



NEW FRONTIERS: THE USE OF GENERATIVE **ARTIFICIAL INTELLIGENCE** TO FACILITATE **TRAFFICKING IN PERSONS**



POLICY BRIEF NOVEMBER 2024



The Regional Support Office of the Bali Process (RSO) extends its gratitude to the Australian Government Department of Home Affairs, which has provided primary funding for the RSO since its establishment in 2012, and to the International Organization for Migration (IOM), which hosts the RSO in Bangkok, Thailand and supports its administration. The RSO thanks the Royal Thai Government for its ongoing support for the RSO to operate in Bangkok, Thailand.

The work of the RSO would not be possible without the support and commitment of Bali Process members, each of whom contribute time, resources, and personnel to work with the RSO.



The current Policy Brief was developed within the Organization for Security and Co-operation in Europe (OSCE)'s extra-budgetary project '*Responding to technology-facilitated trafficking in human beings*', implemented by the Office of the OSCE Special Representative and Co-ordinator for Combating Trafficking in Human Beings (OSR/CTHB). We extend our gratitude to the governments of Austria, Cyprus, France, Malta, Norway, the United Kingdom and the United States for generously funding the mentioned extra-budgetary project.

The OSR/CTHB highly appreciates the contributions from experts and practitioners from the OSCE participating States, especially from the Netherlands, Ukraine and the United States, in jointly navigating how artificial intelligence can impact the crime of trafficking in human beings, both from a point of misuse and positive use.

Published by the OSCE Office of the Special Representative and Co-ordinator for Combating Trafficking in Human Beings (OSR/CTHB) and the Regional Support Office of the Bali Process (RSO)

© 2024 OSCE/OSR CTHB and RSO ISBN 978-3-903128-81-1 (OSCE)

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, <u>https://www.osce.org/cthb</u>

Regional Support Office of the Bali Process (RSO) 27th Floor Rajanakarn Building, 3 South Sathorn Road, Sathorn, Bangkok 10120, Thailand, Tel: +66 2 343 9477 Fax. +66 2 676 7337 Email: info@rso.baliprocess.net, <u>www.rso.baliprocess.net</u>

Cite as: Policy Brief. New Frontiers: The Use of Generative Artificial Intelligence to Facilitate Trafficking in Persons (Bangkok/Vienna, 2024)

All rights reserved. The contents of this publication may be freely used and copied for educational and other non-commercial purposes, provided that any such reproduction is accompanied by an acknowledgement of the OSCE/Office of the Special Representative and Co-ordinator for Combating Trafficking in Human Beings and of the Regional Support Office of the Bali Process as the source.

This report was produced by the OSCE Office of the Special Representative and Co-ordinator for Combating Trafficking in Human Beings and the Regional Support Office of the Bali Process.

Design by Wendy Htet and Sebastian Higginson

Lead author: Phil Bennett, Counter-trafficking Technology Consultant Contributing authors: Radu Cucos, OSCE, Ryan Winch, RSO

The authors would like to express their gratitude to the numerous experts, practitioners, and stakeholders who provided valuable insights and feedback during the development of this report. Reviewers of this report included Lynn Dudenhoefer, Evan Jones, Lindsay Erjavic, Martha Stickings, and Zein Maulana.

TABLE OF CONTENTS

Foreword	4
Key Insights	6
Recommendations	7
Trafficking in Persons	9
Rise of Generative AI	10
The Use of Generative AI in Transnational Crime	13
Proactive Measures and Interventions	22
Conclusion	25
Glossary	26
Endnotes	27

FOREWORD

The Organization for Security and Co-operation in Europe (OSCE) and the Regional Support Office of the Bali Process (RSO) have jointly developed this brief on the emerging nexus of artificial intelligence (AI), trafficking in persons (TIP)* and transnational crime. This collaboration brings together two regional anti-trafficking organisations in the fight against transnational crime: the OSCE, the world's largest regional security organisation, working to ensure stability, peace, and democracy for over one billion people across North America, Europe, and Asia; and the RSO, supporting a forum of 49 members primarily from across the Asia-Pacific dedicated to countering people smuggling, trafficking in persons, and related transnational crime. Together, these organisations' reach extends over four continents and 98 countries.

Our collaborative effort to develop this report underscores a fundamental reality: trafficking in persons is a global challenge that transcends borders, and the advent of AI technologies has the potential to amplify both its reach and complexity. As AI continues to reshape our world, its impacts—both positive and negative—will be felt on a truly global scale. It is precisely this global nature of both trafficking and AI that necessitates coordinated, regional and international responses.

The partnership between the OSCE and the RSO in producing this brief exemplifies the kind of crossregional collaboration that will be essential in supporting effective preparation and response to AI-facilitated trafficking. By combining our diverse perspectives, expertise, skills and resources, we can develop more comprehensive strategies and solutions that address the nuances of this evolving threat across different geographical and cultural contexts, while also delivering these insights to a global audience.

The intersection of AI and transnational crime, particularly its application in human trafficking, represents an emerging and critically important area of study. This brief has been developed with a clear objective: to equip policymakers, law enforcement agencies, and the technology sector with the insights needed to anticipate and pre-emptively address the potential implications of AI on trafficking in persons.

While we respond to the early instances of the use of AI by transnational criminal organisations, such as within Southeast Asia's cyber-scam centres, a more systemic approach is required. The potential for transnational criminal organisations to significantly expand their operations using AI technologies is considerable, and with it comes the risk of exponentially increasing harm to individuals and communities worldwide.

It is imperative that we act now, before the most severe impacts of AI-enabled trafficking are realised. We have a unique time-limited opportunity—and indeed, a responsibility—to plan, train, and develop policies that can mitigate these emerging threats. This report aims to concretise this discussion by outlining specific scenarios where AI and trafficking could intersect, and to initiate a dialogue on how we can prepare and respond effectively.

This document is not intended to be definitive, but rather to serve as a foundation for a broader, ongoing discussion. The ideas presented here are initial steps, and it will require innovative thinking, adequate resourcing, and sustained engagement from all sectors to build upon them effectively.

As we explore this complex issue, we must acknowledge that while the challenge before us is formidable, it is not insurmountable. By fostering collaboration between technology experts, law enforcement,

^{*} Note: The term 'trafficking in persons' used throughout this Policy Brief is equivalent to the term 'trafficking in human beings' used by the OSCE as reflected in the OSCE anti-trafficking commitments. Throughout this brief the terms 'human trafficking' and 'trafficking in persons' are used interchangeably. For more information, refer to Page 9.

policymakers, and anti-trafficking organisations across regions and continents, we can work towards developing robust strategies to counter the misuse of AI in trafficking in persons.

The future of this endeavour is being shaped now, and it is important for all of us to ensure that emerging technologies become tools for prevention and protection, rather than exploitation. Let this report serve as a call to action, prompting us to implement proactive measures that safeguard human security in the age of artificial intelligence. The OSCE and RSO are committed to leading this initiative, but success will require the engagement and dedication of stakeholders across both the OSCE's and Bali Process' Membership, as well as more broadly across the globe. Together, we can establish a united front against the abuse of AI to facilitate trafficking in persons and create a safer, more just world for all.

Dr. Kari Johnstone

OSCE Special Representative and Co-ordinator for Combating Trafficking in Human Beings

David Scott

Hung.

Fuad Adriansyah

RSO Co-Manager (Australia)

RSO Co-Manager (Indonesia)

KEY INSIGHTS

Recent advancements in generative AI have achieved unprecedented levels of sophistication. AI systems are now adept at generating content that convincingly emulates human creativity, including the ability to craft complex personas that can transcend cultural and linguistic boundaries. It is likely that transnational criminal organisations will increasingly exploit this technology, making it more difficult and expensive for law enforcement to detect criminal activity and bring traffickers to justice.

So far there has been very little research undertaken into how human traffickers are utilising generative AI. Consequently, discussions about AI safety and governance have not sufficiently considered the risks of AI-enabled human trafficking, despite there being clear use-cases. Many of the mechanisms used by transnational criminal organisations to create scams and generate deepfake imagery are relevant to existing trafficking business models.

The recent advancements in generative AI pose the following risks to anti-trafficking efforts:

- 1. Transnational criminal organisations can use generative AI to engage with communities who were previously unaffected by trafficking. This is due to the technology's ability to bridge cultural and linguistic divides.
- 2. Recruitment using deception and coercion via digital platforms is likely to be the most common usage of generative AI by human traffickers.
- 3. It is unlikely that current AI safety and governance efforts alone will sufficiently combat human trafficking risks. This is because many of the scenarios, including recruitment and coercion, closely resemble innocuous conversations between people.
- 4. Relatively simple technology integrated with generative AI could be used to automate conversations and scale trafficking recruitment and coercion processes.
- 5. Many generative AI models are available with open-source licences and can be downloaded to computers free of charge. Advanced models can currently operate on high-end laptops. This could make it more difficult for technology companies and law enforcement to detect AI usage by transnational criminal organisations.

Over the next few years, we can expect further significant technical advancements in generative AI technologies. This will be largely driven by commercial investments. One dimension of change will be the increased sophistication and accuracy of AI models. Another dimension will be the advancements of AI automation and the development of open-source frameworks that reduce technical complexity. This will likely lead to sophisticated conversational AI personas which could be used to engage with potential victims. Finally, AI models are predicted to become cheaper and more accessible to transnational criminal organisations.

Today, a considerable proportion of human trafficking activities occur to some extent on digital platforms. It is difficult to identify these as having occurred because so many of the conversations that recruit and seek to establish control over victims closely resemble millions of other innocuous conversations. Therefore, generative Al—a technology designed to generate synthetic content at scale—poses a significant risk to anti-trafficking efforts. Swift action is now required to adapt anti-trafficking technology initiatives as well as legislative efforts to ensure transnational criminal organisations are not able to easily exploit generative Al.

RECOMMENDATIONS FOR ANTI-TRAFFICKING ORGANISATIONS

1. Organisations should upgrade data gathering and documentation processes to aid in tracking criminal abuses of Al. A societal response to the threat of Al will require more data on how Al is being used by traffickers. This will help develop new technological responses to tackle the issue and inform prevention efforts.

RECOMMENDATIONS FOR GOVERNMENTS

- 1. Consider promoting an approach requiring technology companies operating digital platforms to take steps to mitigate and remediate human trafficking on their platforms and across related supply chains. This would include identifying, managing, and preventing risks such as trafficking activities that could arise from end-users or businesses utilising their services.
- 2. Existing anti-trafficking and/or anti-forced labour legislation should be extended to require technology businesses—who host services with large numbers of users that enable user connections, conversations or advertisements—to report on efforts undertaken to tackle human trafficking taking place on their platforms. Commercial revenue should not be the only factor in determining which technology companies are subject to legislation.
- **3.** Encourage cross-sectoral collaborative initiatives designed to enable companies, governments and non-governmental organisations (NGO) to share knowledge about human trafficking and the use of AI in trafficking activities. These should be designed to enable companies to understand trafficking risks as part of their obligations under existing AI legislative risk-based approaches, e.g. the European Union Artificial Intelligence Act¹ and The Council of Europe Framework Convention on Artificial Intelligence and human rights, democracy and the rule of law.²
- 4. Update relevant processes and guidance to encourage technology companies to report and share with relevant state authorities all cases of misuse of AI related to suspected human trafficking cases.

RECOMMENDATIONS FOR THE TECHNOLOGY INDUSTRY

- 1. Learn and understand human trafficking typologies and processes. Update tertiary education technology safety courses, company product safety training, safety policies and partnership agreements, so that technologists in companies of all sizes understand the risks and are able to implement informed responses.
- 2. Build safety technologies to detect automated AI-enabled trafficking recruitment and control. Implement AI safety features to detect the creation of personas aligned to trafficking typologies, e.g. generating language containing threats and coercion. Extend the scope to include relatively rare languages and smaller-language communities.
- **3.** Join research programmes and cross-sectoral collaborative anti-trafficking initiatives to share knowledge about the rapidly changing human trafficking landscape. Encourage the involvement of individuals with lived experience and other anti-trafficking experts.

RECOMMENDATIONS FOR ANTI-TRAFFICKING RESEARCH ORGANISATIONS AND NON-GOVERNMENTAL ORGANISATIONS

- **1.** Begin research initiatives to monitor the use of Al by human traffickers. Identify communities most at risk and liaise and collaborate with technology companies to evaluate suitable responses.
- 2. Implement prevention programmes in vulnerable communities to raise awareness of the threat of sophisticated online recruitment techniques. Consider extending prevention programmes to communities and languages less affected by trafficking.
- **3.** Document instances of suspected criminal uses of generative AI in trafficking cases. This will help improve the overall understanding and inform a collective response.

TRAFFICKING IN PERSONS

Definitions from the Protocol to Prevent, Suppress and Punish Trafficking in Persons Especially Women and Children (Palermo Protocol)³:

Article 3

(a) "Trafficking in persons" shall mean the recruitment, transportation, transfer, harbouring or receipt of persons, by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation. Exploitation shall include, at a minimum, the exploitation of the prostitution of others or other forms of sexual exploitation, forced labour or services, slavery or practices similar to slavery, servitude or the removal of organs;

(c) The recruitment, transportation, transfer, harbouring or receipt of a child for the purpose of exploitation shall be considered "trafficking in persons" even if this does not involve any of the means set forth in subparagraph (a) of this article;

(d) "Child" shall mean any person under eighteen years of age.

This definition can be divided into three constituent elements⁴ :

The Act (What is done)

- Recruitment
- Transportation
- Transfer
- Harbouring
- Receipt of persons

The Means^{*} (How it is done)

- Threat or use of force
- Coercion
- Abduction
- Fraud
- Deception
- Abuse of power or vulnerability
- Giving payments or benefits
- Abduction

The Purpose (Why it is done)

For the purpose of exploitation, including:

- Exploiting the prostitution of others
- Sexual exploitation
- Forced labour
- Slavery
- Other similar practices and the removal of organs

*Only act and purpose apply to children

THE RISE OF GENERATIVE AI

A BRIEF HISTORY

In recent years we have witnessed staggering technological advances in Al. During 2020, OpenAl released a groundbreaking new Al model called GPT-3. It was the third version of an Al language model developed by the company which surprised experts around the world with its ability to generate textual content almost indistinguishable from content created by humans. In November 2022,

OpenAl released ChatGPT, a chatbot that used the same technology to provide a simple chat interface accessible to all. The release of ChatGPT attracted enormous media attention. Subsequently, the commercial investment in Al grew quickly and is currently expected to reach 200 billion USD globally by 2025.⁵

April 2024

Llama 3 LLM is released by Meta with exceptional language performance and efficiency. This model can be downloaded without charge to a computer and used locally.⁶

2022

The ChatGPT chatbot is released by OpenAl and goes viral around the world. ChatGPT breaks all records on the rate of user adoption of online platforms.⁷

2020

OpenAl release the GPT-3 large language model and astonishes the technology community with its scale and performance.⁸

2018

A new large language model called GPT is developed by OpenAl.⁹

2017

A landmark paper, '*Attention Is All You Need*' is submitted by scientists from Google introducing a new Al architecture called a 'transformer'. This innovation would later be adapted and improved to enable various types of generative Al.¹⁰

TODAY'S ECOSYSTEM

Generative AI is undoubtedly the area of AI that has attracted the most attention. This type of AI can generate content such as video, audio, computer code, imagery and text with humanlike characteristics. Since 2022 institutions have invested hundreds of billions of dollars into the development and implementation of new AI technologies and there are now hundreds of competing companies and generative AI models. Generative AI is expected to become a 1.3 trillion USD market by 2032.¹¹

Al models are now used routinely to analyse imagery and converse with users on external datasets and documents. This is called 'multimodal technology' and enables people and other computers to converse with Al models using a mixture of media, not just text. This will lead to the development of advanced consumer technology such as Al personal assistants, as well as becoming an extremely powerful tool for research and business.



Figure 1: A screenshot of a user asking ChatGPT 40 for information about an image. July 2024.

At the same time as the increasing commercial interest, there has also been a significant focus on strengthening AI ethics and safety from technology companies, governments and research establishments. The most common topics have included combatting bias and discrimination, fraud, data privacy issues, disinformation, generation of sexual abuse imagery, and the use of generative Al in health and defence systems.

To understand and respond to the potential threats of AI, it is important to understand how it can be utilised as well as the potential trajectory of change during the next few years.

AUTOMATION AND THE AI AGENT

Much of the impetus and direction of the sudden growth in AI investment has been driven by the promise of future commercial returns. Although chatbots are the most well-known incarnation of generative AI, there are many other ways in which this technology can be used.

Many of the most advanced generative AI models require specific computer hardware to operate efficiently and so some companies host the models and charge other companies to connect to them. This has resulted in thousands of corporations, governments and research institutions using the latest AI models to build new products, improve efficiency and conduct research.

The ability to cheaply connect new and existing technology to the latest generative AI models has resulted in the development of many new opensource technologies that can help utilise the models to tackle real-world problems. One of the biggest breakthroughs is the concept of an Al agent. An Al agent is relatively simple software which can run on any computer and interact with AI models as well as its wider environment. Typically, agent software is designed to operate semi-autonomously and with specific tasks in mind. The most well-known category of agents is chatbots. These can interact with a person and increasingly, internet search systems, so that users can access the latest information on the internet via the chatbot. However, they can also perform more sophisticated tasks, especially when integrated with other specialised AI agents. One example that has been developed is a multiagent system to conduct research on the internet to answer a research question. This example might use a hierarchy of agents with specialisms such as authoring, reviewing and creating charts.

Al agents and automation are now a topic of research in many companies and institutions.

FUTURE

It is extremely difficult to predict how the development of AI models and associated technologies will develop in the longer term. However, we can extrapolate recent events to deduce some of the likely technical changes that will hinder efforts to tackle human trafficking:

- Generative AI models will become more accurate, have improved reasoning capability, and exhibit more realistic human-level performance than ever before. Multilingual capabilities will improve significantly.
- 2. Multimodal technologies will become better at interpreting and generating different types of content such as images, video and audio. Generated media, including illegal material, will become more realistic.
- As computers become more powerful, more capable AI models will run on mobile devices and personal computers. More open-source models will become available.

- 4. Al agents will automate more complicated tasks, including those involving human interaction.¹²
- 5. As the AI technology efficiency improves, the usage costs will continue to reduce.

There is currently significant excitement surrounding Al; the underlying potential of this technology is undeniable, promising profound impacts across various aspects of human life.

However, history has shown that transnational criminal organisations will take advantage of new technology when it offers ways to evade detection and increase profits. The development of the world wide web allowed traffickers to advertise victims of commercial sexual exploitation on websites to reach more potential clients. When social media emerged, traffickers have used it to recruit victims online. New financial technology allowed traffickers to avoid the scrutiny of the banking system. Today, there are cases in which traffickers have no physical contact with victims or other participants. These technologies have increased the cost of investigating and prosecuting trafficking crimes. With the development of consumer AI we will witness a new stage of



Figure 2: Sample AI image generated by Gemini AI. October 9, 2024.

THE USE OF GENERATIVE AI IN TRANSNATIONAL CRIME

The recent advances in AI have been exploited by transnational criminal organisations in various ways and many of the methods are already well-documented. Examples include generating deepfake imagery,¹³ publishing disinformation using social media 'bots',¹⁴ financial fraud,¹⁵ and hacking.¹⁶ The use of this technology by human traffickers, however, is not as well understood, yet many of the mechanisms available to traffickers are identical or similar to known methods in related crimes.

Most conversations occurring on digital platforms for the purpose of trafficking in persons are difficult to identify because the nature of the conversations can be very similar to legitimate conversations. Therefore, as generative Al improves, it is likely to be used by traffickers looking to reach new communities, increase the scale of the crime through automation and avoid detection.

To understand the potential threat of Al in the context of human trafficking it is useful to examine the motivations of transnational criminal organisations to adopt technology. Technology is used by human traffickers to enhance existing transnational criminal activity by:

- 1. Reducing costs
- 2. Increasing revenue
- 3. Reducing the likelihood of being detected.

A significant proportion of trafficking activity is expected to continue to utilise the latest consumer technology and existing infrastructures, rather than building bespoke technologies. Although bespoke technology is often out of reach for many traffickers, transnational criminal organisations might use it to automate and create scale. By understanding these motivations we can examine the evolution in the use of generative AI technology.

Today, this technology is already being used to copy and paste translations for the purpose of deception.¹⁷ Sophisticated personas can be crafted by asking chatbots to perform a translation task that can include a cultural context. This will allow

transnational criminal organisations to extend their reach to previously unaffected communities. In many cases, the performance of generative AI language models exceeds commonly used online translator services, especially with less common languages.

Recruitment and control via fraud and coercion are the likely uses of this technology by human traffickers. Psychological coercion including grooming, shaming and deception are possible. A further threat is the automation of the discovery of victims using open-source AI agent technology which can be customised to traverse social networks and engage with potential victims.¹⁸ Multimodal AI can make the deception even more convincing using imagery, audio and video. Voice synthesis technology has been extended to allow individual voices to be cloned, allowing perpetrators to emulate a trusted person.¹⁹

In many trafficking typologies, transnational criminal organisations will seek to move a conversation with a potential victim from social media where the conversations are visible, to messaging apps that use end-to-end encryption.²⁰ It is likely that AI agent technology could be configured with the same goal. As AI models become more sophisticated, and automation becomes more accessible it is likely that online conversations involving human trafficking will become more difficult to identify.

The operating models used by transnational criminal organisations to access and operate technology solutions are likely to remain unchanged. Consumer AI technology will be used as-is, but more sophisticated automation solutions are more likely to be purchased using a similar approach to other technology-focused crimes. Illegal hardware and software platform offerings could be adapted and used to engage victims on digital platforms. This might include offerings similar to 'off the shelf' phone-farm infrastructures which are commonly used by transnational criminal organisations for various illicit activities, including click fraud (manipulating advertising revenue), phishing and spreading disinformation.²¹

AI AND TRAFFICKING INTO CYBER-SCAM CENTRES

Trafficking in persons for forced criminality has grown significantly in recent years, particularly in the context of forced scamming and cyber-scam centre operations.²² This criminal industry consists of transnational criminal organisations that recruit and traffic victims into scam compounds where, often under threat of violence, they are forced to scam people using social media and messaging apps. Many of these cyber-scam centres are based in Southeast Asia but are now spreading to other parts of the world.

Scams such as romance fraud and investment fraud rely on deception and building trust with scam victims, sometimes over many months. Typically, text and curated images are used to help sustain the deception, although more recently deepfake photos and video have also been used by some scammers.²³ Deepfake tools are quickly becoming more accessible to transnational criminal organisations and help to enhance the deception and enable the scam. As such groups continue to adopt these elements it is likely that it will increase profitability in the short-term and is therefore a driver of trafficking in persons.

Al is increasingly becoming a tool for the recruitment of trafficking victims into scam centres, while simultaneously altering the demographics targeted by these recruiters. The most direct impacts of Al on this process are currently twofold:

- 1. Language barrier reduction: AI has enabled traffickers to communicate more fluently in a wider range of languages, including less commonly spoken ones. Previously, the lack of widespread knowledge of these languages had somewhat protected certain linguistic communities from online trafficking recruitment. Now, with AI-powered translation and language generation, these barriers are diminishing.
- 2. Shift in victim demographics: The language skills of those being trafficked into scam centres have become less critical. Traffickers can now rely on Al to facilitate communication, rather than recruiting victims with specific language skills. This expands the pool of potential victims and changes the criteria traffickers use in their recruitment process.

These developments, while still in their infancy, underscore the need for heightened awareness and updated prevention strategies to address AI-facilitated trafficking recruitment. While AI use in cyber-scam centres remains a situational tool only used by some scammers in some contexts, the potential for it to be scaled up is something preparations should be made for now.

In the longer-term, the impact of AI on this crime type is less certain. While AI will continue to become more accessible and sophisticated, there might also be criminal tools developed to automate scamming conversations using AI agents. Accordingly, it is possible that the use of AI automation to engage scam victims could reduce the level of trafficking into this criminal industry. AI automation could be more attractive to scamming criminals due to its ability to scale, reduce risk and reduce costs of trafficking people into forced criminality.

FRAMING THE CRIMINAL USE OF GENERATIVE AI

The AI field is evolving quickly, and it can be challenging to conceptualise both current and potential future capabilities. One way to do this is to frame AI capabilities in terms of their ability to tackle complex tasks and how they can be used to automate processes. For example, a criminal copying and pasting translated text from an AI tool into a messaging app is a relatively simple task that is undertaken manually. The process of discovering potential victims, engaging with those potential victims and then establishing and maintaining a conversation using text, voice and video is a complex task requiring automation. The next section uses the framing illustrated in Figure 3 to examine how some of the key AI capabilities might be used by transnational criminal organisations to conduct trafficking in persons.



Figure 3: Generative AI can be used to conduct tasks such as sending a message, as well as automating these tasks to generate scale

CAPABILITY: REAL-TIME TRANSLATION OF TEXT AND SPEECH

Affected Trafficking Acts	Recruitment; exploitation
Affected Trafficking Means	Fraud/deception; psychological coercion including grooming and seduction
Threat Summary	Transnational crime figures can find and converse with potential victims who use different languages and have different cultures to their own, including groups previously unaffected by human trafficking. Typically, victim discovery will be via social media and conversations will occur via messaging platforms. Automation can enable large-scale victim search and recruitment.

Estimated progression of cost/skills of AI real-time translation and speech over time



Figure 4: Estimated progression of cost/skills of AI real-time translation and speech, over time. Not to scale.

DESCRIPTION

Consumer-level text-based language translation has been available for many years on websites and mobile apps. However, recent advancements in generative AI have led to freely available consumer chatbot technology that provides an understanding of culture and context. This capability is particularly conducive to facilitating some aspects of trafficking in persons.

Today, this technology is already being used to copy and paste translations for the purpose of deception. Sophisticated personas can be crafted by asking chatbots to perform a translation task which can include cultural context. This will allow transnational criminal organisations to extend their reach to previously unaffected communities.

More advanced uses of this technology are emerging. Voice synthesis technology can now clone individual voices, allowing perpetrators to impersonate a trusted individual. Recruitment and control via fraud and coercion are the most likely uses of this technology by human traffickers. Psychological coercion including grooming, seduction, shaming, sextortion and deception are also likely. Implementing threats via voice or text-based AI technology will be harder to accomplish while commercial AI models remain the most popular platforms. This is due to safety systems capturing and preventing statements of threat.

The automation of the criminal processes of finding and recruiting potential victims by traversing social networks could use customised open-source AI agent software. This will enable transnational criminal organisations to extend their reach and scale. This currently requires a high level of technical ability, but it's probable this will become easier and less expensive to develop as automation technology is built for commercial and consumer products. Multimodal AI will make automated conversations more convincing by using generated imagery and video.

In-progress conversations with potential victims are represented only as data and are therefore portable. The conversation history can be used to provide content to the AI agent. It means transnational crime figures could use a mixture of different online and offline AI during a conversation to evade detection. Whereas transnational crime figures engaging in conversation are interested to move the conversation to an exploitation scenario as quickly as possible, AI models would not need to focus on a rapid conversation, potentially extending the recruitment phase to many months or years, because the incremental cost is small.

Social media platforms, gaming platforms and dating sites are examples of vulnerable digital platforms.

CAPABILITY: GENERATION OF PUBLICATIONS, ADVERTS AND PERSONAS

Affected Trafficking Acts	Recruitment; exploitation
Affected Trafficking Means	Fraud/deception
Threat Summary	Transnational criminal organisations can create convincing adverts and websites designed to attract potential victims. The removal of language and cultural barriers will allow access to new communities. Similarly, technology can be used by transnational criminal organisations to generate websites, media and adverts to exploit victims who have been trafficked for the purpose of commercial sexual exploitation. Automation will lead to articles published to multiple audiences and using techniques such as astroturfing to create the perception of credibility.

Estimated progression of cost/skills of AI real-time translation and speech over time



Figure 5: Estimated progression of cost/skills of AI generation of articles, adverts and personas over time. Not to scale.

DESCRIPTION

Today, online adverts via websites and social media are common ways for transnational criminal organisations to recruit. Translation software and new chatbot AI technology will help authors create more engaging and convincing adverts by using generative AI's ability to create context-specific content that can engage with a variety of different groups.

Beyond the use of consumer technology, transnational criminal organisations may also adopt commercial or bespoke technology to increase scale and effectiveness. Some of this is an extension to existing commercial capabilities in digital marketing, such as market segmentation, which is the ability to target adverts to specific online groups. The effectiveness of this capability is expected to increase.

Digital 'astroturfing' is used to influence people's decisions by artificially creating the impression of credibility. This could be accomplished in several ways. Firstly, by automatically creating multiple online personas and generating conversational posts related to an employer or advert. Secondly, entire websites could be generated containing content strengthening the credibility of a recruiter, advert or employer. Finally, individual personas could be created or replicated containing artificially generated voice and imagery and used to advertise and recruit. Astroturfing is not a new concept and has been used in the past to generate momentum of support for political candidates and extremists. Generative AI is expected to increase the effectiveness by creating more convincing conversational engagement using AI agent software.

Trafficking recruitment and exploitation is likely to become more effective using generative AI. Existing vulnerabilities such as poverty will be exploited. This will affect efforts to tackle forced labour, commercial sexual exploitation and other typologies where there is recruitment or exploitation occurring across language or cultural boundaries. However, additional communities including internet-savvy and well-educated professionals could also become targets as AI can generate the jargon and terminology used by these communities in adverts and other recruitment media.

A particular risk for women and girls is that advertisements related to commercial sexual exploitation will be enhanced using AI generated personas and content. Typically, sexual services are advertised on social media platforms, messaging groups and dedicated adult services websites (ASWs). AI-generated advertisements and imagery could make it harder to identify differences between adverts used by consenting people engaged in prostitution and traffickers.

CAPABILITY: GENERATION OF DEEPFAKE MEDIA

Affected Trafficking Acts	Recruitment; transportation; exploitation
Affected Trafficking Means	Psychological coercion; reputational harm; deception
Threat Summary	Transnational criminal organisations can use AI to generate "deepfake" videos and images. Content can closely resemble individuals or documents. Fake documents including identity documents and certifications can be generated for the purpose of victim deception and money laundering. Non-consensual sexual images and videos are generated using existing real images of people and are used to threaten and to coerce. This threat could evolve to exploit victims' images in new entertainment and collaborative environments such as virtual or augmented virtual experiences.

Estimated progression of cost/skills of AI generation of deepfake media over time



Figure 6: Estimated progression of cost/skills of AI generation of deepfake media over time. Not to scale.

DESCRIPTION

Deepfake technology allows users to generate a new image or video either using source media, or simply from within the AI model itself. Recently the use of deepfake technology to generate images and videos has been used for the purposes of creating disinformation, fraud (including identity fraud), pornography and child sexual abuse imagery.

The most likely use of deepfake media in trafficking scenarios are:

- 1. Creating a virtual identity for the purpose of deception or control, e.g. to recruit and transport an individual across borders.
- 2. Impersonating somebody for the purpose of deception or control. This could be a close relative, for example.
- 3. Generating non-consensual sexual imagery of a potential victim for the purpose of coercion and control, including minors.

Deepfake technology can be used alongside other AI capabilities, including those used to generate adverts and converse with potential victims. In general, deepfakes increase the realism and therefore the likelihood of deceiving someone. Women and girls are the most likely victims of sexual deepfake imagery.²⁴ This media can be used to coerce and control an individual by threatening to release the media and create reputational harm. Therefore, there is a risk that this technology is utilised by human traffickers to recruit and control victims.

Deepfake AI can be used to generate fake companies, fraudulent travel documents such as visas and passports, certification documents, and fake identities for the purpose of money laundering.²⁵ This can allow transnational criminal organisations to move the profits of trafficking more easily. It is expected that AI's use for the purpose of financial crime will become more sophisticated and automated over time.

PROACTIVE MEASURES AND INTERVENTIONS

Over the last few years there has been a significant focus by companies, governments and research institutions to grapple with the risks of Al. An array of different topics has been considered, including the generation of disinformation, deepfake media, health, the use of Al military technology, intellectual property rights and various effects on human rights such as privacy.^{26,27,28} Some of these are relatively new threats, such as deepfake technology which was out of the reach of consumers only a few years ago.

To combat AI-enabled human trafficking we can consider broadly three lines of defence:

- The first line is the AI models themselves. This is related to the design and governance of model development to reduce the likelihood of models being used for criminal purposes.
- The second line relates to all digital systems where people can connect or collaborate, including social media platforms, gaming platforms and forums. This is how Al-enabled systems can connect with people.
- 3. The third line is people themselves. This relates to prevention initiatives, education and awareness of potential threats.

FIRST LINE: AI GOVERNANCE

Much of the global debate has focused on the first of these lines of defence—the AI model. Over the last few years there has been significant progress:

- In November 2023, in response to the sudden technical advancements, the United Kingdom hosted the first multinational AI Safety Summit.²⁹ This high-profile event set objectives to foster greater international collaboration and to encourage organisations to take a 'risk-based' approach to assessing and responding to AI threats.
- Most large companies that are developing Al models have released either guiding principles or policies governing the development of Al.³⁰
- There are now significant research initiatives focused on ethics and AI risks.³¹
- New Al-related legislation has recently been adopted in the European Union³² and advanced

discussions are taking place in the United States.³³ At the international level, the Council of Europe has adopted the first-ever international legally binding treaty aimed at ensuring the respect of human rights, the rule of law and democratic legal standards in the use of AI systems .

 The United Nations B-Tech project has begun looking at ways to incorporate a human rightsbased approach to AI development and created a taxonomy of generative AI human rights harms,³⁴ and the UN multi-stakeholder High-level Advisory Body on Artificial Intelligence has also published the report 'Governing AI for Humanity'.³⁵

Given this seemingly significant effort, are the risks that human traffickers will exploit AI being considered appropriately?

There are scenarios where AI safety features will mitigate some of the relevant risks. Consider the scenario where a criminal attempts to coerce a child to give them their mobile phone number: Figure 7 shows an example of an exchange between a person and the OpenAI GPT-40 language model:



Figure 7: An OpenAl GPT-40 response to a simulated request to translate a threat to a potential victim [tested July 2024].

The technology has identified the request as potentially harmful; however, it does not know the context in which the requested translation will be used. (In fact, it has requested feedback from the potential criminal!) Figure 8 shows an equivalent request on a Llama 3.1 8B Al model. In this example the model has identified the request has coercion and refused to assist the user.



Figure 8: A Llama3.1 8B response to a simulated request to translate a threat to a potential victim [tested August 2024].

'Jailbreaking' is a term used to describe ways in which AI models can be tricked into releasing content that could cause harm. Preventing these types of potentially harmful workarounds has been a particular focus of AI companies as they currently present one of the most visible safety issues.

Figure 9 shows a subsequent request which is similar to the previous example, however, in this example the context of the request has been modified to be seemingly benign. In this example, the model releases the translation.



Figure 9: A Llama3.1 8B response to a simulated refactored request to translate a threat to a potential victim [tested August 2024].

An adjustment to the initial request that removes the hostility by changing the context can result in an unchallenged response. Although this could be perceived as a weakness of AI models, the reality is that carefully crafted prompts used in trafficking scenarios can bypass safety technology when the criminal intent of the user is hidden. Other content, such as deceptive job adverts or recruitment conversations would be even harder to confidently label as a safety issue.

Many leading commercial AI models are only available online and are not available for download. However, a growing number of models are open source. This means that the model can usually be downloaded and operated on another computer or device. The model used in the examples in Figure 8 and Figure 9 is open source and was downloaded to a laptop and used in an offline mode. This poses additional challenges when trying to ensure safety: for hosted systems it might be possible to track illicit usage of the system and identify safety concerns. However, the usage of an open-source AI model cannot be monitored if it is being used offline.

Much of the threat of Al discussed in the previous chapters are enhancements to existing human trafficking processes that occur on the internet every day. Traffickers use technology in relative safety because discovering the conversations and processes that are a part of the crime is difficult and expensive. The harmful material is very similar to the many innocent conversations, social media posts and digital adverts that are published every day. For the same reason, it may be difficult to govern the Al model design sufficiently to mitigate this risk.

Al safety systems should attempt to incorporate mechanisms that prevent Al language models from disclosing technical approaches and code samples that could be used to breach digital platforms and allow the automation of criminal user engagement.

SECOND LINE: DIGITAL PLATFORMS

In this context, digital platforms include any software platform on which people can connect, converse or advertise to others.

The ecosystem of potentially vulnerable digital systems includes:

- Large social media platforms
- Apps hosted on social platforms
- Gaming platforms networks
- Instant messaging platforms
- Discussion forums and jobs boards
- Dating apps

Digital platforms are regularly used by transnational criminal organisations to recruit and control people for the purpose of exploitation and human trafficking.³⁶ Systems are designed to enable social engagement, and many do not enforce strong authentication based upon human identity. Although the very large social media platforms are frequently used in this way, hundreds of other smaller platforms and websites are also vulnerable to being used, and most do not have the same safety system resources available as larger platforms.

To counter the threat, companies and technologists responsible for digital platforms must become more familiar with human trafficking processes and the communities who are threatened by them. A wholesale programme of education and awareness amongst technologists is required, including enhancements to university technology courses and collaborative efforts across the private sector and NGOs to ensure that the threat and understanding of human trafficking is built into the lexicon of technology product development.

Widescale technology-based interventions can unintentionally risk harm to vulnerable communities. Therefore, it is recommended that the private sector works with survivors and those with lived experience across different contexts and communities to co-develop interventions that minimise risk whilst increasing the likelihood that traffickers using generative AI on the platforms can be detected.

THIRD LINE: NGOS AND RESEARCH INSTITUTIONS

Although there may be governance or technologybased interventions, the complexity and scope of trafficking in persons means that existing front-line prevention programmes as well as anti-trafficking research initiatives should be strengthened and adapted to understand and counter potential Albased targeting of vulnerable communities.

Vulnerable communities will increasingly become targets of traffickers using digital channels, alongside other crimes such as scams and extortion. Therefore, existing programmes of education and awareness of online crimes should be extended to include online recruitment from highly convincing Al-generated personas.

Front-line organisations, including NGO hotlines and case teams should extend their data capture to record any instances of suspected Al-usage outlined in previous sections.

Research into Al-enabled crimes should be extended to include trafficking in persons. Focus areas should include:

- The uses of consumer AI technology to connect to vulnerable communities previously unaffected by trafficking.
- The potential use of sophisticated automated systems to scale the crime, which could be used by well-financed transnational criminal organisations.
- Tracing financial profits and determining how Al is used by transnational criminal organisations to launder money.
- The intersection of gender-based violence using deepfake non-consensual sexual imagery and trafficking control mechanisms.

CONCLUSION

As this policy brief has demonstrated, the intersection of artificial intelligence and human trafficking presents a complex and evolving challenge to the anti-trafficking community, as well as more generally to all of society. The potential for AI to amplify the reach and effectiveness of trafficking operations is significant, from enhancing recruitment techniques and victim control to facilitating money laundering and evading detection. However, it is important to recognise that while these threats are serious, they are not insurmountable. With proactive measures, collaborative efforts, and innovative thinking, we can work to mitigate these risks and harness the power of AI for good in the fight against trafficking in persons.

The recommendations outlined in this report provide a starting point for action. They emphasise the need for a multi-faceted approach involving governments, the technology industry, NGOs, and survivors. Key areas of focus include the development of clear and concrete anti-trafficking measures for technology companies, the enhancement of AI safety features, improved education and awareness programs, and increased support for research initiatives. These measures, if implemented effectively, can help create a more robust defence against AI-enabled trafficking in persons while also promoting responsible AI development and use.

In line with this, while the challenges posed by AI in the context of trafficking in persons are significant, they also present an opportunity for the global community to come together in new and meaningful ways. The 'whole of society' approach to combating human trafficking should cross borders, as technology and AI increasingly enable trafficking crimes to do. By maintaining a proactive stance, investing in research and prevention, and fostering cross-sector collaboration, we can work towards a future where technology serves as a powerful tool in the prevention and disruption of trafficking in persons, rather than a means of its proliferation. To see this come to fruition, the time to act is now.

GLOSSARY

Al Agent

Al software which can run autonomously, interact with its environment (e.g. the internet), and is designed with a specific goal. An example is a virtual assistant. Some Al agents can interact with other Al agents.

Artificial Intelligence (AI)

A branch of computer science focused on creating systems capable of performing tasks that typically require human intelligence.

Al Model

An AI model is a computer program trained on data to do specific tasks, such as generate content or translate text.

Astroturfing

A deceptive technique to make digital content appear more genuine or credible by using artificial personas to interact with the content.

Deepfake

An image or recording which has been altered or generated using Al. Deepfakes often depict either a real or non-existent person or persons.

Generative Al

A type of artificial intelligence that can generate text, images, videos and other content. Generative Al uses Al models which have been pre-trained on large amounts of data.

Jailbreak

In the context of AI, jailbreaking is using techniques to bypass safety mechanisms built into AI models.

Large Language Model (LLM)

A type of generative AI which is focused on generation of text content. LLMs are trained on very large amounts of text. However, "large" refers to the complexity and resulting sophistication of the AI model.

Multimodal Al

A type of generative AI which can accept and generate multiple types of content, including text, audio, images and video. An example might be a chatbot which people can use to analyse documents and generate images.

ENDNOTES

1 European Parliament, EU AI Act: first regulation on artificial intelligence (2023), available at: <u>https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence</u>

2 Council of Europe Portal, The Framework Convention on Artificial Intelligence, available at: <u>https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence</u>

3 Protocol to Prevent, Suppress and Punish Trafficking in Persons Especially Women and Children (2000) (Palermo Protocol)

4 United Nations Office on Drugs and Crime (UNODC), Human Trafficking - the Crime, available at: <u>https://www.unodc.org/unodc/en/human-trafficking/crime.html</u>

5 Goldman Sachs, Al investment forecast to approach \$200 billion globally by 2025 (2023), available at: https://www.goldmansachs.com/insights/articles/ai-investment-forecast-to-approach-200-billion-globally-by-2025

6 Meta, Introducing Meta Llama 3: The most capable openly available LLM to date (2024), available at: <u>https://ai.meta.com/blog/meta-llama-3/</u>

7 OpenAl, Introducing ChatGPT (2022), available at: https://openai.com/index/chatgpt/

8 Will Douglas Heaven (MIT Technology Review), OpenAl's new language generator GPT-3 is shockingly good—and completely mindless (2020), available at: <u>https://www.technologyreview.</u> com/2020/07/20/1005454/openai-machine-learning-language-generator-gpt-3-nlp/

9 OpenAI, Improving language understanding with unsupervised learning (2018), available at: <u>https://openai.com/index/language-unsupervised/</u>

10 Sharon Goldman (Venture Beat), 'Attention is All You Need' creators look beyond Transformers for Al at Nvidia GTC: 'The world needs something better' (2024), available at: <u>https://venturebeat.com/ai/attention-is-all-you-need-creators-look-beyond-transformers-at-nvidia-gtc-the-world-needs-something-better/</u>

11 Bloomberg, Generative AI to Become a \$1.3 Trillion Market by 2032, Research Finds (2023), available at: <u>https://www.bloomberg.com/company/press/generative-ai-to-become-a-1-3-trillion-market-by-</u> 2032-research-finds/

12 Europol, New report finds that criminals leverage AI for malicious use – and it's not just deep fakes (2020), available at: <u>https://www.europol.europa.eu/media-press/newsroom/news/new-report-finds-criminals-leverage-ai-for-malicious-use-%E2%80%93-and-it%E2%80%99s-not-just-deep-fakes</u>

13 Jean Mackenzie and Nick Marsh (BBC), South Korea faces deepfake porn 'emergency' (2024), available at: https://www.bbc.co.uk/news/articles/cg4yerrg4510

14 BBC Bitesize, What are 'bots' and how can they spread fake news?, available at: <u>https://www.bbc.</u> <u>co.uk/bitesize/articles/zjhg47h</u> 15 Allyson Versprille (Bloomberg), Al Is Making Financial Fraud Easier and More Sophisticated, US Treasury Warns (2024), available at: <u>https://www.bloomberg.com/news/articles/2024-03-27/impersonation-phishing-getting-trickier-with-ai-treasury-warns</u>

16 Paulina Pielichata (Risk.net), AI hack threat forcing banks to review cyber controls (2024), available at: https://www.risk.net/risk-management/7959597/ai-hack-threat-forcing-banks-to-review-cyber-controls

17 Brian New (CBS News), How AI is revolutionizing Internet fraud and romance scams (2024), available at: https://www.cbsnews.com/texas/news/i-team-how-ai-is-revolutionizing-internet-fraud/

18 Lisa O'Carroll (The Guardian), Al fuelling dating and social media fraud, EU police agency says (2024), available at: <u>https://www.theguardian.com/technology/2024/jan/09/ai-wars-dating-social-media-fraud-eu-crime-artificial-intelligence-europol</u>

19 Charles Bethea (The New Yorker), The Terrifying A.I. Scam That Uses Your Loved One's Voice (2024), available at: <u>https://www.newyorker.com/science/annals-of-artificial-intelligence/the-terrifying-ai-scam-that-uses-your-loved-ones-voice</u>

20 Polaris, On-Ramps, Intersections, and Exit Routes: A Roadmap for Systems and Industries to Prevent and Disrupt Human Trafficking (2018), available at: <u>https://polarisproject.org/wp-content/uploads/2018/08/A-Roadmap-for-Systems-and-Industries-to-Prevent-and-Disrupt-Human-Trafficking-Social-Media.pdf</u>

21 Laura Dobberstein (The Register), Exposed: Chinese smartphone farms that run thousands of barebones mobes to do crime (2024), available at: <u>https://www.theregister.com/2024/03/21/china_smartphone_farms/</u>

22 United Nations Office on Drugs and Crime (UNODC), Scams and trafficking for forced criminality: UNODC establishes emergency response network to combat human trafficking in Southeast Asia (2024), available at: https://www.unodc.org/roseap/en/2024/05/emergency-response-network/story.html

23 60 Minutes Australia, Human trafficking victims tortured into scamming innocent people (2024), available at: <u>https://www.youtube.com/watch?v=7b7JAX03×2Q</u>

24 Nicholas Kristof (The New York Times), The Online Degradation of Women and Girls That We Meet With a Shug (2024), available at: <u>https://www.nytimes.com/2024/03/23/opinion/deepfake-sex-videos.</u> <u>html</u>

25 Alanna Titterington (Kaspersky Daily), How fraudsters bypass customer identity verification using deepfakes (2024), available at: <u>https://www.kaspersky.co.uk/blog/how-deepfakes-threaten-kyc/28057/</u>

26 Hanna Darnton, Lindsey Andersen, J.Y. Hoh and Samone Nigam (BSR), A Human Rights Assessment of the Generative AI Value Chain (2024), available at: <u>https://www.bsr.org/en/blog/a-human-rights-assessment-of-the-generative-ai-value-chain</u>

27 United Nations Human Rights Office of the High Commissioner (OHCHR), Advancing Responsible Development and Deployment of Generative AI (2023), available at: <u>https://www.ohchr.org/sites/default/files/documents/issues/business/b-tech/advancing-responsible-development-and-deployment-of-GenAI.pdf</u>

28 UK Government, Historic first as companies spanning North America, Asia, Europe and Middle East agree safety commitments on development of AI (2024), available at: <u>https://www.gov.uk/government/news/historic-first-as-companies-spanning-north-america-asia-europe-and-middle-east-agree-safety-commitments-on-development-of-ai</u>

29 UK Government, AI Safety Summit: Hosted by the UK (2023), available at: <u>https://www.aisafetysummit.</u> gov.uk/

30 Paul B. de Laat, Companies Committed to Responsible AI: From Principles towards Implementation and Regulation? Philosophy & Technology 34, 1135-1193 (2021), available at: <u>https://link.springer.com/</u> article/10.1007/s13347-021-00474-3

31 The Alan Turing Institute, Artificial intelligence (Safe and ethical), available at: <u>https://www.turing.ac.uk/</u> research/research-programmes/artificial-intelligence-ai/safe-and-ethical

32 European Parliament, EU AI Act: first regulation on artificial intelligence (2023), available at: <u>https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence</u>

33 The White House, Blueprint for an Al Bill of Rights: Making Automated Systems Work for the American People (2022), available at: <u>https://www.whitehouse.gov/ostp/ai-bill-of-rights/</u>

34 United Nations Human Rights Office of the High Commissioner (OHCHR), B-Tech Project: OHCHR and business and human rights, available at: <u>https://www.ohchr.org/en/business-and-human-rights/b-tech-project</u>

35 United Nations Al Advisory Body, Governing Al for Humanity: Final Report (2024), available at: <u>https://www.un.org/sites/un2.un.org/files/governing_ai_for_humanity_final_report_en.pdf</u>

36 Walk Free, Anti-Social: Modern Slavery on Social Media, available at: <u>https://www.walkfree.org/global-slavery-index/findings/spotlights/modern-slavery-on-social-media/</u>



THE ORGANIZATION FOR SECURITY AND CO-OPERATION IN EUROPE

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. Recognised 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 politicomilitary 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, democratisation, 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 | Czech Republic | 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

The materials in this publication are for general information purposes only, provided on an 'as is' basis, without warranties of any kind, including fitness for any particular purpose. The OSCE, specifically, does not make any warranties with respect to the accuracy or completeness of the information in this publication. The views, findings, interpretations and conclusions expressed herein are those of the author(s) and do not necessarily represent the official position of the OSCE and/or its participating States. To the extent permitted by law, the OSCE does not accept any liability for any loss, damage, liability or expense incurred or suffered, which may arise as a result of, or in connection with, the use of information contained in this publication. This publication does not address questions of responsibility, legal or otherwise, for acts or omissions on the part of any person. The use of particular designations of countries or territories does not imply any judgement by the publisher, the OSCE, as to the legal status of such countries or territories, of their authorities and institutions or of the delimitation of their boundaries.



THE REGIONAL SUPPORT OFFICE OF THE BALI PROCESS

In 2002, the Bali Process on People Smuggling, Trafficking in Persons and Related Transnational Crime was formed as a non-binding, multilateral forum to facilitate policy dialogue, cooperation and information sharing in Asia and the Pacific Region. Co-chaired by Australia and Indonesia, Bali Process Membership includes 45 Member States and 4 international organisations, and 26 observer countries and international organisations.

In 2012, the Regional Support Office of the Bali Process (RSO) was established in Bangkok, Thailand, to provide technical support to the Bali Process and strengthen cooperation on international migration, including human trafficking and people smuggling. The RSO is the only cooperation mechanism of its kind in the Asia-Pacific region, with the breadth of its membership allowing it to draw on policy knowledge, technical expertise, and operational experience from across Bali Process Members to facilitate information sharing, support collaboration between Members, and to implement practical solutions to shared regional migration challenges.

MEMBER STATES: Afghanistan | Australia | Bangladesh | Bhutan | Brunei Darussalam | Cambodia | China | DPR Korea | Fiji | France | Hong Kong SAR | India | Indonesia | Iran | Iraq | Japan | Jordan | Kiribati | Lao People's Democratic Republic | Macau SAR | Malaysia | Maldives | Mongolia | Myanmar | Nauru | Nepal | New Zealand | Pakistan | Palau | Papua New Guinea | Philippines | Republic of Korea | Samoa | Singapore | Solomon Islands | Sri Lanka | Syria | Thailand | Timor-Leste | Tonga | Türkiye | UAE | USA | Vanuatu | Viet Nam

OBSERVER STATES: Austria | Belgium | Canada | Denmark | European Commission | Finland | Germany | Italy | Netherlands | Norway | Poland | Romania | Russian Federation | South Africa | Spain | Sweden | Switzerland | United Kingdom

MEMBER ORGANISATIONS: International Organization for Migration (IOM) | International Labour Organization (ILO) | UN Refugee Agency (UNHCR) | United Nations Office on Drugs and Crime (UNODC)

OBSERVER ORGANISATIONS: Asian Development Bank (ADB) | APC Migration | International Centre for Migration Policy Development (ICMPD) | International Committee of the Red Cross (ICRC) | Intergovernmental Consultations on Migration, Asylum and Refugees (IGC) | International Federation of Red Cross and Red Crescent Societies (IFRC) | INTERPOL | United Nations Development Programme (UNDP) | The World Bank



Regional Support Office of the Bali Process (**RSO**) 27th Floor Rajanakarn Building 3 South Sathorn Road, Sathorn, Bangkok 10120, Thailand

> Tel. +66 2 343 9477 Fax. +66 2 676 7337 info@rso.baliprocess.net

For further information on the Bali Process and the RSO please visit **www.rso.baliprocess.net**





baliprocessrso



www.linkedin.com/company/ regional-support-office-ofthe-bali-process

in



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

info-cthb@osce.org

www.osce.org/cthb





www.facebook.com/ osce.org www.x.com/ osce_cthb

https://www.linkedin.com/ showcase/ osce-cthb/