Security Intelligence Terrorism Journal (SITJ), Vol. 03 No. 01 (2026), pp. 22-26
Research Article
doi: https://doi.org/10.70710/sitj.v3i1.85

Assessing the Threat of Online Scamming–Based Human Trafficking: An Analysis of Transnational Criminal Capacity and National Security Implications in the Myawaddy Case

A.P. Santoso[1,a,*]

[1]Sekolah Tinggi Intelijen Negara, Bogor, Indonesia
[a]a.p.santoso38@gmail.com
*Corresponding author

Article Info
Received: 9-Jan-2026
Revised: 10-Jan-2026
Accepted: 10-Jan-2026

Keywords
Human Trafficking; National Security; Online Scamming; Threat Analysis; Transnational Crime; Vulnerability Assessment

Abstract
Online scamming–based human trafficking has emerged as a complex transnational phenomenon that combines digital deception with coercive exploitation. This research analyzes the threat posed by human trafficking syndicates operating in Myawaddy, Myanmar, by examining their operational intent, capacity, and the vulnerabilities that enable sustained victimization. This study employs a qualitative methodology, drawing data from semi-structured interviews with repatriated Indonesian victims, institutional stakeholders involved in protection and law enforcement, and subject matter experts, complemented by secondary data from international organization reports and scholarly literature. The analysis is framed using Hank Prunckun's threat assessment and vulnerability assessment framework. The findings indicate that the threat level is high, driven by persistent criminal intent and advanced transnational operational capability, while vulnerabilities remain acute due to economic pressure, limited digital safeguards, normalized online recruitment practices, and gaps in cross-border oversight. From a national security perspective, this threat is non-traditional and multidimensional, affecting human security, political and diplomatic capacity, social resilience, economic stability, and cybersecurity. The study concludes that addressing this threat requires an integrated security response that combines disruption of transnational scam operations with structural efforts to reduce domestic vulnerabilities that sustain exposure to exploitation.

1. Introduction

Human trafficking constitutes a serious violation of human rights and a persistent challenge to state security. Beyond individual victimization, trafficking undermines social stability, expands transnational criminal networks, and weakens the capacity of states to protect their citizens. It is generally understood as a process involving recruitment, transportation, transfer, harboring, or receipt of persons through coercion, deception, abuse of power, or exploitation of vulnerability for the purpose of exploitation (UNODC, 2023; Barner et al., 2014). These processes often result in sustained physical and psychological harm and generate broader implications for public order and governance (Fabbri et al., 2023; Stöckl et al., 2021).

The expansion of digital technologies has significantly transformed the operational landscape of human trafficking. Recruitment and control increasingly occur through online platforms, messaging applications, and social media, enabling perpetrators to reach wider target populations while minimizing

physical exposure and detection (Sweileh, 2018; IOM, 2021). Within this transformation, online scamming has become a central operational instrument, functioning both as a recruitment mechanism and as a means of exploitation through digitally mediated fraud activities (Dynel & Ross, 2021; Ebot et al., 2024).

In the context of trafficking, online scamming frequently operates as a gateway to forced criminality. Victims are deceived through fraudulent employment narratives and subsequently coerced into participating in online fraud operations under conditions of confinement, threat, and violence (UNODC, 2023; Hung, 2023). This dynamic complicates legal and protection frameworks by obscuring the boundary between victimhood and criminal liability.

Southeast Asia has emerged as a focal region for online scamming–based human trafficking, particularly in border areas characterized by weak governance and fragmented authority. Among these locations, Myawaddy in Myanmar has gained prominence as an operational hub hosting closed compounds where victims are confined and integrated into large-scale scam operations targeting global victims (CSIS, 2023; Ramaj, 2023). The persistence of these operations reflects the surrounding security environment, which limits effective law enforcement intervention.

Indonesia has been significantly affected as a country of origin for victims. Indonesian citizens have repeatedly been recruited through online employment schemes and subjected to prolonged exploitation abroad. The consequences extend beyond the period of confinement, as survivors often face psychological trauma, social stigma, and barriers to reintegration after repatriation (Idemudia et al., 2021; Chambers et al., 2024). These patterns indicate that online scamming–based human trafficking should be examined not only as a criminal justice issue but also as a national security concern.

While existing studies have examined online scams, trafficking impacts, and victim recovery, fewer have integrated structured threat and vulnerability analysis with an assessment of national security implications in a conflict-adjacent border context such as Myawaddy. Therefore, this research addresses the following question: How can the threat posed by online scamming–based human trafficking syndicates operating in Myawaddy be analyzed from a national security perspective? To answer this question, the study applies a structured threat and vulnerability framework and interprets the findings within a non-traditional security perspective.

2. Literature Review

2.1. Online Scamming-Based Human Trafficking

Online scamming–based human trafficking represents an evolution of traditional trafficking practices in response to digitalization. Traffickers increasingly exploit online platforms to recruit, manipulate, and control victims through professionalized digital narratives that normalize participation (UNODC, 2023; Wang & Zhou, 2023). Once recruited, victims may be transported across borders and confined in controlled environments where they are forced to engage in online fraud activities, reflecting trafficking for forced criminality (Hung, 2023; IOM, 2017).

2.2. Threat and Vulnerability Analysis

Threat analysis focuses on an actor's intent and capability to cause harm. Hank Prunckun conceptualizes threat as the interaction between desire and expectation, combined with knowledge and resources, while vulnerability is shaped by attractiveness, ease of attack, and impact (Prunckun, 2019). This framework allows for structured assessment of both perpetrator capacity and target exposure, particularly in complex transnational contexts.

2.3. National Security and Non-Traditional Threats

Contemporary security studies emphasize that national security extends beyond military threats to include non-traditional challenges affecting human security, political stability, economic resilience, and information integrity (Buzan, 1983; Wantannas, 2010). Cyber-enabled transnational crimes that

systematically harm citizens and exploit digital space can therefore be understood as security threats requiring multidimensional responses.

3. Method

This study employs a qualitative exploratory research design to capture the complex and socially constructed nature of online scamming–based human trafficking. Primary data were collected through semi-structured interviews with repatriated Indonesian victims, institutional stakeholders involved in protection and law enforcement, and experts in national security and cybercrime. Secondary data were obtained from academic literature, official documents, and reports published by international organizations. Data analysis followed a process of thematic reduction and interpretation, supported by Hank Prunckun's threat and vulnerability assessment framework to structure evaluation.

4. Results

The analysis of interview data demonstrates that the threat posed by online scamming–based human trafficking in Myawaddy is neither incidental nor episodic, but systemic and persistent. Rather than functioning as isolated criminal acts, exploitation occurs within an organized structure that enables sustained recruitment, control, and forced participation in digital fraud activities. This section presents the findings through a structured discussion that examines the operational characteristics of the syndicate, the vulnerabilities that facilitate exploitation, the impacts on victims and state capacity, and the broader implications for national security.

4.1. Structure and Persistence of Exploitation

Online scamming–based human trafficking in Myawaddy operates as an organized and continuous system of exploitation. Recruitment, confinement, and forced labor are not separate phases, but interconnected components of a single operational process. Victims are recruited through digital channels, transported across borders, and incorporated into controlled environments where exploitation can be sustained over long periods. Myawaddy functions not merely as a geographic location, but as a strategic operational space. The area enables concealment, restricted access, and limited external oversight, allowing syndicates to maintain closed systems of control. Within these environments, victims experience strict regulation of movement, communication, and daily routines. Such controls reduce opportunities for escape and reporting, reinforcing the persistence of exploitation.

The structured nature of these operations indicates that exploitation is institutionalized rather than improvised. The continuity of recruitment and exploitation suggests that the syndicate has normalized coercive practices as part of its operational model. As a result, the threat is embedded in both organizational arrangements and spatial conditions, making it resilient to short-term disruptions.

4.2. Threat Characteristics

From a threat assessment perspective, the syndicate demonstrates a strong and sustained intent to continue recruitment and generate financial returns through online scamming activities. Recruitment is repeatedly conducted using narratives of legitimate overseas employment, indicating deliberate planning and consistency rather than opportunistic targeting. The persistence of these practices reflects a calculated assessment that potential risks remain manageable.

Operational capability significantly amplifies this threat. The syndicate exhibits organizational knowledge in managing cross-border movement, enforcing confinement, and integrating victims into online scamming operations. Victims are assigned specific roles and monitored to ensure compliance, indicating the presence of internal coordination and supervision mechanisms. The operation resembles an institutionalized production system rather than ad hoc coercion. Financial resources, coercive enforcement, and digital infrastructure allow the syndicate to sustain operations and adapt when conditions change. Together, strong intent and advanced capability demonstrate that the syndicate possesses both the motivation and the means to maintain exploitation over time.

4.3. Vulnerability of Targets and Ease of Exploitation

The vulnerability assessment indicates that the target population remains highly exposed to exploitation. Economic pressure and aspirations for overseas employment reduce resistance to recruitment narratives, particularly when offers are presented through professional and normalized digital formats. Limited capacity to verify information online further weakens individual defenses against deception. Ease of exploitation is reinforced by structural conditions that favor perpetrators. Recruitment through digital platforms requires minimal resources and can be conducted repeatedly with limited risk of disruption. Weak oversight of online recruitment channels and cross-border mobility creates an environment in which syndicates can operate with relative freedom.

Psychological and social barriers further intensify vulnerability. Fear of stigma, legal consequences, and misclassification as perpetrators discourages victims from reporting exploitation. These conditions allow recruitment and exploitation to be reproduced efficiently, indicating that vulnerability is systemic rather than incidental.

4.4. Impact on Victims and State Capacity

The impact of online scamming–based human trafficking extends beyond the period of confinement and forced labor. Victims experience physical and psychological harm that persists after repatriation, affecting their ability to reintegrate socially and economically. Trauma, fear, and social isolation often continue long after victims leave the site of exploitation. At the state level, repeated cases of exploitation generate cumulative burdens related to protection, repatriation, recovery, and reintegration. These processes require sustained coordination and allocation of resources across institutions. Over time, such demands place pressure on governance capacity and social support systems.

The impact is therefore both individual and structural. While harm is directly experienced by victims, its consequences extend to the state's ability to manage protection responsibilities and maintain social resilience. This reinforces the classification of online scamming–based human trafficking as an issue with broader security relevance.

4.5. National Security Implications

From a national security perspective, online scamming–based human trafficking in Myawaddy constitutes a non-traditional and multidimensional threat. It directly undermines human security by exposing citizens to coercion, violence, and exploitation beyond effective state protection. These harms challenge the fundamental responsibility of the state to safeguard its population.

The threat also affects political and diplomatic capacity by highlighting limitations in cross-border protection and enforcement. Social resilience is strained through trauma, stigma, and marginalization among survivors, while economic resources are burdened by repeated response and recovery efforts. At the same time, the reliance on digital platforms places cybersecurity and information governance at the core of the threat. These dimensions interact rather than operate independently. The Myawaddy case illustrates how cyber-enabled transnational exploitation can evolve into a complex security challenge that exceeds conventional criminal justice frameworks and requires integrated, multidimensional responses.

5. Conclusion

This study concludes that online scamming–based human trafficking in Myawaddy constitutes a sustained and high-level threat to Indonesia's national security. The threat is driven by persistent criminal intent and reinforced by advanced transnational operational capability that integrates digital recruitment, cross-border movement, coercive confinement, and organized scam production. Rather than functioning as isolated criminal incidents, exploitation operates as an institutionalized system that is able to reproduce itself over time and adapt to external pressure.

The analysis also demonstrates that the severity of this threat is amplified by acute structural vulnerabilities on the target side. Economic pressure, limited digital safeguards, and the normalization of

online recruitment practices create favorable conditions for repeated victimization, while gaps in cross-border oversight reduce the effectiveness of prevention and early intervention. These vulnerabilities are not incidental, but systemic, allowing exploitation to persist even when individual cases are addressed through rescue and repatriation.

From a national security perspective, the implications extend beyond individual harm to affect broader state capacity and social resilience. Online scamming–based human trafficking undermines human security, burdens protection and recovery mechanisms, and exposes weaknesses in digital governance and cross-border coordination. Addressing this threat therefore requires an integrated security response that combines disruption of transnational criminal operations with sustained efforts to reduce domestic vulnerability and strengthen digital and institutional resilience.

References

Abroshan, H., Devos, J., Poels, G., & Laermans, E. (2021). COVID-19 and phishing: Effects of human emotions, behavior, and demographics on the success of phishing attempts during the pandemic. *IEEE Access, 9*, 121916–121929.

Barner, J. R., Okech, D., & Camp, M. A. (2014). Socio-economic inequality, human trafficking, and the global slave trade. *Societies, 4*(2), 148–160.

Buzan, B. (1983). *People, states and fear: The national security problem in international relations*. Wheatsheaf.

Center for Strategic and International Studies. (2023). *Cyber scamming goes global: Unveiling Southeast Asia's high-tech fraud factories*. CSIS.

Chambers, R., Gibson, M., Chaffin, S., Takagi, T., Nguyen, N., & Mears-Clark, T. (2024). Trauma-coerced attachment and complex PTSD: Informed care for survivors of human trafficking. *Journal of Human Trafficking, 10*(1), 41–50.

Dynel, M., & Ross, A. S. (2021). You don't fool me: On scams, scambaiting, deception, and epistemological ambiguity. *Social Media + Society, 7*(3).

Ebot, A. C., Siponen, M., & Topalli, V. (2024). Towards a cyber-contextual transmission model for online scamming. *European Journal of Information Systems, 33*(4), 571–596.

Fabbri, C., Stöckl, H., Jones, K., Cook, H., Galez-Davis, C., Grant, N., & Zimmerman, C. (2023). Labor recruitment and human trafficking: Analysis of a global trafficking survivor database. *International Migration Review*.

Hung, A. H. C. (2023). Tortured between two hells: Collective social normalization of forced criminality. *Journal of Human Trafficking, 9*(3), 363–375.

Idemudia, U., Okoli, N., Goitom, M., & Bawa, S. (2021). Life after trafficking: Reintegration experiences of survivors. *International Journal of Migration, Health and Social Care, 17*(4), 449–463.

International Organization for Migration. (2017). *Global estimates of modern slavery*. IOM.

International Organization for Migration. (2021). *World migration report 2022*. IOM.

Prunckun, H. (2019). *Methods of inquiry for intelligence analysis* (3rd ed.). Rowman & Littlefield.

Ramaj, K. (2023). The aftermath of human trafficking: Return and reintegration challenges. *Journal of Human Trafficking, 9*(3), 408–429.

Sweileh, W. M. (2018). Research trends on human trafficking: A bibliometric analysis. *Globalization and Health, 14*(1).

United Nations Office on Drugs and Crime. (2023). *Online scam operations in Southeast Asia*. UNODC.

Wang, F., & Zhou, X. (2023). Persuasive schemes for financial exploitation in online romance scams: An anatomy of Sha Zhu Pan. *Victims & Offenders, 18*(5), 915–942.

Wantannas. (2010). *Keamanan nasional: Sebuah konsep dan sistem keamanan bagi bangsa Indonesia*. Dewan Ketahanan Nasional Republik Indonesia.