multiple indicators that characterise documented scam centre recruitment patterns, such as relocation packages, messaging-app routing as the primary contact mechanism, and document handling. Customer service, call-centre, and sales support roles, while representing a significant portion of the dataset, are comparatively less likely to meet the threshold for elevated-risk classification, though they may still present exploitative features in individual cases.

This variation across sectors carries implications for policy and practice. Regulatory frameworks governing online recruitment may benefit from incorporating sector-specific risk flags, particularly where iGaming or forex-related roles are combined with relocation offers and private messaging as the sole contact pathway. Such an approach could support frontline practitioners in prioritising high-risk content for further review while maintaining proportionality toward legitimate recruitment activity.

Figure 11:
Primary Occupational Categories



4.5 Indicator Analysis

Analysis of indicator frequency across the curated qualitative dataset identifies the five most prevalent markers of recruitment methods with elevated risk of human trafficking:

1. **Messaging-app routing: Primary contact via Facebook, Telegram, WhatsApp, Signal, Viber, or similar platforms rather than formal email or phone systems.**

2. **Rapid onboarding or immediate start: No background checks, credential verification, or trial period; offers of immediate employment.**

3. **Relocation and housing included: Explicit offers of relocation assistance, housing, visa processing, or travel arrangements.**

4. **Vague role descriptions: Job postings lacking clear role definition, performance metrics, or occupational specificity.**

5. **Copy-paste or templated language: Identical or near-identical text distributed across multiple platforms or accounts.**

The convergence model presented above provides a structured framework for assessing the risk level of individual recruitment advertisements. For frontline practitioners, this model means that no single indicator in isolation is sufficient to establish a trafficking concern - rather, it is the accumulation of several indicators across multiple domains (recruitment content, channel and process, credibility signals, facilitation, and exploitation risk) that elevates an advertisement from a grey zone to a high-risk classification. This tiered approach is designed to reduce both false positives and missed detections, and it may serve as a basis for standardised screening protocols at the national level.

Figure 12:
Top Indicator Markers by Frequency

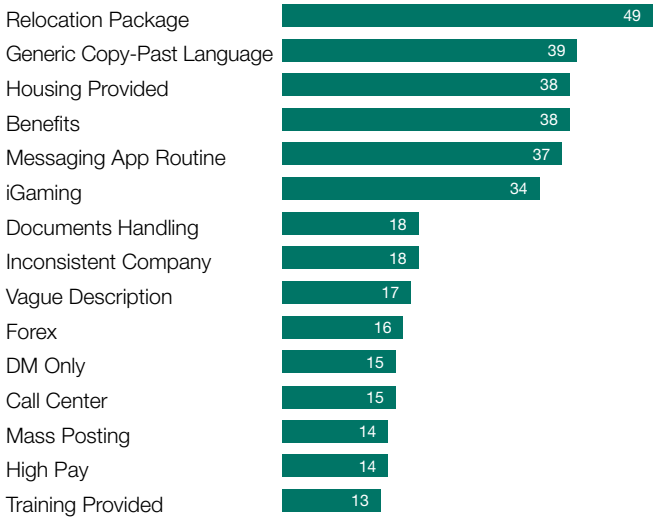
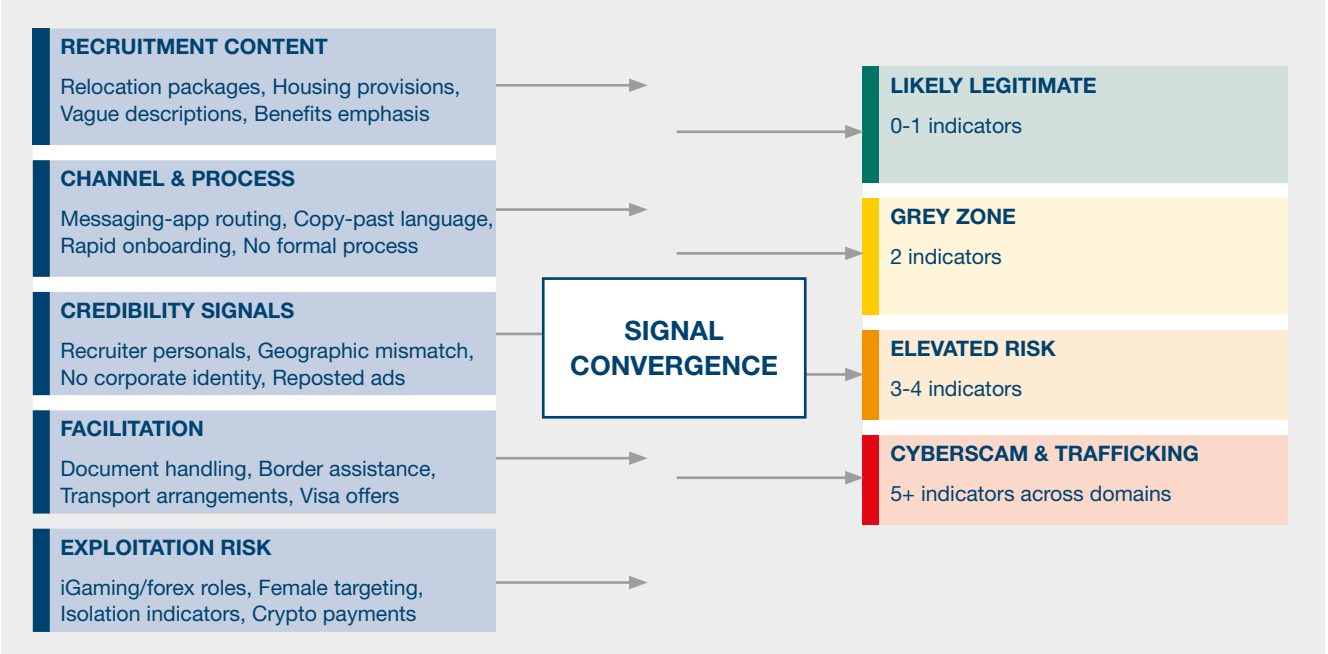


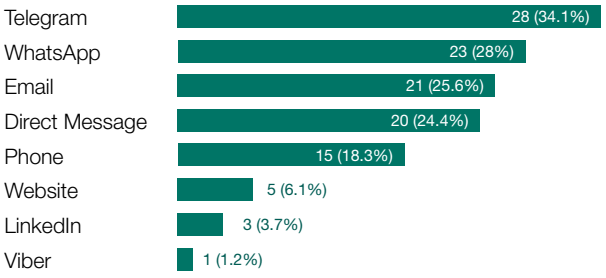
Figure 13:
Online Signal Assessment
Indicator Convergence Model



4.6 Contact Pathways and Facilitation Mechanisms

Contact pathway analysis reveals a strategic preference for messaging applications over traditional employment contact channels. Telegram accounts for 34 per cent of recruitment pathways, followed by WhatsApp at 28 per cent; email, direct messaging on social platforms, phone, and formal website referrals comprise substantially smaller portions. This pronounced concentration in messaging apps is indicative of a deliberate strategic shift away from platform-moderated channels towards encrypted and ephemeral messaging environments; this shift enables rapid one-to-one relationship-building with prospective victims while circumventing platform-level content moderation mechanisms. From an operational perspective, this finding suggests that platform-specific anti-trafficking interventions on mainstream social media – while necessary – may prove insufficient in isolation. For law enforcement, platform operators, and labour regulators, this pattern implies that disruption strategies must encompass messaging-app ecosystems where initial recruiter contact increasingly occurs; without co-ordinated action across messaging platforms, mainstream platform takedowns may simply displace rather than eliminate recruitment activity.

Figure 14:
Primary Contact Pathways



Movement logistics – whether explicitly offered or implicitly referenced – appear in over half of all advertisements; and the relocation packages observed typically combine explicit international movement mechanisms (visa processing, flight arrangements, accommodation provision) with implicit local movement within destination countries (airport transfers, placement in recruiter-provided housing). This combination of provisions, which systematically removes the prospective worker's independent logistical agency and decision-making capacity, is consistent with patterns documented in trafficking contexts where victim dependence on the employer is deliberately constructed from the point of initial recruitment. For frontline practitioners in labour inspectorates and border agencies, this multifaceted facilitation infrastructure is a key indicator that distinguishes potential trafficking recruitment from conventional labour migration.

Gender Dimensions of Scam Centre Trafficking

5

5.1 Gender dimension

Women and girls make up 61 per cent of detected global trafficking victims according to the UNODC Global Report on Trafficking in Persons (2024).[64] Recent reports from OHCHR identified that 21.1 per cent of victims trafficked in cyber scam operations were women.[65] According to INTERPOL, 20 per cent of human trafficking facilitators were female.[66] In the OSCE region, three Ukrainian women were trafficked into a fraudulent call centre in Poland in 2026,[67] 12 women were trafficked into a fraudulent call centre in Montenegro in 2020,[68] and Taiwanese women were identified as trafficking victims in an illegal call centre in Croatia in 2018.[69]

Female workers are disproportionately assigned to romance scam operations requiring video calls and intensive social engineering skills. More critically, they face systematic sexual abuse from compound managers and guards. The survivor consultant confirmed that some compounds maintain what are termed "entertainment sections," where female workers are coerced into sexual services for compound management and visiting associates. This represents a layered exploitation model combining both trafficking for forced criminality and sexual exploitation.

Case examples from both Southeast Asia and Balkan operations presented in this report illustrate consistent patterns of gender-specific exploitation. Female victims recruited for romance scam operations must conduct prolonged social engineering against target victims while facing sexual coercion from compound management. The survivor consultant described female-specific operating procedures within compounds, including requirements to maintain sexually-suggestive profiles on dating platforms and to engage in video calls designed to build intimate connections with fraud victims – all under coercive control and threat of violence.

Despite this global pattern, the scam centre context presents a distinct gender profile with the number of male victims prevailing. While women who are trafficked to scam centres face distinctly different and compounded forms of exploitation, data on the scope of their role in cyber-scam compounds is nascent.

5.2 Dataset Indicators of Gender-Based Targeting

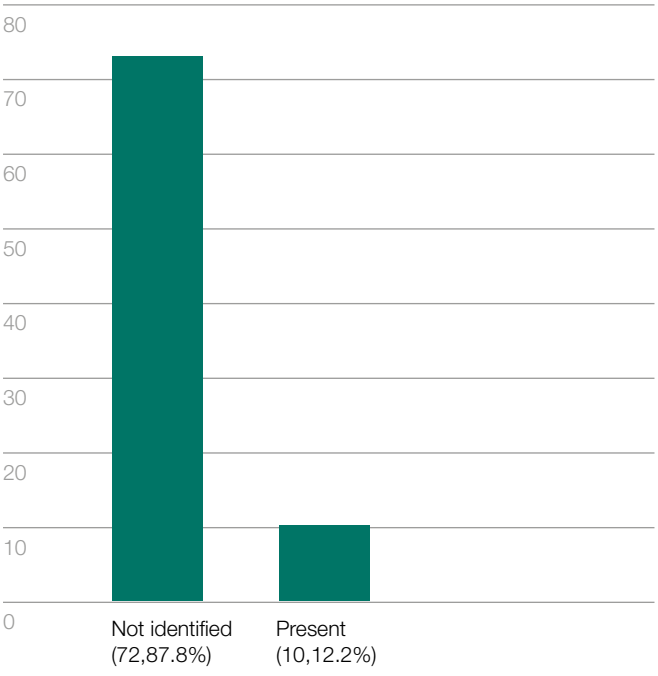
5.2.1 Curated Dataset (Qualitative Analysis)

Analysis of the curated dataset identifies gender-based risk indicators in 12 per cent of advertisements, concentrated in iGaming and hospitality roles. Specific gender-targeting language includes explicit "female-only" targeting; emphasis on physical appearance, personality, or age; and reframing of positions as modelling, entertainment, or glamour-industry roles. These language patterns correlate strongly with elevated-risk classification and are consistent with documented sexual exploitation patterns observed in Southeast Asian compounds. For practitioners, the clustering of gender-based language with specific occupational sectors suggests that certain industry framings function as proxies for sexual exploitation risk.

5.2.2 Telegram Dataset (Quantitative Analysis)

To complement the qualitative findings of the curated dataset, a keyword analysis was conducted across the Telegram dataset of 750 unique recruitment messages. This analysis examined the prevalence of gender-related, appearance-based, and facilitation indicators across a larger and less curated sample of recruitment content.

Figure 15:
Gender-Based Targeting Indicators



The Telegram dataset reveals a notable pattern in how gender-based targeting operates at scale. Explicit gendered language, such as references to women or female-specific terms, is rare in broadcast recruitment channels. Instead, appearance-related terminology, including words such as "attractive," "presentable," and "good-looking," appears with greater frequency, particularly within iGaming and trading-related advertisements. This suggests that recruiters may be using appearance and personality criteria as indirect selection mechanisms to target women, without deploying overt gender-specific language that would be more likely to trigger automated content moderation.

This finding is consistent with the curated dataset, where gender-based targeting similarly operates through role framing and appearance emphasis rather than direct gender specification. From an enforcement and platform governance perspective, this pattern points to a deliberate evasion strategy: gendered targeting that is designed to function below the threshold of keyword-based automated detection, and which may therefore require human review protocols to identify reliably.

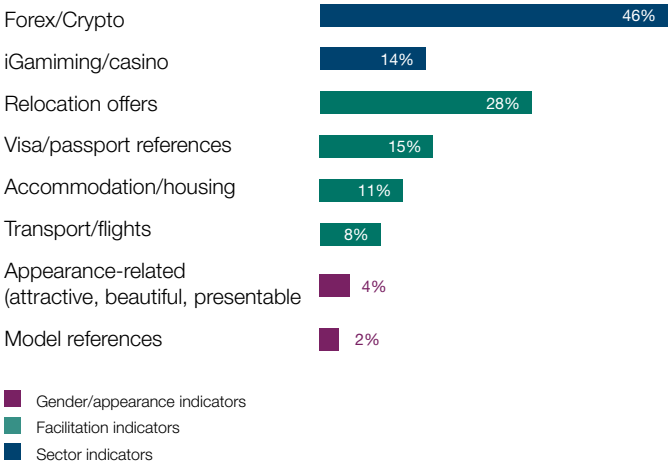
Facilitation indicators, including relocation offers, accommodation provisions, visa or passport references, and transport arrangements, are substantially more prevalent across the Telegram dataset than gender-specific language. In a small but notable share of messages, appearance-related language co-occurs with relocation offers, representing a convergence of gendered targeting and movement facilitation. For practitioners, recruitment content combining appearance criteria with relocation or travel provisions may warrant elevated scrutiny, regardless of the occupational sector in which it appears.

These findings suggest that explicit gendered language is substantially less prevalent in Telegram's broadcast recruitment channels than in direct-message curated advertisements-a difference that likely reflects the public nature of Telegram messaging and the requirement to circumvent platform content moderation. The underlying patterns, however, remain consistent: appearance-based selection criteria, combined with extensive facilitation offers and concentration in high-risk sectors, indicate that gender-based targeting operates through more subtle mechanisms across large-scale recruitment channels. This modulation of language suggests perpetrator sophistication: overt gendering language appears only in more private or curated contexts, whereas broadcast channels employ coded appearance and personality criteria that function identically while evading automated content detection. For content moderation teams, this pattern suggests that appearance-based language warrants closer scrutiny in recruitment contexts and may require human review protocols rather than keyword-based automation.

5.3 Online Sexual Exploitation Convergence

A notable correlation may be observed between the expansion of online sexual exploitation investigations and reported scam centre expansion across OSCE participating States: such investigations increased from 9 cases to 1,665 between 2021 and 2025 across a sample of OSCE states,[70] a trajectory that appears to coincide with reported increases in scam centre recruitment activity. While the relationship between these two trends requires further investigation, the data suggests a possible convergence in which perpetrators may be leveraging scam centre infrastructure for dual-purpose sexual exploitation and fraud operations.

Figure 16:
Telegram Dataset
Targeting and Facilitation Indicators



Case Studies and Operational Examples

6

6.1 Southeast Asian Operational Model

6.1.1 Compound Conditions and Victim Profiles

Survivor testimony describes severe working conditions across documented scam compounds, including 12-18 hour shifts, physical punishment for failure to meet fraud quotas, and systematic debt bondage, with individuals reportedly owing between $5,000 and $30,000 for their initial transfer between operators. Movement is heavily controlled through facial recognition systems, surveillance of all work and communication areas, and restrictions on external contact. Workers are required to use specific software tools to conduct fraud operations while concealing actual perpetrator locations, including geographic spoofing platforms.

Victim profiles tend toward individuals aged 18 to 40 with multilingual capacity and some professional or university-level education. The lived experience consultant identified victims originating from at least 60 countries.[71] Approximately 80 per cent of compound workers are male, with women disproportionately assigned to romance scam operations.

6.2 Emerging Displacement Patterns: Southeast Asia to the OSCE Region

Open-source monitoring of recruitment platforms and social media has identified what may constitute an emerging displacement pattern in the scam centre ecosystem. Following intensified law enforcement crackdowns, where co-ordinated international operations have disrupted compound infrastructure since mid-2025 – there are indications that some operators may be relocating their operations to jurisdictions perceived as offering weaker enforcement environments.

One such jurisdiction that appears to be emerging as a potential destination is in the South Caucasus region. Social media monitoring has identified recruitment advertisements in Facebook groups associated with Southeast Asian job recruitment that explicitly reference relocation of operations from Southeast Asia to the South Caucasus. The screenshot below, sourced from a public Facebook group examined for the purpose of this assessment showed the following pattern: a recruiter openly advertises that their company has "shifted" from Southeast Asia to the South Caucasus and invites interested individuals to make contact via a Telegram handle.

This pattern may be consistent with broader intelligence suggesting that the scam centre operational model is evolving in response to enforcement pressure. A source with direct experience of scam centre recruitment networks has observed that individuals who previously posted deceptive job advertisements to lure people into scam centres - typically concealing the true nature of the work - appear to have shifted their approach since approximately mid-2025. According to this source, some recruiters now openly acknowledge that the positions involve scam-related work, suggesting a growing brazenness in recruitment tactics that may reflect both market normalisation and reduced fear of enforcement in certain jurisdictions.

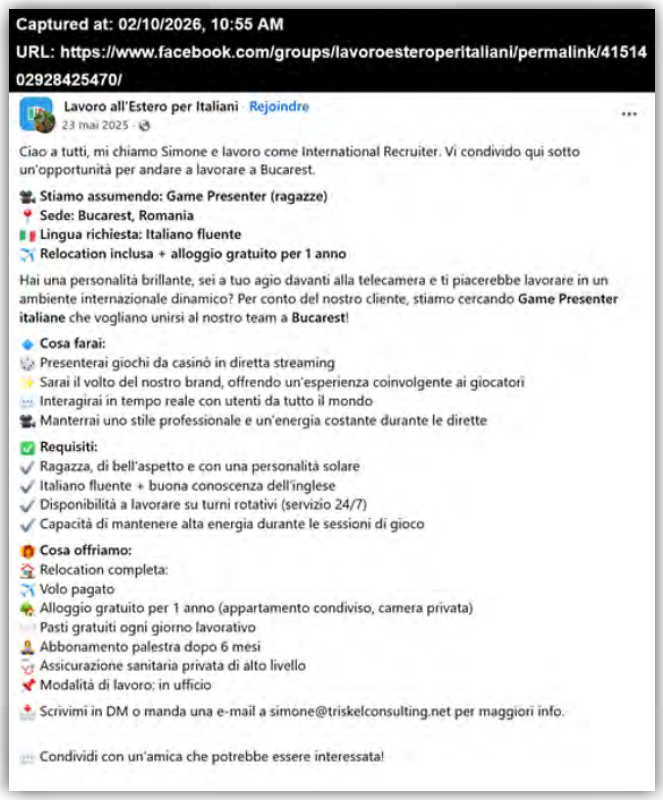
The source further indicated that the ownership structure of some smaller scam operations appears to be changing. Individuals who were themselves initially trafficked into scam compounds – particularly those of Indian, Bangladeshi, and Pakistani origin – may have subsequently learned the operational methods, established connections with existing scam infrastructure, and begun establishing their own smaller-scale operations. These individuals reportedly rent apartments and recruit co-nationals, leveraging shared language and cultural familiarity to facilitate recruitment. This pattern of victim-to-perpetrator transition has been documented in other trafficking contexts and represents a particularly concerning dimension of the scam centre ecosystem.

The possible connection between the reported relocation to the South Caucasus and the intensified crackdowns in Southeast Asian hubs warrants further investigation. If confirmed, this pattern would suggest that enforcement success in one jurisdiction may inadvertently displace operations to OSCE participating States or neighbouring regions, underscoring the need for a co-ordinated, multi-jurisdictional approach to disruption. OSCE participating States may wish to monitor recruitment patterns targeting or originating from the South Caucasus and comparable jurisdictions that could serve as alternative operational bases for displaced scam centre networks.

6.3 Illustrative Case Vignettes from the Dataset

Vignette A:
Italian-Language Game Presenter, Eastern Europe and South-Eastern Europe

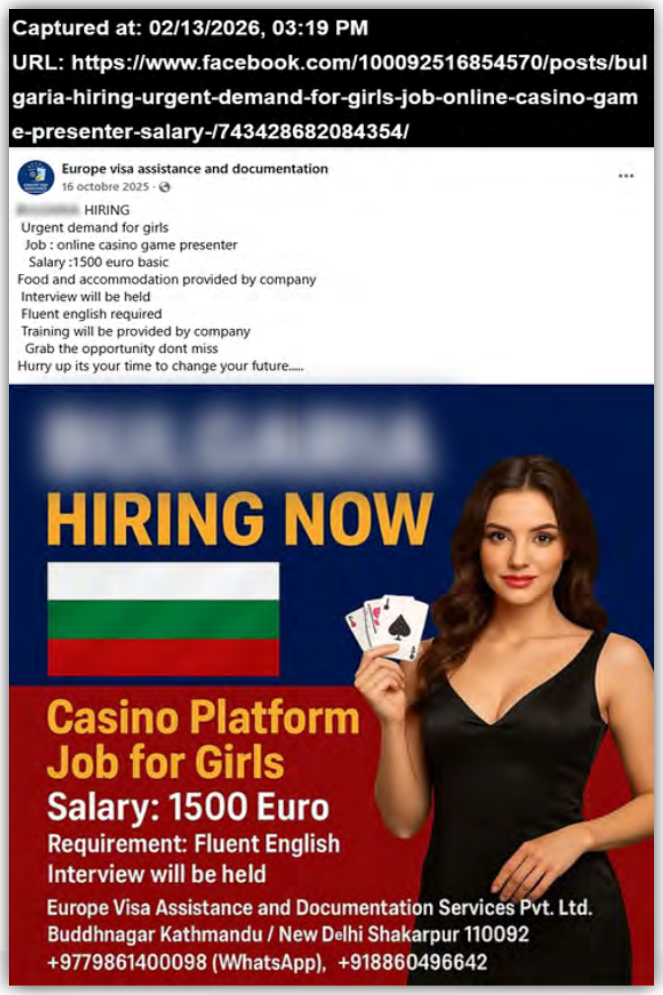
This advertisement, sourced from Italian language spaces, explicitly targets girls with emphasis on physical appearance ("good-looking") and personality ("sunny personality"). The use of diminutive language ("girls" rather than "women") and appearance-based criteria are hallmarks of sexual exploitation recruitment. The regional location and role framing (game presenter) align with documented iGaming fraud and sexual exploitation networks.



Screenshot
Italian iGaming recruitment ad, Bucharest. Translated:
"Hi everyone, my name is Simone and I work as an International Recruiter... We are hiring: Game Presenter (girls). Requirements: Girl, good-looking and with a sunny personality..."

Vignette B:
Female Casino Platform Job, Eastern Europe and South-Eastern Europe (International Recruiter)

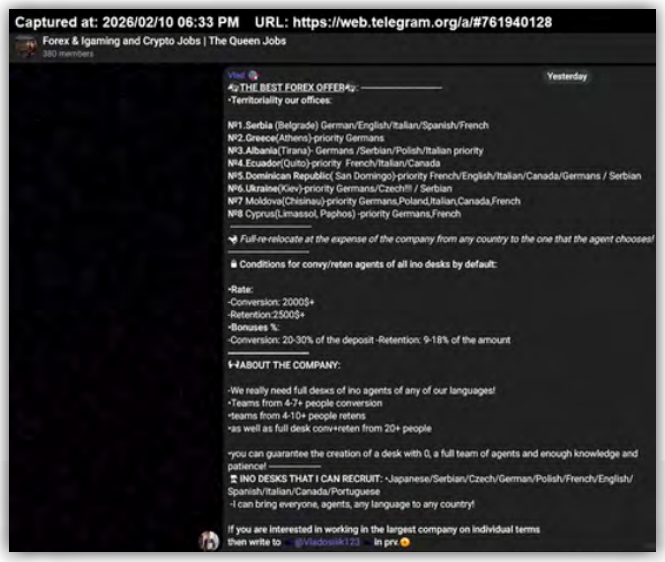
This advertisement combines multiple exploitation pathways: visa facilitation (increasing victim dependence on traffickers for movement and documentation), female-only targeting, casino employment (inherently objectifying), and geographic targeting (a known hub region). The presence of international recruiters suggests transnational recruitment networks extending beyond the OSCE region.



Screenshot
International recruiter advertising female casino jobs in Eastern Europe and South-Eastern Europe with visa assistance

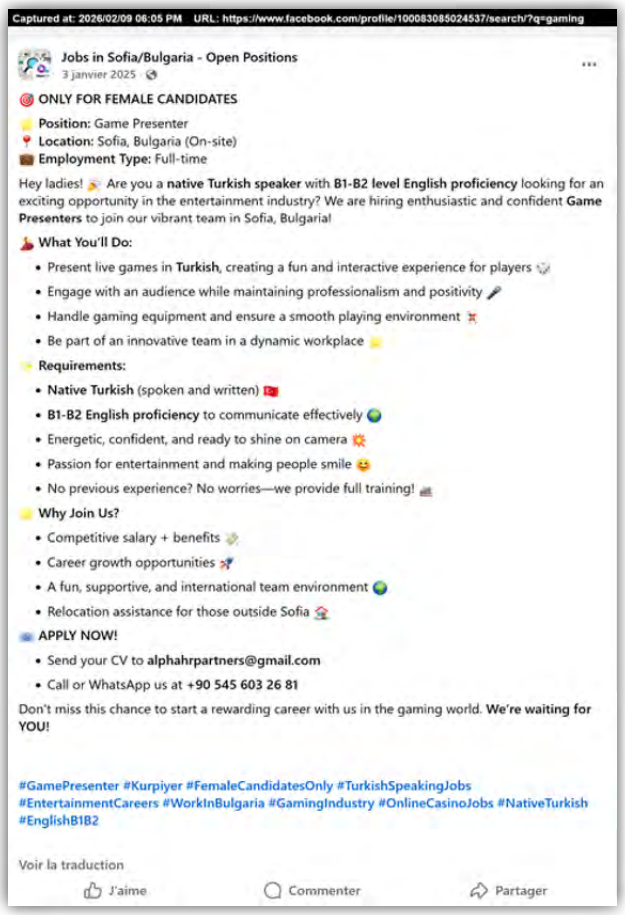
Vignette C:
Forex Recruitment Pipeline

The Telegram forex ecosystem represents a specialized recruitment vertical focused on "retention" and "conversion" roles. Vignettes AD-030 and AD-033 show advertisements targeting multiple OSCE regions – including Eastern Europe and South-Eastern Europe, the South Caucasus, and the Eastern Mediterranean – with roles defined as "retention manager," "conversion specialist," and "recovery manager." These roles do not exist in legitimate forex operations; they are compound-specific functions wherein perpetrators are tasked with preventing victim withdrawal of funds or manipulating existing victims into continued production.



Screenshot
Telegram forex recruitment, multi-country, specialized role language

Vignette D:
iGaming Network Clustering



Screenshot
Turkish female game presenter, Eastern Europe and South-Eastern Europe urban centre. Minimal detail, messaging-app contact

Consolidated Indicator Taxonomy

7

7.1 Overview

The following taxonomy presents the full indicator framework used to assess recruitment content in this study. Indicators are organised into five categories: (A) Recruitment Appeal and Targeting, (B) Channel and Process, (C) Credibility Manufacturing, (D) Facilitation and Movement, and (E) Exploitation Risk and Safeguarding. The taxonomy is designed to be applicable beyond this dataset – as a practical screening tool for frontline practitioners, platform moderators, and regulatory bodies assessing online recruitment content for indicators of trafficking and cyber-fraud.

Content exhibiting four or more indicators across categories should be classified as Elevated-Risk and escalated for further investigation or removal.

A. Recruitment Appeal and Targeting Indicators

1. **High salary with minimal qualifications:** Compensation significantly above market rate for stated role and required experience.
2. **Rapid salary increases or bonus structures:** Promises of steep salary progression or bonus payments contingent on performance metrics.
3. **Vague role description:** Absence of clear occupational definition, performance expectations, or reporting structure.
4. **Occupational framing misalignment:** Role title inconsistent with role description (e.g., “game presenter” for fraud roles).
5. **Occupational clustering around fraud-adjacent roles:** iGaming, forex, crypto trading, customer service/call centre, retention, conversion, recovery roles.
6. **No experience required or minimal qualifications:** Roles open to applicants with minimal or no relevant professional experience.
7. **Language emphasis:** Emphasis on multilingual capacity, specific language combinations, or language premium pay.
8. **Age or demographic targeting:** Explicit or implicit targeting of specific age groups, nationalities, or demographic categories.
9. **Relocation and housing:** Explicit offers of relocation assistance, housing provided, visa processing, or travel arrangements.
10. **Visa or document processing assistance:** References to visa support, work permit processing, or document handling.
11. **Work-from-home or flexible location:** Remote work or location-independent roles, particularly with cryptocurrency or customer service framing.
12. **Female-only or appearance-based targeting:** Explicit gender limitation or emphasis on physical appearance, personality, or age.
13. **Celebrity, modelling, or entertainment framing:** Reframing of positions (croupier, game presenter) as modelling, entertainment, or glamour-industry roles.

B. Channel and Process Indicators

1. **Messaging-app routing for primary contact:**
   Telegram, WhatsApp, Signal, Viber, or other messaging applications as primary contact mechanisms.
2. **Copy-paste or templated language:**
   Identical or near-identical text distributed across multiple platforms or accounts.
3. **Rapid onboarding or immediate start:**
   No background checks, credential verification, or trial period; offers of immediate employment.
4. **Payment requests or deposits:**
   Requests for deposits, processing fees, or educational payments prior to employment.
5. **Cryptocurrency emphasis or crypto-transaction roles:**
   Explicit mention of cryptocurrency, blockchain, or roles involving crypto transactions.
6. **No company verification or weak corporate identity:**
   Absence of registered company information, verifiable office locations, or company website.

C. Credibility-Manufacturing Indicators

1. **Use of recruiter profiles or personas:**
   Recruitment through named individual recruiters with limited verifiable history.
2. **Geographic mismatch between recruiter location and job location:**
   Recruiter based in a different country than job location.
3. **Minimal recruiter profile or stock photos:**
   Recruiter profiles with limited information or use of generic or duplicated images.
4. **Multiple job titles or roles offered by a single recruiter:**
   Single recruiter advertising diverse occupational categories, suggesting batch recruitment.

D. Facilitation and Movement Indicators

1. **Document handling emphasis:**
   References to passports, visas, travel documents, or document processing.
2. **Border crossing assistance:**
   Explicit or implicit offers of help navigating international borders, immigration, or customs.
3. **Transportation or travel arrangements:**
   Offers of flight booking, ground transportation, or travel co-ordination.
4. **Debt bondage framing:**
   Language suggesting applicant indebtedness for visa, transportation, or housing, to be "repaid" through labour.

E. Exploitation-Risk and Safeguarding Indicators

1. **iGaming, online casino, or “game presenter” language:**
   Roles explicitly referencing online gaming, casino, croupier, or live-dealer positions.
2. **Forex, “retention,” “conversion,” or "recovery" roles:**
   Language specific to financial fraud, victim retention, or money-mule networks.
3. **Call-centre, customer service, or sales roles with fraud indicators:**
   Occupational framing suggesting customer-interaction fraud.
4. **Isolation risk (messaging-app routing + housing + relocation):**
   Co-occurrence of isolation mechanisms (control of communication, housing, movement).
5. **Sexual exploitation indicators (appearance, entertainment, female-only):**
   Gender-based targeting emphasizing appearance and sexual objectification.
6. **Compound-like language or structure (occupational hierarchy, team-based, control mechanisms):**
   Language suggesting hierarchical management, team-based operations, or control mechanisms.

7.2 Application Guidelines

The taxonomy is designed as a structured screening framework rather than a diagnostic checklist. No single indicator should be considered sufficient to classify an advertisement as exploitative; rather, it is the convergence of indicators across multiple categories that may signal elevated risk.

In applying this framework, the cross-category breadth of indicators present in a given advertisement may be more analytically significant than the number of indicators within any single category. For example, an advertisement that combines a relocation offer (Category A) with messaging-app routing (Category B) and document handling (Category D) may present a different risk profile than one that triggers several indicators within one category alone.

Contextual judgement remains essential. Certain indicators are common features of legitimate recruitment in specific sectors, such as relocation packages or messaging-app contact. Their significance increases when they co-occur with other markers, such as vague role descriptions, weak corporate identity, or the absence of verifiable employer information.

Where content meets or exceeds the four-indicator threshold across categories, it may be appropriate to flag it for further review within existing institutional mechanisms, whether platform-level trust and safety processes, national referral mechanisms, or relevant law enforcement channels. Content falling below this threshold but exhibiting indicators in Categories D or E (facilitation, movement, and exploitation risk) may nonetheless warrant continued monitoring.

The framework is intended to complement existing national and international identification and referral mechanisms. Its potential value lies in supporting earlier detection of recruitment content that may be linked to trafficking or cyber-fraud, at a stage where intervention remains possible before individuals enter the recruitment pipeline.

The framework is intended to complement existing national and international identification and referral mechanisms.

Recommendations for Policy and Practice

8

8.1 Prevention

OSCE participating States face a substantive prevention challenge when it comes to cyber-scam operations. Recruitment content is engineered to evade casual scrutiny while incorporating sufficient indicators to enable post-recruitment deception and coercion. Prevention efforts are advised to address the following areas of intervention:

Legal framework: National laws' human trafficking definition should include forced criminality as a form of trafficking. OSCE participating States should formally recognize cases where individuals are compelled to engage in criminal activity as a form of human trafficking. This must be reflected in both legislation and policy documents.

Regulatory frameworks: Introduction or strengthening of regulations requiring employment agencies, recruiters, and labour brokers to register, verify, and maintain audit trails of recruitment activities and candidate placements.

Regulation of recruitment channels: Most cases begin with deceptive job offers. Greater oversight is needed over online job platforms, messaging applications used for recruitment, private employment agencies.

Awareness-raising: Public communication campaigns should target young, multilingual, and unemployed populations with messaging about scam centre recruitment, using the indicator taxonomy as educational reference in multiple languages. These initiatives should include meaningful youth engagement, to ensure peer-to-peer and community-based outreach.

Platform engagement: Co-ordination with Facebook, Telegram, LinkedIn, VK, and other platforms to enhance detection, reporting and removal of scam-centre-linked recruitment content, using indicator-based classification. Such engagement should also be established through partnership between law enforcement agencies and technology and social media companies.

Educational integration: Inclusion of forced criminality and scam centre recruitment awareness in secondary and tertiary education, particularly for language and engineering students and students entering international labour markets.

8.2 Protection

OSCE participating States should develop tailored victim-centred protections addressing the unique vulnerabilities of trafficking victims and victims of forced criminality.[72] Protection efforts should encompass:

Victim identification and referral: States should enhance efforts to identify victims of forced criminality proactively and promptly using the indicator taxonomy proposed in this paper and in the OSCE model Standard Operating Procedures[73] and refer them to protection services rather than prosecuting or forcibly deporting them, including training of frontline responders (e.g., police, labour inspectors, border officials, social workers).

Training and capacity building: All front-line agencies (i.e., law enforcement, migration authorities, and consular staff) should be trained to identify indicators of forced criminality, including but not limited to restriction of movement, debt bondage, psychological coercion, and control over communication as well as on the non-punishment principle, trauma, psychological coercion, and the irrelevance of consent.

Tailored survivor-informed protection services: Establishment of specialized services for survivors of trafficking for forced criminality and the establishment of dedicated rehabilitation programmes addressing the specific psychological trauma of forced participation in fraud.

Protection from prosecution: Individuals involved in scam operations under coercion should not be treated as offenders. Legal mechanisms must be in place and consistently applied to exempt victims from criminal liability where coercion is present. The application of the non-punishment principle is crucial as many survivors fear prosecution for crimes they were forced to commit related to their exploitation in human trafficking. States should enshrine the non-punishment principle in law and provide guidance and training for police, prosecutors, and judges on explicit legal protections from prosecution and punishment for trafficking victims compelled to commit illegal acts, aligned with international standards, OSCE commitments and the Council of Europe Convention on Action against Trafficking in Human Beings.

Family notification and support: Mechanisms to contact families of trafficking victims (where safe to do so) and provide information, financial support, and repatriation assistance.

Debt clearing/relief: Legal remedies to clear debts imposed on trafficking victims through fraud or coercion.

8.3 Disruption and Prosecution

Operational disruption of cyber-scam centre infrastructure and prosecution of perpetrators require co-ordinated action across law enforcement, financial investigation and intelligence, and cyber security:

Specialized prosecution units: Establishment of dedicated units focused on trafficking for forced criminality, ensuring specialized expertise and continuity.

Evidence standards for indicator-based investigations: Development of prosecutorial guidance on the use of indicator convergence in establishing trafficking victim status and fraud, recognizing that perpetrator confessions are unlikely and circumstantial evidence will dominate. Prosecutorial guidance and training should include instructions on not prosecuting trafficking victims for criminal acts they were compelled to commit related to their trafficking situation.

International co-operation: Establishment of dedicated co-ordination mechanisms with OSCE participating States and international partners to enable rapid information-sharing and joint operations. As these schemes are transnational, stronger cross-border co-operation is essential. Strengthened MLA frameworks and extradition treaties enabling prosecution of perpetrators who have fled to third countries.

Financial investigation and asset recovery: Specialized financial investigation units targeting money laundering and illicit financial flows associated with scam centre operations, co-ordinating with financial intelligence, private sector, financial institutions and cyber police. Seizure and recovery of cryptocurrency wallets, bank accounts, real-estate assets, and other proceeds (that should be applied toward compensation for trafficking victims and financial victims).

Cyber disruption: Takedown operations targeting scam-centre-operated platforms (fake investment apps, fraudulent crypto exchanges), call-centre infrastructure (VoIP providers, cloud hosting), and money-mule co-ordination systems.

Telecommunications regulation: Regulation of VoIP providers, SIM card issuance, and routing providers to prevent use by scam centres for fraud delivery.

Money-mule network disruption: Identification and prosecution of money-mule networks, with protective measures for individuals who are themselves trafficking victims.

Corporate liability: Expansion of corporate liability frameworks to address organizations that facilitate scam centre operations (landlords, immigration brokers, recruitment agencies, financial institutions, technology and social media platforms).

Sentencing harmonization: Alignment of sentencing practices across jurisdictions to ensure that traffickers who force victims to scam others receive sentences commensurate with the severity of human trafficking.

Conclusion

9

The Southeast Asian cyber scam centre phenomenon using trafficking victims to defraud millions of financial victims of fraud has long been understood as a region-specific problem – a consequence of geopolitical instability, governance vacuums, military entrenchment in organized crime, and geographic proximity to China. This assessment challenges that assumption.

The growing structural parallels between Southeast Asian compound operations and OSCE area recruitment infrastructure are significant and warrant close examination: deceptive job framing; messaging-app routing; relocation and housing inducements; targeting of multilingual professionals; rapid hiring cycles; vague job role descriptions; and occupational clustering around iGaming, forex, and call-centre roles. The findings suggest that scam centre recruitment of trafficking victims is a replicable and replicated model, responsive to geographic variation and local enabling conditions.

The Eastern Europe and South-Eastern Europe region accounts for a substantial share of elevated-risk indicators in the curated dataset. A range of contextual factors may make parts of the region conducive to the establishment of scam-centre activity, including gaps in labour inspection and oversight of employment agencies, geographic conditions that may facilitate movement and financial transfers, the availability of cryptocurrency exchange infrastructure, and a strategic position for transit. Reporting from law enforcement across multiple jurisdictions further points to the presence of sophisticated fraud- and trafficking-related activity.

Central Asia shows a different threat profile. Central Asian states exhibit predominantly domestic rather than cross-border recruitment, with Grey Zone classifications predominating over elevated-risk. Yet the scale of law enforcement response indicates substantial operational activity.[74]

Central and Western European countries remain significant financial victim-origin jurisdictions, with nationals reporting substantial financial losses to romance fraud,[75] and appearing among trafficking victims identified in Southeast Asian compounds. National fraud strategies provide country-level response frameworks,[76] yet forced scamming requires a co-ordinated international response. The convergence of victim-origin countries, perpetrator hubs, and transit zones across the OSCE region suggests that scam centre operations represent an urgent and evolving threat to OSCE security, economy, and human protection.

Gender is embedded in the operational model. Sexual exploitation indicators appear in 12 per cent of the curated dataset, predominantly associated with iGaming roles. Female victims are subjected to dual exploitation: forced scamming and systematic sexual abuse and trafficking for sexual exploitation. The rise in online sexual exploitation investigations across OSCE participating States (from 9 to 1, 665 between 2021 and 2025) correlates with reported scam centre expansion in a manner that warrants further investigation, suggesting that law enforcement has not yet achieved sufficient victim identification or perpetrator disruption capacity.

This assessment is not hypothetical. It is grounded in OSINT from 82 coded recruitment advertisements, analysis of 750 unique Telegram messages from dedicated recruitment channels, survivor testimony from trafficking victims, and triangulation with national reporting from multiple jurisdictions. The indicator taxonomy developed in this report – convergence-based rather than single-marker driven – reflects the operational reality that scam centre recruitment is engineered to blend into legitimate labour-mobility infrastructure until the moment of movement or onboarding.

The scale of detected trafficking across OSCE participating States is substantial. OSCE survey reporting indicates that 102,000 trafficking victims were recorded across OSCE participating States between 2021 and 2024.[77] The emerging evidence suggests that forced scamming represents a growing proportion of this total.

The indicators identified in this assessment warrant a co-ordinated preventive response by OSCE participating States and other international stakeholders. Law enforcement agencies across multiple jurisdictions have documented elements of this phenomenon, and the early-warning indicators are visible across platforms and geographic zones. A timely and co-ordinated approach to prevention, victim protection, and operational disruption could help reverse the current trajectory before entrenched infrastructure takes root within the OSCE region.

The OSCE, as an institution committed to human security and human rights, has a mandate and responsibility to address this emerging threat. The Consolidated Indicator Taxonomy and recommendations in this assessment provide the evidentiary foundation and operational roadmap for that response. The OSCE Conference of the Alliance against Trafficking in Persons (2026) provided an opportunity for structured dialogue on this emerging threat.[78] Co-ordinated and timely action by OSCE participating States and institutional partners is essential to prevent this crime modality from multiplying across the OSCE region threatening security, economies, and human safety and dignity of its participating States.

The OSCE, as an institution committed to human security and human rights, has a mandate and responsibility to address this emerging threat.

References

1 UNODC, "Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia" (April 2025) Inflection_Point_2025.pdf;
International Scammers Steal Over $1 Trillion in 12 Months in Global State of Scams Report 2024 | Global Anti Scam Alliance

2 OHCHR, "UN report details grave abuses against those trafficked into scam centres" (February 2026). https://www.ohchr.org/en/press-releases/2026/02/un-report-details-grave-abuses-against-those-trafficked-scam-centres

3 UNODC, "Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud" (October 2024). https://www.unodc.org/roseap/en/2024/10/cyberfraud-industry-expands-southeast-asia/story.html

4 INTERPOL, "Global Financial Fraud Threat Assessment", (March 2026). https://www.interpol.int/en/News-and-Events/News/2026/INTERPOL-report-warns-of-increasingly-sophisticated-global-financial-fraud-threat

5 UNODC, "Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia" (April 2025).

6 Croatia - United States Department of State

7 Croatia - United States Department of State

8 UNODC, "Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia" (April 2025) Inflection_Point_2025.pdf

9 UNODC, "Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia" (April 2025) Inflection_Point_2025.pdfInflection_Point_2025.pdf

10 Kazakhstan - United States Department of State

11 Citizens of Uzbekistan, Kazakhstan, and Kyrgyzstan rescued from human trafficking in Myanmar

12 Strengthening Mongolia's online investigations capacity: RSO and IOM lead counter-trafficking workshop in Ulaanbaatar - The Regional Support Office of the Bali Process

13 PUBLIC SIT REP and ICAT Webinar Series #3 Unmasking the digital threat Trafficking in persons, cyber and cyber enabled - YouTube

14 UNODC, "Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia" (April 2025) Inflection_Point_2025.pdf

15 PUBLIC SIT REP and ICAT Webinar Series #3 Unmasking the digital threat Trafficking in persons, cyber and cyber enabled - YouTube

16 Tajikistan - United States Department of State

17 PUBLIC SIT REP and ICAT Webinar Series #3 Unmasking the digital threat Trafficking in persons, cyber and cyber enabled - YouTube

18 UNODC, "Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia" (April 2025) Inflection_Point_2025.pdfInflection_Point_2025.pdf

19 Warsaw police uncover criminal network involved in human trafficking and narcotics - English Section

20 PUBLIC SIT REP and ICAT Webinar Series #3 Unmasking the digital threat Trafficking in persons, cyber and cyber enabled - YouTube

21 UNODC, "Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia" (April 2025) Inflection_Point_2025.pdf

22 Uzbekistan - United States Department of State

23 Austria - United States Department of State

24 Belarus - United States Department of State

25 Croatia - United States Department of State

26 Reports from experts with lived experience confirm that victims have been trafficked from compounds in the UAE to Georgia.

27 Eight suspected of human trafficking and fraud; UP: The largest chain in the Balkans has been discontinued

28 Извештаи – ЈАВНО ОБВИНИТЕЛСТВО НА РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА

29 Warsaw police uncover criminal network involved in human trafficking and narcotics - English Section

30 US Department of State, "Imposing Sanctions on Online Scam Centers in Southeast Asia" (September 2025). https://www.state.gov/releases/office-of-the-spokesperson/2025/09/imposing-sanctions-on-online-scam-centers-in-southeast-asia

31 UK and US take joint action to disrupt major online fraud network - GOV.UK

32 UK crackdown on vile scam centres steps up with sanctions on illicit crypto network - GOV.UK

33 U.S. Embassy Jakarta and Indonesian National Police Join Global Coalition to Disrupt Online Scam Syndicates - U.S. Embassy & Consulates in Indonesia

34 OSCE, "24th Conference of the Alliance against Trafficking in Persons" (2025). https://www.osce.org/event/alliance24 and 26th Conference of the Alliance against Trafficking in Persons (2026)

35 OHCHR, "A matter of survival: The human cost of cyber scam operations" (February 2026). https://www.ohchr.org/en/stories/2026/02/matter-survival-human-cost-cyber-scam-operations-south-east-asia

36 OCCRP, "Scam Empire: Inside a Merciless International Investment Scam" (March 2025). https://www.occrp.org/en/project/scam-empire

37 INTERPOL releases new information on globalization of scam centres

38 https://www.polskieradio.pl/395/7789/Artykul/3640035%2Cwarsaw-police-uncover-criminal-network-involved-in-human-trafficking-and-narcotics

39 Cut off international human trafficking channel from Taiwan – PROSECUTOR'S OFFICE OF THE REPUBLIC OF NORTH MACEDONIA; Further details from this case have been provided to the OSCE by the Prosecutor's Office

40 https://rm.coe.int/evaluation-report-on-the-implementation-of-the-council-of-europe-conve/1680a2aefc

41 Eight suspected of human trafficking and fraud; UP: The largest chain in the Balkans has been discontinued

42 UNODC, "Trapped in scam crime: new campaign exposes human cost behind fake job offers" (December 2025). https://www.unodc.org/roseap/en/2025/12/trapped-in-scam-crime/story.html

43 The 33 indicators are organised across five analytical categories: (A) Recruitment Appeal and Targeting (13 indicators, including high salary with minimal qualifications, vague role description, occupational clustering around fraud-adjacent roles, relocation and housing, female-only or appearance-based targeting); (B) Channel and Process (6 indicators, including messaging-app routing, copy-paste or templated language, weak corporate identity); (C) Credibility Manufacturing (4 indicators, including geographic mismatch between recruiter and job location, minimal recruiter profile); (D) Facilitation and Movement (4 indicators, including document handling emphasis, border crossing assistance, debt bondage framing); (E) Exploitation Risk and Safeguarding (6 indicators, including iGaming/casino language, forex/retention/conversion roles, isolation risk, sexual exploitation indicators). The full taxonomy is presented in Section 7.

44 Nature, "'Simple job, high salary': unveiling the complexity of scam-forced criminality in Southeast Asia" (2025). https://www.nature.com/articles/s41599-025-05605-1

45 UNODC, "Cyberfraud in the Mekong reaches inflection point" (April 2025). https://www.unodc.org/unodc/frontpage/2025/April/cyberfraud-in-the-mekong-reaches-inflection-point--unodc-reveals.html

46 Amnesty International, "Cambodia: Government allows slavery and torture to flourish inside hellish scamming compounds" (June 2025). https://www.amnesty.org/en/latest-news/2025/06/cambodia-government-allows-slavery-torture-flourish-inside-scamming-compounds/

47 OSCE, "New Frontiers: The Use of Generative Artificial Intelligence to Facilitate Trafficking" (2024). https://www.osce.org/files/f/documents/7/d/579715.pdf

48 US Secret Service, "Cryptocurrency Scams - Pig Butchering" (January 2025). https://www.secretservice.gov/sites/default/files/reports/2025-01/Public-Alerts-2025-Cryptocurrency-Scams-Pig-Butchering.pdf

49 Chainalysis, 2026 Crypto Crime Report: Scams

50 ScamWatchHQ, "Pig Butchering: The $12.4 Billion Romance-Crypto Scam Epidemic" (2025). https://www.scamwatchhq.com/pig-butchering-the-12-4-billion-romance-crypto-scam-epidemic-breaking-hearts-and-bank-accounts/

51 Cut off international human trafficking channel from Taiwan – PROSECUTOR'S OFFICE OF THE REPUBLIC OF NORTH MACEDONIA; Further details from this case have been provided to the OSCE by the Prosecutor's Office

52 OSCE lived experience consultant and survivor testimonies

53 Following the money 2.0 - A collaborative approach to human trafficking investigations involving virtual assets | Office of the Special Representative and Co-ordinator for Combating Trafficking in Human Beings

54 OSCE lived experience consultant and survivor testimonies

55 INTERPOL releases new information on globalization of scam centres

56 A "wicked problem" - Seeking human rights-based solutions to trafficking into cyber-scam operations in South-East Asia | OHCHR

57 USIP, "Transnational Crime in Southeast Asia" (May 2024). https://www.usip.org/sites/default/files/2024-05/ssg_transnational-crime-southeast-asia.pdf

58 CNN, "2025 was a terrible year for the 'Four Families' accused of running global cyber scam operations" (January 2026). https://www.cnn.com/2026/01/04/asia/china-myanmar-scam-crime-families-intl-hnk-dst

59 CSIS, "Cyber Scamming Goes Global: Sourcing Forced Labor for Fraud Factories" (2025). https://www.csis.org/analysis/cyber-scamming-goes-global-sourcing-forced-labor-fraud-factories

60 Council of Europe, GRETA, "Report on labour trafficking in North Macedonia" (2024).

61 US Department of State, "2025 Trafficking in Persons Report: Serbia" (2025). https://www.state.gov/reports/2025-trafficking-in-persons-report/serbia/

62 IOM, Combatting Human Trafficking in the Digital Era: Western Balkans (2025). https://migrantprotection.iom.int/en/spotlight/articles/initiative/combatting-human-trafficking-digital-era-innovative-approaches-bosnia

63 Times of Central Asia, "Kazakhstan Blocked Nearly 85 Million Fraudulent Phone Calls in 2025" (2025). https://timesca.com/kazakhstan-blocks-nearly-85-million-fraudulent-phone-calls-in-2025/

64 UNODC, Global Report on Trafficking in Persons 2024 (December 2024). https://www.unodc.org/documents/data-and-analysis/glotip/2024/GLOTIP2024_BOOK.pdf

65 report-a-wicked-problem.pdf

66 https://www.interpol.int/en/content/download/23175/file/INTERPOL%20Crime%20Trend%20Update%20-%20Human%20trafficking-fueled%20scam%20centres.pdf?inLanguage=eng-GB&version=1

67 Warsaw police uncover criminal network involved in human trafficking and narcotics - English Section

68 https://rm.coe.int/evaluation-report-on-the-implementation-of-the-council-of-europe-conve/1680a2aefc

69 Croatia - United States Department of State

70 OSCE, Survey 2026, https://cthb.osce.org/sites/default/files/documents/publications/2026/03/SurveyReport_2026_Screen_260318.good_.pdf page 11.

71 UNODC Global Report on Trafficking in Persons (December 2024). https://www.unodc.org/unodc/en/press/releases/2024/December/unodc-global-human-trafficking-report.html

72 OHCHR, "UN experts urge immediate human rights-based action to tackle forced criminality" (May 2025). https://www.ohchr.org/en/press-releases/2025/05/un-experts-urge-immediate-human-rights-based-action-tackle-forced

73 Survivor and Trauma-Informed Model Standard Operating Procedures (SOPs) | Office of the Special Representative and Co-ordinator for Combating Trafficking in Human Beings

74 Serbian Times, "Belgrade companies behind international fraud: Call-centers stole 250 million euros" (2024). https://serbiantimes.info/en/belgrade-companies-behind-international-fraud-call-centers-stole-250-million-euros/

75 UK NFIB, Romance fraud statistics 2024/25. Reported in: https://www.infosecurity-magazine.com/news/brits-lose-106m-to-romance-fraud/

76 UK Government, "Fraud Strategy: Stopping Scams and Protecting the Public" (2023). https://www.gov.uk/government/publications/fraud-strategy

77 OSCE, "New OSCE Survey Report: Rising identification of human trafficking victims" (March 2026). https://cthb.osce.org/cthb/662914

78 OSCE, "24th Conference of the Alliance against Trafficking in Persons" (2025). https://www.osce.org/event/alliance24 and 26th Conference of the Alliance against Trafficking in Persons (2026)

The Organization for Security and Co-operation in Europe works for stability, prosperity and democracy in 57 States through political dialogue about shared values and through practical work that makes a lasting difference.

Office of the Special Representative and
Co-ordinator for Combating Trafficking
in Human Beings
Wallnerstr. 6, 1010 Vienna, Austria
Tel: + 43 1 51436 6664
Fax: + 43 1 51436 6299
email: info-cthb@osce.org
www.osce.org/cthb

OSCE Organization for Security and Co-operation in Europe