Highlights of the 2021 Roundtable on tech-facilitated THB in Central Asia

Combating technology-facilitated trafficking in human beings in Central Asia and across the OSCE Asian Partners for Co-operation

27-28 April 2021 | Vienna, Austria and via teleconference

OSCE Organization for Security and Co-operation in Europe

OSCE Asian Partnership for Co-operation

Asian Partnership for Co-operation

Highlights of the 2021 Roundtable on tech-facilitated THB in Central Asia

Combating technology-facilitated trafficking in human beings in Central Asia and across the OSCE Asian Partners for Co-operation

27-28 April 2021 | Vienna, Austria and via teleconference

Disclaimer

The recommendations, statements and positions set out in the following summary have been drafted by the OSCE based on the ideas and suggestions that were raised during the event and informed by the panel discussions. They do not necessarily reflect the position of the author and of each individual panellist or the position of their respective organizations. The views, opinions, conclusions, and other information expressed in this document are not necessarily endorsed by the Organization for Security and Co-operation in Europe (OSCE).

Acknowledgements

The OSCE Office of the Special Representative and Co-ordinator for Combating Trafficking in Human Beings thank all the panellists and speakers who agreed to share their expertise in the course of the two days of the online conference. Each of the experts and practitioners offered unique insights for participating States and the OSCE Asian Partners to step up efforts to prosecute offenders and eradicate human trafficking at the national, regional and international levels.

TABLE OF CONTENTS

INTRODUCTION

The OSCE enjoys a long-standing level of co-operation with the Asian Partners for Co-operation. Over the past decades, the Asian Partners for Co-operation have contributed substantially to the OSCE's dialogue on various aspects of comprehensive security, at the same time providing ideas for future and even closer security co-operation. In furtherance of close and productive collaboration between the OSCE and Asian Partners for Co-operation, the OSCE Office of the Special Representative and Co-ordinator for Combating Trafficking in Human Beings (OSR/CTHB) organised the Roundtable Combating technology-facilitated trafficking in human beings in Central Asia and across the OSCE Asian Partners for Co-operation.

The major objective of the Roundtable was to discuss how technology is being misused by traffickers in human beings in Central Asia and across the OSCE Asian Partners for Co-operation, especially at the stage of advertising victims of sexual exploitation on online platforms. The specific focus of discussion on the advertisement of victims is needed because this is the most visible part of technology-facilitated trafficking and offers more opportunities to identify victims and traffickers. Since the crime of trafficking for sexual exploitation is financially motivated and traffickers' main goal is to earn as much illegal proceeds as possible, they need to advertise their victims on open platforms easily accessible for the buyers of sexual services. The Internet, especially the open web, is one of the most optimal platforms from this point of view because it provides traffickers and potential traffickers with an environment in which they can operate with an enhanced level of safety and anonymity and advertise their victims to a broad audience on hundreds or thousands of platforms with minimal costs.

Due to the coronavirus pandemic, the event was held online and attracted more than 170 registered participants representing a large spectrum of national and international stakeholders working directly or indirectly on combating trafficking in human beings. The panellists of the event included prominent experts and practitioners from international organisations and law enforcement agencies including Europol, Interpol, and US Department of Homeland Security, as well as from OSCE Asian Partners for Co-operation, which included Afghanistan, Australia, Japan, Republic of Korea and Thailand, sharing views and examples of technology-facilitated THB, as well as existing practices, policies and legislations combatting the issue.

Throughout the roundtable, the panel presentations showcased a variety of different methods, technologies and online platforms deployed by perpetrators and criminal networks to commit the offence throughout all trafficking stages in the region, as well as highlighted promising practices, existing policies and legislations, as well as the need for collaboration among the stakeholders.

OPENING REMARKS

Mr. Valiant Richey, OSCE Special Representative and Co-ordinator for Combating Trafficking in Human Beings (SR-CTHB), and **H.E. Ambassador Igli Hasani**, Permanent Representative of the Republic of Albania to the International Organisations in Vienna, Chair of the OSCE Asian Partnership for Co-operation, opened the roundtable.

At the opening session, speakers described the scope and purpose of the conference: (i) understanding how technology is being misused by traffickers in Central Asia and other OSCE Asian partners; (ii) exchanging knowledge, expertise, and good practices among stakeholders; and (iii) identifying possible solutions to the problem.

Speakers highlighted how the **development of technology has had a decisive influence** on the crime of trafficking in human beings, fundamentally changed its landscape, criminal conduct as well as the discourse, counter-strategies, prevention and responses to the crime by anti-trafficking stakeholders. Research and direct evidence showed that technology is being misused by traffickers **during all stages of the crime**, including recruitment, control, and exploitation of victims.[1] The misuse of technology and digital, network communications tools and platforms by traffickers has led to an exponential increase in the scale of exploitation of victims, thus urgently requiring **a coordinated and multilateral approach** from all countries and stakeholders.

To illustrate the **transnational nature of the crime** in today's digitally connected world and the consequent **need for multilateralism**, speakers gave the example of a situation where the victim was recruited and sexually exploited through, for example, live streaming platforms and services in one country, which was then used by offenders in a second country and the servers of the company used to record and store the content made of that trafficking victim located in a third country. In other words, technology has **transcended the traditional geographical limitations** of the crime, making it more profitable, lowering the entry / cost barriers for offenders and traffickers and at the same time, creating significant legal loopholes and multi-jurisdictional challenges to the existing national trafficking policies and patchy cyber legislations.

Adding to the problem are the negative impacts of the coronavirus pandemic on trafficking in human beings' situations worldwide – notably among which is the proliferation of produced and exchanged videos and images of sexually abused adults and children in the digital world, due to the population's sudden and increased shift to online activities. For example, the US National Centre for Missing and Exploited Children (NCMEC) reported a quadrupled number of child sexual abuse reports globally, from 1 million in April 2019 to 4.1 million a year later.[2]

The opening speakers underlined that we should not accept conclusions that state that technology-facilitated trafficking was somehow less harmful to victims than normal or traditional trafficking of human beings because there is no physical contact.[3] Speakers reiterated that technology-facilitated exploitation not only increases harm to victims, for example, by increasing access to abusers, expanding the market and harming more victims, but it also allows for multiple forms of exploitation, including recording and distributing the exploitation contents which facilitate revictimization and affect the victims long after the actual abuse has ended.

Finally, speakers emphasized that the roundtable's discussions and findings are topical and important not only for the OSCE Asian Partners for Co-operation, but they are also relevant to the entire OSCE region, as technology has created a global market where traffickers can exploit their victims online and connect with users from all around the world. Speakers therefore encouraged joint efforts and knowledge sharing between countries with advanced technical capabilities and policies and those with limited ones, in order for any anti-trafficking efforts to succeed.

[1] Please refer to the OSCE – Tech Against Trafficking publication, '*Leveraging innovation to fight trafficking in human beings*: a comprehensive analysis of technology tools', published 22 June 2020, available at https://www.osce.org/cthb/455206

[2] European Commission, EU strategy for a more effective fight against child sexual abuse, 2020, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20200724_com-2020-607-commission-communication_en.pdf

[3] Examples of such false perceptions include the perceived harmfulness of such exploitative conduct by the parents who, given their circumstances, chose to sexually exploit their own children via live-streaming and did not think of it as abuse due to the lack of physical contact between the child and the paedophiles.

PANEL 1

Technology-facilitated THB for sexual exploitation – definitions, trends, and specific characteristics

Panel 1 provided a general overview of the definitions and trends of technology-facilitated trafficking in human beings, specifically regarding how criminal networks and traffickers are increasingly using technology in all stages of committing the crime. Given the transnational nature of the issue, case studies were presented to illustrate the importance of multilateral and multi-stakeholder partnerships and collaboration in preventing and addressing the crime.

The panel was moderated by **Mr. Radu Cucos**, Associate Officer on CTHB, the Office of the OSCE Special Representative and Co-ordinator for Combatting Trafficking in Human Beings (OSR-CTHB). Invited panel speakers included **Ms. Eleonora Forte**, Strategic Analyst, EUROPOL, **Mr. Eric McLoughlin**, U.S. Homeland Security Investigations Attaché in Bangkok, U.S. Department of Homeland Security and **Mr. Matthew Dompier**, Criminal Intelligence Officer, Crimes Against Children, INTERPOL General Secretariat.

Panellists presented the emerging challenges of technology-facilitated trafficking in human beings, notably among which are:

(i) **increased anonymity**, for example the use of end to end encrypted communications tools and apps,

(ii) **greater mobility**, traffickers do no longer need a physical location to exploit victims – they can exert control and exploit the victims from the distance, for example through live streaming, advertising, downloading and distributing illicit contents,

(iii) **massive scale of commercialisation**, victims and illicit materials are being advertised on multiple platforms, recorded videos can be played multiple times and live streaming does no longer need to be one on one – many offenders can make use of abused victims at the same time,

(iv) **reduced workforce**, criminal networks could reduce the infrastructure and number of members needed to perpetrate the criminal activities – they need only a few tech-savvy members instead, and

(v) **legislative loopholes**, for example it remains a challenge to use digital evidence in prosecutions; national cyber policies are patchy and lagging behind technological advancements, thus creating an opportunity for offenders.

Moving beyond the imminent challenges to responding to and investigating technology-facilitated trafficking in human beings, speakers looked at the operational aspect of the criminal activities, highlighting **how technology is being used in each and every single step of the trafficking process**, from the recruitment stage, profiling potential victims in online forums, social media and gaming platforms, up to the laundering of criminal proceeds step.

In the **recruitment phase**, traffickers reportedly make use of employment portals and social media as they create recruitment agencies and scout for potential victims through the traditional 'lover boy method' (creating a fake sentimental relationship with potential victims). Speakers further emphasized the importance of **early investigations and interventions during the recruitment phase**, so that potential victims can be identified and safeguarded from harm as early as possible. Recognising the recruiting methods currently deployed by perpetrators is therefore crucial in this regard. There are two specific profiling techniques of victims by traffickers: the first one is termed the '**hook fishing**' technique, referring to the false job advertisements (for example modelling contracts etc.) which are created by criminal networks and used as bait in order to attract potential victims. The second technique, called '**net fishing**', refers to the situation when criminals are actively roaming around social media platforms and forums to scout for job seekers.

In some cases, criminal networks even pretend to be official recruiters from recruitment agencies, asking potential victims for recruitment fees and/or creating their own fully fledged websites that look like career portals for jobs abroad.

After being recruited and/or groomed online, the victims will then be t**ransported to the place of exploitation** through, for instance, train / flight tickets bought online / remotely by perpetrators, or in some cases, via car sharing applications. During the **harbour and control phase**, traffickers make use of video messaging and communications tools to blackmail and threaten the victims (for example by threatening to distribute explicit photos and videos of the victims online, or with their friends and families). Following the control stage, victims are then **exploited and advertised online** through, for example, adult services websites, classified websites, dating website and on dating apps. While the initial contact and payment might be made via dating websites, the actual abuse of victims might occur on some other platforms, such as Skype video conferencing, thus making it harder for investigations.

Finally, trafficking networks use FinTech, digital wallets, and new technologies which enable **anonymized transactions** in order to exchange and launder their criminal proceeds. Speakers emphasize that the traditional payment methods such as prepaid cards and online payments are still dominant – however, the use of new technologies such as cryptocurrencies can be expected to be on the rise in the future.

Speakers also deplored the **demand side** and **profit-driven motivation** of offenders. On the one hand, trafficking in human beings for sexual and labour exploitation exists and is perpetrated by criminal networks in the EU and Central Asia because it is **sustained by a stable demand**. On the other hand, some offenders, for example the creators of the websites which host child sexual abuse materials, are found to not be necessarily driven by a sexual interest in children, but rather **driven by the profits and business model earned through ad revenue and click traffic to these websites**. They therefore keep on replicating such illicit websites over and over after each time they are taken down by law enforcement agencies, knowing that people who do have a sexual interest in children will be drawn there. The opportunity for the monetisation and commercialization of the abuse available to criminals through the use of technology should therefore not be overlooked.

Another trend of technology-facilitated trafficking in human beings highlighted by speakers includes the increasingly **prominent role of female offenders**.

Female offenders, sometimes trafficked women themselves, reportedly have a hands-on, tech-savvy part of the trafficking process. This includes actively roaming around social media platforms to find and recruit new victims, advertising the victims online, setting the targets for the victims, paying online service providers' fees, as well as collecting payments and criminal proceeds and wiring them across the criminal networks. Male offenders are found to be increasingly keeping more distance from the exploitation location. However, this gender role reshuffle does not mean a change in the leadership structure – leading positions and the accumulation of the criminal proceeds remain in the hands of male offenders.

Another concerning trend with the use of technology in the trafficking process discussed during the panel is that some abusers reportedly offered a business-like agreement with the victims, setting up some division of profits in order to trick the victims into believing that they are no longer victims or less exploited and threatened than before.

Although **technology** has made the exploitation of victims more efficient and widespread, it **can also be used to support investigations** – examples include the use of web crawling, filter technology, keyword matching, robust / binary hashing, artificial intelligence etc. in conducting automated searches through hundreds and thousands of escort advertisements posted online. Since traffickers tend to replicate advertisements on multiple platforms, the use of such technologies could help identify their common traits (such as same contact email addresses or telephone numbers, identical wording) at a much faster and wider scale, thus helping to speed up the intervention and investigation processes.

The complexity, cross-border and cross-cutting nature of the crime **requires a coordinated, multilateral and multi-stakeholder response**. In order to highlight this, speakers presented successful case studies and examples of such partnerships and joint investigations and interventions. Examples include the Operation Blackwrist, named after the identification of a minor with a black wrist. The operation started with an INTERPOL official identifying videos of child sexual abuse (CSA) being shared and distributed on the dark web. The investigations team quickly grew with the support and collaboration early on from multiple countries and stakeholders, including the US Department of Homeland Security Investigations (HIS), Thailand's Department of Special Investigations (GSI), the New Zealand Department of Internal Affairs, the Australian Federal Police, and non-governmental organisations such as ECPAT Thailand.

The operation's multi-lateral and multi-stakeholder joint efforts led to leads for offenders in multiple countries and successful interventions and rescues of victims. Since every country has their own rule of evidence and thresholds that they need for search and arrest warrants, the partnerships were fruitful in facilitating the process, shortening the intervention time in rescuing victims, gathering evidence, and holding offenders accountable. To sum up, this two-year long international operation led to the overall rescue of 50 children in multiple countries and the arrest of offenders in Thailand, Australia and the United States.

A two-year international operation coordinated by INTERPOL has led to the rescue of 50 children, as well as the arrest and prosecution of child sex offenders in Thailand, Australia and the United States.

Other examples of multilateral and multi-stakeholder partnerships include the INTERPOL's international child sexual exploitation database, which is used as a centralized clearinghouse for law enforcement around the world, and National Center for Missing and Exploited Children (NCMEC) reports. The databases collect reports from multiple sources including from electronic service providers such as Microsoft, Google, Facebook. Illicit CSA materials are then analysed and reported back to the appropriate jurisdictions for interventions, safeguarding victims and prosecuting offenders. It is worth noting that 90 percent of NCMEC reports (reported by US electronic service providers) have been referred to countries outside of the US.

Speakers also reiterated the importance of drafting and enforcing international and national policies which require technology companies, ICT service providers and social media platforms, especially multinational corporations, to implement monitoring and policing algorithms and processes in their online platforms and services, as well as to strengthen and make transparent their tools and platforms' reporting and safeguarding mechanisms.

Finally, speakers concluded by highlighting the main aspects of the impacts of the coronavirus pandemic on trafficking in human beings: (i) online recruitment and advertisement of victims have increased, as populations are increasingly shifting activities online; (ii) minors are at higher risks due to their increased online activities (for example online schooling) and lack of (or limited) digital awareness of the risks and threats posed by perpetrators; and (iii) exploitation is increasingly moved to more hidden locations due to the availability of livestreaming tools etc.

Speakers also raised an important point that, due to technology being widely accessible and present in every stage of trafficking in human beings, we should not differentiate between technology-facilitated trafficking and the 'traditional' crime, as the latter without a tech component is hard to come by. Rather, we should **accept technology as a new reality** and as an **inherent component of trafficking in human beings in today's world**.

Recommendations:

1. Engage in cross-border and inter-agency co-operation to share and exchange good practices and technical know-how and capabilities to combat the transnational nature of tech-facilitated THB;
2. Continuously invest in training and building technical capabilities of law enforcement officials, judges, and prosecutors;
3. Make use of new technologies such as web crawling, indexing and artificial intelligence in THB investigations to identify instances of human trafficking, including patterns of organized criminal activities;
4. Incorporate the use of digital evidence in the official procedure and protocol in THB investigations, enforcement, and criminal justice responses;
5. Understand and address the demand and profit-driven business model that incentivize criminals to monetise and commercialize the abuse, for example through ad revenue and click traffic to websites depicting illicit contents and exploitation of children and adults;
6. Create and enforce policies which require technology companies, social media platforms and service providers to implement monitoring processes in their online platforms and services, as well as to strengthen and make transparent their tools and platforms' reporting and safeguarding mechanisms;
7. Foster awareness, alignment of efforts and partnerships with the private sector, especially with technology companies, to combat tech-facilitated THB.

PANEL 2

Analysis of online platforms in Central Asia and across the OSCE Asian Partners for Co-operation with high risks of THB

Panel 2 discussed the specific platforms and technologies used by traffickers in Central Asia and across the OSCE Asian Partners for Co-operation. In order to effectively counter trafficking in the digital space, it is crucial to understand and recognize which platforms and tools are being used by perpetrators, and where the criminal activities are taking place. In the context of Central Asian, East and Southeast Asian regions, panellists reconfirmed the popularity, accessibility and widespread use of many of the platforms and tech tools identified and highlighted in panel 1 by both victims, potential victims and vulnerable groups, as well as traffickers and offenders.

The panel was moderated by **Mr. Radu Cucos**, Associate Officer on CTHB, the Office of the OSCE Special Representative and Co-ordinator for Combatting Trafficking in Human Beings (OSR-CTHB). **Prof. Yasuzo Kitamura**, Professor of International Law, Chuo University, Tokyo, Japan, **Mr. Brandon Kaopuiki**, Technical Advisor, Global Hub Against Online Sexual Exploitation of Children, International Justice Mission, **Ms. Zhanar Seitayeva**, Law Enforcement Academy under the Prosecutors General Office of Kazakhstan and **Mr. Romulus N Ungureanu**, PhD, International Law Enforcement Advisor featured as panel speakers.

Following on the overview of trends and the role of technology in today's trafficking in human beings which were discussed by the speakers from the first panel, Panel 2's speakers presented the specific platforms with high risk of THB used in the countries of Central Asia and across the OSCE Asian Partners for Co-operation, especially in Japan, Thailand, Kazakhstan, Kyrgyz Republic, Tajikistan, Turkmenistan, Uzbekistan, South Korea and Mongolia.

The panel highlighted that **Asia accounted for over half of the world's internet users in 2020**,[4] making it the leading region in terms of not only internet and social media usage, but also of the potential high number of vulnerable groups with high trafficking risks (for example teenagers and young internet users with limited awareness of trafficking risks online).

Although specific social media platforms, gaming and dating sites and apps might vary by country and region (for example Central Asia vs East Asia), panellists **reiterated the similar patterns, methods and misuse of technology in every trafficking stage** discussed in panel 1. These include the use of:

- social networking to profile, search, recruit and target vulnerable groups,
- mobile communication to anonymously communicate with victims, buyers and other criminals,
- online advertising in the open and dark web to appeal to offenders,
- digital media and livestreaming to abuse victims,
- moving criminal proceeds through the legal financial institutions and their money transfer services, and
- digital cameras and surveillance to monitor victims.

In Japan, **social networking service (SNS) apps and dating websites** are considered popular and widely used by traffickers for sexual exploitation of girls. Although the Japanese government enacted the Internet Dating Site Regulation Law since September 2003 (and amended in 2019), requiring its dating sites to implement age verifications of users, the illicit

[4] Source: Internet World Stats https://www.internetworldstats.com/stats.htm

activities between adult men and underage girls, called 'enjo kōsai' or 'compensated dating' in Japanese, are still happening. This is partly due to the fact that, after the initial contact from such dating sites, offenders and victims could then switch to other communication tools and messaging apps, such as LINE, Twitter, Facebook, Kakao Talk, Instagram, Hima-bu, to continue the conversations without facing further restrictions or strict monitoring policies imposed by the sites. Furthermore, traffickers and offenders have also been found to be **using secret languages, codes or emojis to avoid detection** by the search engines, policing and monitoring algorithms.

Examples of dating sites and SNS used for matching

Dating Sites or matching applis or "Deai-kei" site	Pato
	Dine https://dine.app/ja
	Tinder https://tinder.app/ja
	Badoo https://badoo.com/ja
	Paris
	Happy Mail https://happymail.co.jp
	Sugar Daddy
	Tokare date
	With https://with.is/welcome
	Waku Waku mail

SNS Social Networking Service	Line https://line.me/ja/
	Twitter
	Facebook - Online platform
	Kakao Talk - Online platform
	Instagram
	Hima-bu

In South and Southeast Asia, the use of **technology for victim surveillance, monitoring and controlling purposes** have been observed, for example from bonded labour in illegal mines in India to the commercial fishing sector, especially the illegal, unreported and unregulated (IUU) fishing in Thailand, to the manufacturing, food processing factories and commercial enterprises in the formal economies.

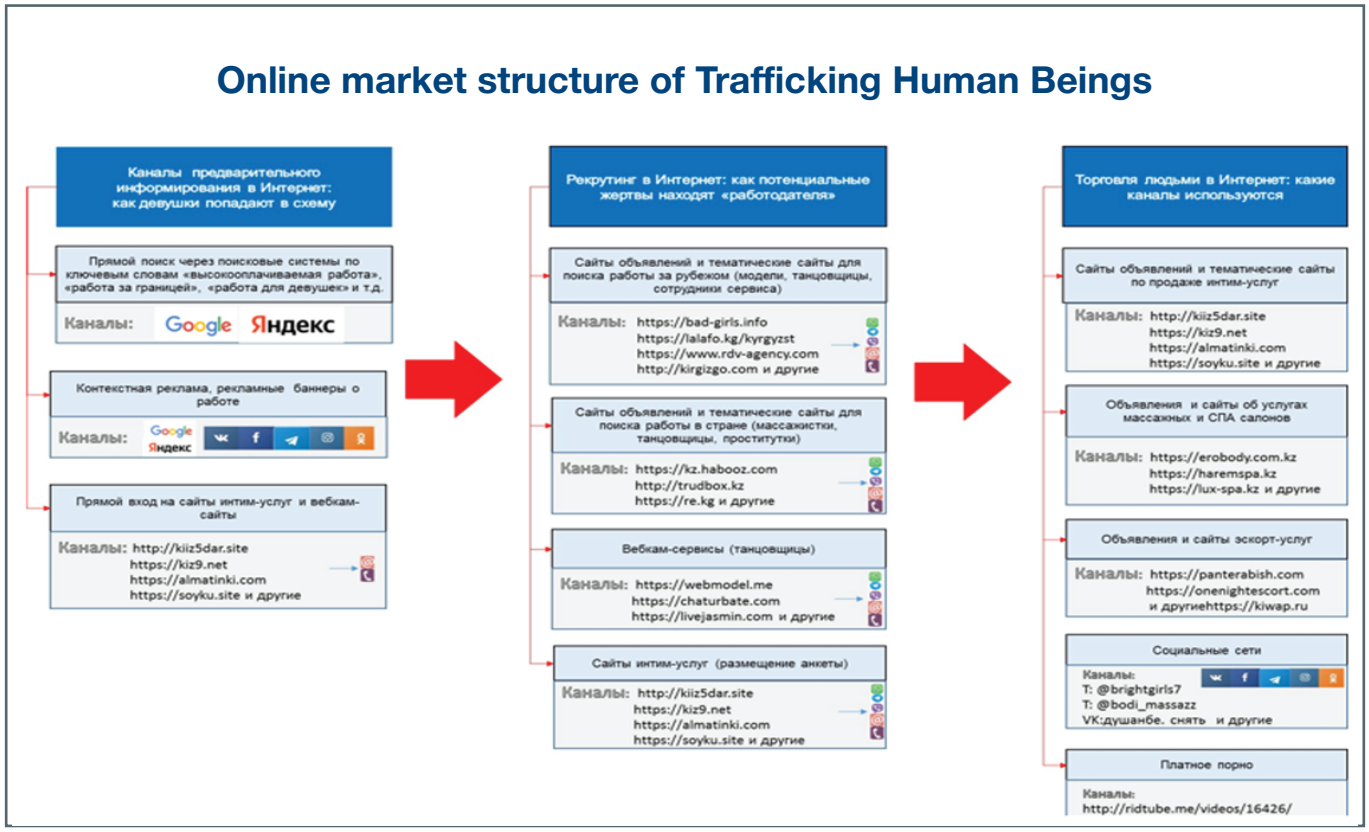
Similar to that in Japan, in the Philippines, traffickers start out by connecting with victims through social media, then move to a text messaging platform or app. A **typical trafficker in the Philippines is primarily financially motivated, female**, and often in her late 20s looking for money; whereas the typical offender is an older male and has a sexual interest in children. In the Philippines, **the use of mainstream money remittance agencies is common** - these platforms enable the transfers of money from another country (often from the offender's country) into the Philippines (and into the traffickers' accounts).

In one specific case of an offender who requested and directed explicit violent sexual abuse of multiple young victims (including those who were just 12 and 13 years old), the offender, over the course of about 10 years,

sent approximately $130,000 from the US to the Philippines **in very small transactions, which unfortunately went undetected** until a social media platform filed their cyber tip line reports investigating/revealing his case.

In Central Asian countries, including Kazakhstan, Kyrgyz Republic, Tajikistan, Turkmenistan, Uzbekistan, online platforms are also being used to advertise sexual services. Among the Central Asian countries, Turkmenistan had the highest prevalence of trafficking victims in 2018, with 11.2 victims per 1000 population, followed by Uzbekistan, Tajikistan, Kazakhstan, and Kyrgyz Republic. Kazakhstan, on the other hand, had the highest internet penetration percentage among the five countries, at 77.20 percent; whereas Turkmenistan ranked only fourth with 25.5 percent in 2021.

The presentations made by panellists concluded that sexual services in Central Asian countries are being offered on different types of platforms, including open web websites, social media websites and communication apps such as Telegram and WhatsApp. There are platforms focusing narrowly on national level but there are also online platforms which aggregate sexual services adds across a number of countries from the Central Asia. The volume of sexual services platforms and adds is greater in countries where there are less barriers to the Internet access and use. In most of the analysed countries, the sexual services are being provided by women, nevertheless, online platforms have been identified which advertise sexual services provided by men and trans-sexual.



In South Korea, incidents of sexual exploitation can be found on popular dating apps and platforms such as Tinder, Amanda, Noondate, GLAM, HelloTalk, OkCupid, Badoo, etc. Coupled with the proliferation of dating apps and platforms, the internet infrastructure, namely easily accessible and high-speed internet in South Korea was also considered by the speakers as providing an enabling environment for traffickers.

The speakers concluded by highlighting certain areas and opportunities for tech improvement, namely in **detection** and **reporting**. The tech sector is reportedly already detecting and reporting the illicit contents circulated on their platforms, which, in some cases, led to a high volume of cyber tipline reports flowing to nearly every country in the world. The speakers therefore **advocated for an increase in detection** of not only known images and materials, but **especially of the new contents**. The earlier the new materials are identified, and consequent interventions take place, the less harm and abuse are done to the victims. In other words, stakeholders should not wait for images to be recovered by law enforcement before they are added to the databases, and then subsequently identified – they could be proactively identified as new material with the help of technologies such as image classifiers, artificial intelligence, or machine learning algorithms.

Concerning reporting, although reporting regimes vary across the world in different countries, companies are highly encouraged to voluntarily **report all the information that they are lawfully allowed** to. Similarly, governments are recommended to consider **mandating increased levels of reporting**, where those requirements don't currently exist. Finally, reiterating recommendations from panel 1, the speakers emphasized the importance of collaboration, especially of establishing multi-sectoral partnerships with technology companies, service providers, the private sector and academia.

Recommendations:

1. Develop a systematic process of mapping of online platforms with high risks of THB in order to have the awareness of where THB is taking place online and develop efficient responses to the problem;
2. Engage academia, anti-trafficking NGOs and survivors in the process of identification and mapping of online platforms with high risks of THB and share information with the relevant stakeholders;
3. Establish and foster awareness, alignment of efforts and partnerships with the private sector, especially with technology companies, to combat tech-facilitated THB;
4. Establish and foster awareness, alignment of efforts and partnerships with academia and civil society, who could provide expertise and support in conducting research, collecting data, evidence, and victim assistance;
5. Develop data-driven, evidence-based policies and strategies in consultation with other stakeholders;
6. Leverage technologies such as image classifiers to increase the detection of new illicit materials;
7. Mandate increased levels of reporting for technology companies who provide online messaging / communication / social media / data storage, transfer and hosting platforms, apps and services.

PANEL 3

Existing practices in the OSCE area in addressing technology-facilitated THB

In panel 3, panellists discussed existing practices in addressing technology-facilitated trafficking in the OSCE area and across the OSCE Asian Partners for Co-operation. If in panel 1 and 2 speakers identified the trends, specific characteristics of technology-facilitated trafficking in human beings, as well as the specific tools and online platforms used by traffickers and offenders; speakers in panel 3 and 4 shared existing and good practices (including from an operational/policy standpoint, on protection frameworks and criminal justice system) from their countries' contexts and specifics, and discussed potential solutions / areas for collaboration and improvement.

The panel was moderated by **Mr. Radu Cucos**, Associate Officer on CTHB, the Office of the OSCE Special Representative and Co-ordinator for Combatting Trafficking in Human Beings (OSR-CTHB). Among the panel speakers featured **Mr. Alexandr Panasenko**, Ministry of Interior Affairs of Belarus, **Ms. Jessica Harrison**, Operations Manager, Modern Slavery and Human Trafficking Unit, Threat Leadership Command, UK National Crime Agency, **Ms. Eneli Laurits**, Northern Prosecutors Office of Estonia, and **Ms. Eiko Sudo**, International Organization for Migration Tokyo.

Prior to sharing their countries' specific practices and approaches to technology-facilitated trafficking in human beings, panelists reiterated panel 1 and 2's discussions and key findings, highlighting the similar patterns, methods and the use of digital tools and technologies by traffickers which were observed and reported in their respective countries. Concerning the use of tech and online platforms in human trafficking for sexual exploitation, legal adult service / dating / escort websites and messaging tools and transport / accommodation booking apps are among the most popular tools and virtual places for sexual exploitation reported in Belarus, the UK, Estonia, and Japan.

Panelists underlined the **importance of multilateral and multi-stakeholder collaborations and initiatives** in combatting the crime. Examples highlighted include the Child Rescue Coalition's Child Protection System (CPS)[5] and INTERPOL's Child Sexual Exploitation (ICSE) database, both developed to support and train investigators and law enforcement agencies in analysing and comparing child sexual abuse images, in identifying and indexing millions of IP addresses linked to the sharing of such abuse materials as well as help with victim identification and rescue worldwide.[6]

Although legal adult service websites are reportedly used by traffickers and offenders to advertise, communicate with and exploit victims, speakers addressed that the **majority of advertisers are not victims of exploitation** but rather, independent people in prostitution who could gain some safety benefits from these sites, such as the vetting of customers and support services offered by the sites. Therefore, some speakers stated that **shutting down these sites will not stop the exploitation of victims**, but rather, it will **displace the problem elsewhere** as traffickers and offenders can create and adopt new advertising platforms, or move to another jurisdiction, or in some cases, revert to more discrete and hidden locations and platforms such as member-only forums, illicit marketplace on the dark web, making it more difficult for investigators to discover and trace. Furthermore, such short-term actions could even risk doing harm to the people in prostitution who are relying on these sites for livelihoods and certain safety measures which they offer.

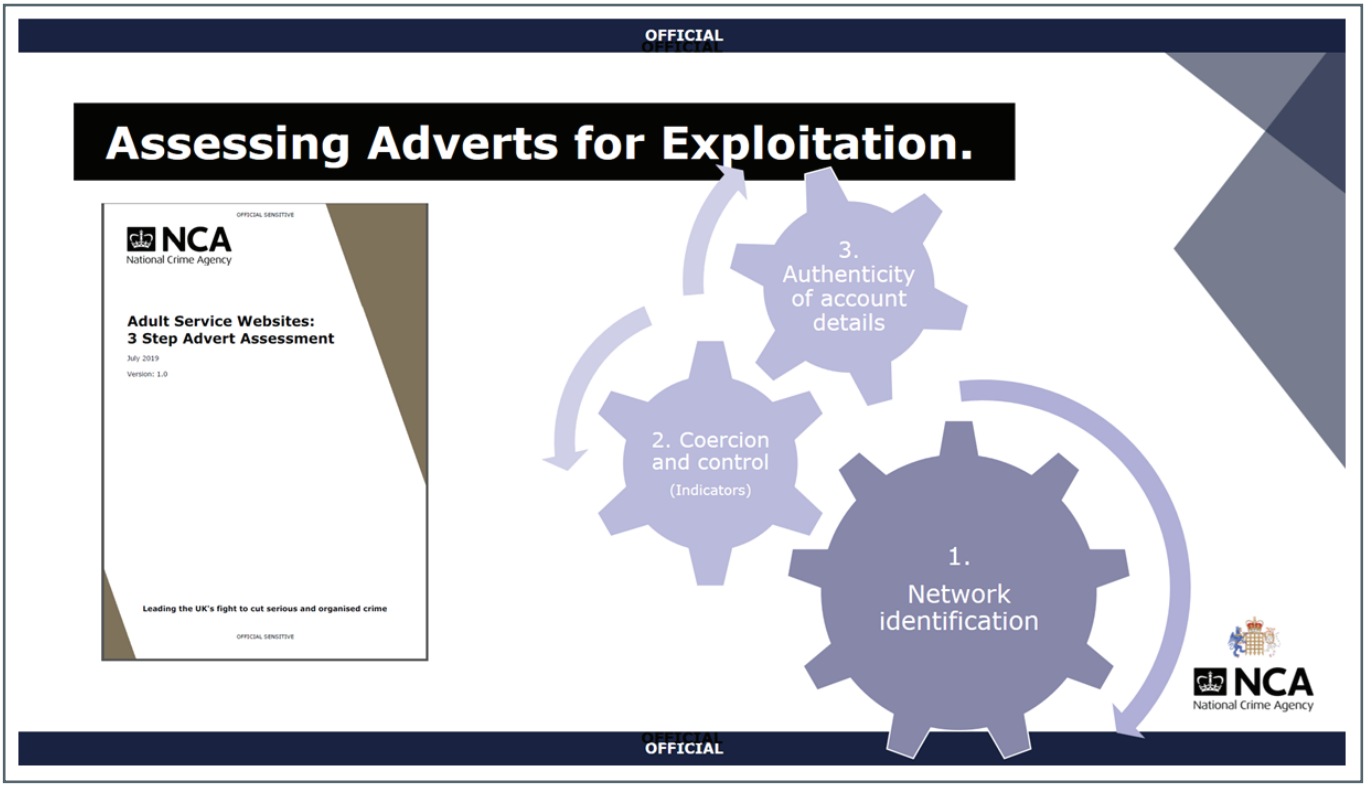
It is, however, equally important to recognise the **enabling role of these websites**, where the links and connections with sexual exploitation are frequently reported. Many of these websites in fact do not have safety measures, adequate monitoring and reporting mechanisms in place, thus endangering the safety of their users, especially of the people in prostitution who are relying on them.

[5] For more information, refer to https://childrescuecoalition.org/law-enforcement/
[6] For more information, refer to https://www.interpol.int/en/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database

The UK's largest adult service websites, such as adultwork.com and vivastreet.com, are being reported as the most targeted platforms by UK trafficking criminals who seek the mass markets to maximize bookings and therefore profits. These adult service websites have, in other words, play a key role in enabling traffickers to expand their 'clients'/ offenders' bases, and thus, increasing the criminal activity's marketplace and outreach in general. Furthermore, traffickers have been observed to **mimic behaviour of legal people in prostitution and their adverts** to conceal from investigators as well as to appeal to the mass market, thus making it challenging for law enforcement to identify and capture them.

Some examples of good practices and collaborative approaches taken by the OSCE countries and Asian Partners for Co-operation include the UK government's development of online platform regulations under the upcoming Online Harms Bill, under which the adult service websites are being considered to be included and regulated; the collaboration between the Estonian prosecutors and online booking platforms such as Booking.com and Airbnb, which supports the investigations and prosecution of trafficking cases; and the Japanese government's efforts in raising public awareness through the dissemination of campaign posters and leaflets, informing the vulnerable and high-risk groups of the threats and risks of trafficking in human beings for sexual exploitation on online social media platforms and messaging / communication apps.

The UK's NCA has also developed a set of indicators and guidance on how to assess and identify networks of adverts which might indicate elements of trafficking, coercion and control. Examples include the **high and sustained volumes of payments over time**; multiple individuals being advertised by a single account; multiple accounts linked by the **same phone numbers, usernames, or IP addresses**; or the presence of **identical adverts** under different individual names.[7]



In addition, in Estonia, law enforcement agencies and prosecutors collaborated with their online platform and service providers, such as the online booking apps mentioned above and the adult service websites, to identify suspicious accounts and adverts, as well as to track the IP, DNS addresses and mobile phone numbers of the traffickers behind those accounts and adverts. This partnership effectively helps shed light on the involvement of larger organized crime groups, who would oftentimes use the same mobile phone number or IP addresses to create, control and post several accounts and adverts.

Identifying and targeting criminal networks, traffickers and offenders making use of these sites would therefore pose the least risks to victims as there is **less displacement.**

[7] These indicators should be considered collaboratively. Furthermore, some indicators imply a greater level of risk and harm than others – among which is the young age of the advertiser / individual.

This approach also helps reduce the adverse effect on the business models and safety of legal independent people in prostitution using the sites.

Given the aforementioned challenges, lessons learnt and sharing of good practices, speakers recommended a comprehensive, four-way approach: (i) **regulate online platforms** and encourage adult service, dating and escort websites, internet service providers and the tech industry to **raise their standards** in terms of implementing and investing in monitoring and safeguarding mechanisms (including the use of tech such as policing algorithms) to create barriers for the illicit use of their platform; (ii) **cultivate strong but appropriate working relationships with the adult service website industry** to encourage proactive reporting, early interventions as well as to acquire necessary data and evidence for the identification and rescue of victims, as well as for the prosecution of traffickers and offenders;[8] (iii) **leverage the use of technologies** such as web scraping and machine learning tools, which help to **accelerate the identification** of control elements and mass advertisements created by criminal networks, as well as to **gather evidence** and **launch victimless prosecutions** and proactive safeguarding operations; and (iv) **address the demand** side by educating the users / customers of such websites - those paying for sex need to think about whether they are engaged in a criminal offence with a trafficked victim.

Speakers further emphasized that, stakeholders should **employ such tech tools with precautions**, since the use of prescriptive indicators and automation might **risk bringing up false positives**, which may distract from the identification of genuine victims.

Recommendations:

1. Leverage and build on the existing multilateral and multi-stakeholder collaborations and initiatives such as the Child Rescue Coalition's Child Protection System (CPS) and INTERPOL's Child Sexual Exploitation (ICSE) database;

2. Regulate online platforms and encourage adult service websites, internet service providers and the tech industry to raise their standards, implement monitoring and safeguarding mechanisms to create barriers for the illicit use of their platforms;

3. Cultivate strong but appropriate working relationships with the adult service website industry to encourage proactive reporting, content moderation, early interventions as well as to acquire necessary data and evidence for the identification and rescue of victims, as well as for the prosecution of traffickers and offenders;

4. Leverage the use of technologies which help accelerate the identification of advertisements created by criminal networks such as web scraping and machine learning tools;

5. Consider the use of tech tools as one source within a multi-layered approach to law enforcement data collection and intelligence development and ensure that practitioners are reviewing and are assessing the information collected and produced by tech tools;

6. Address the demand side by informing the users / customers of adult service websites with educational and awareness-raising public campaigns;

7. Partner with the financial institutions and banking sector to identify and intercept the illicit flows of criminal proceeds being moved through the legal financial channels;

8. Organize systematic capacity building activities for criminal justice and other CTHB practitioners on tech-facilitated THB and facilitate co-operation between cybercrime and CTHB law enforcement authorities.

[8] The UK examples showed that, engagement with the adult service website industry has helped lead to an increase in some safety measures from the market leaders, such as enhanced registration and verification checks, as well as the implementation of traceable payment methods. Some market leaders have in house moderation teams that remove adverts that they believe to be linked to criminality; whereas the others have been instructed to report any concerns of exploitation or wider offending to law enforcement.

PANEL 4

Leveraging policies and legislations to combat technology-facilitated THB

The last panel discussed examples of policies and legislation used and leveraged to combat technology-facilitated trafficking in human beings. The panel was moderated by **Mr. Radu Cucos**, Associate Officer on CTHB, the Office of the OSCE Special Representative and Co-ordinator for Combatting Trafficking in Human Beings (OSR-CTHB). Among the panel speakers featured **Ms. Haley McNamara**, Director, International Centre on Sexual Exploitation, **Mr. Hisashi Mochizuki**, Assistant Director, Cybercrime Division, Community Safety Bureau, National Police Agency, Japan, and **Ms. Alexandra Carra,** Cyber Department in the Attorney General's Office of the Ministry of Justice of Israel.

Speakers began the panel by reiterating the widespread misuse of technology in trafficking in human beings for sexual exploitation in all corners of the world, thus urging governments, prosecutors, law enforcement agencies and the private sectors to take stock of its harmful impacts, especially to **revise and update** their public / corporate policies, legislations and operational procedures and guidelines accordingly and on a regular basis.

The panellists reaffirmed that profits and economic motivations are the main driving forces behind trafficking in human beings. The traffickers are financially motivated to exploit victims – and they could do so effectively including by capitalising on the gaps and loopholes currently existing in the legislations, corporate policies, as well as in the limited safety and safeguarding components (or the lack thereof) in the online platforms, tools and services which are publicly available and accessible to everyone, including the traffickers, offenders, victims and vulnerable groups.

Furthermore, speakers highlighted that companies, including technology companies, online platforms, and service providers, are **profit-driven in today's political and economic structures and systems**. This has contributed to monitoring, reporting, safeguarding, and safety measures in such tech tools, communication apps and online platforms oftentimes being **developed as an afterthought** in not only new tech start-ups but also established multinationals.

In order to effectively address these challenges, speakers advocated **increasing accountability** and **liability for digital platforms and applications from the tech sector**. Speakers reiterated that the **current onus is placed on the users or parents of the underaged users** of these digital, networking and social media platforms (for examples parents would have to proactively turn on website protection filters in their children's computers). This onus was argued **to incentivise lack of meaningful content moderation** from the website operators and tech service providers.

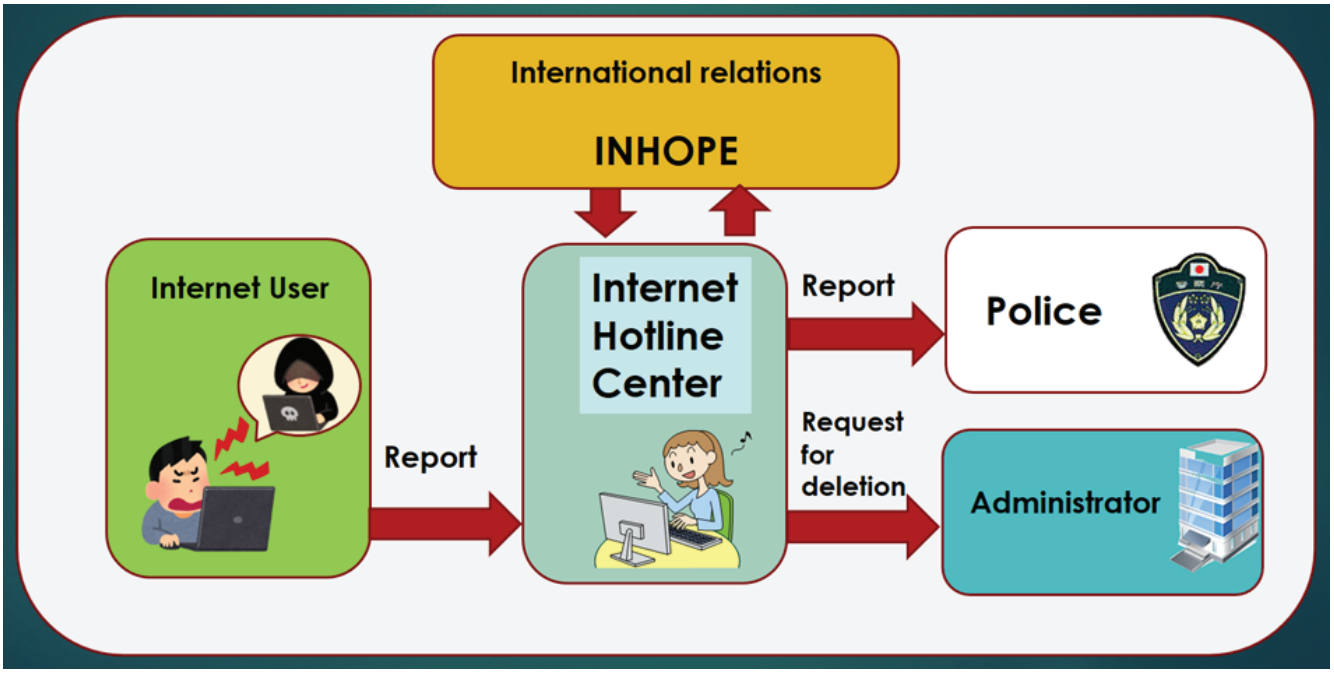
There are nuances and **differences in countries' approaches** in terms of national legislative and policy initiatives and mechanisms addressing technology-facilitated trafficking in human beings for sexual exploitation. Examples range from the UK National Crime Agency's approach in raising the industry standards, good practices and going after the traffickers and criminal networks making use of these platforms (as discussed in panel 3), to the US and Israel's approach in shutting down the platforms reported of facilitating trafficking in human beings, or in allowing website operators to remove contents deemed illicit / inappropriate and thus, protected from liability related to such contents. Examples include the FOSTA-SESTA legislation (the Allow States and Victims to Fight Online Sex Trafficking Act and Stop Enabling Sex Traffickers Act) and the EARN IT Act (Eliminating Abusive and Rampant Neglect of Interactive Technologies Act) which were passed and proposed respectively by the US as an attempt to remove liability protection from the section 230 of the Communications Decency Act of 1996,[9] as well as to impose penalties on the owners and operators of the platforms facilitating trafficking and to remove illicit contents in 2018 and in 2020 respectively.

[9] For more information, refer to https://www.congress.gov/bill/115th-congress/house-bill/1865

In Israel, the government applies and extends the existing substantive penal code to human trafficking offences committed online or via social media, websites and online platforms. Under the Powers to Prevent Online Offences Act (2017), and as an attempt to prevent the continuation of the criminal activity, the Cyber Department in the Attorney General's Office of the Ministry of Justice has also established the 'Forcing Channel', which can issue warrants to Israeli ISPs requesting them to block access to websites containing illicit materials depicting sexual exploitation and abuse.

Other examples of coordinated public efforts to counter technology-facilitated trafficking for sexual exploitation include Japan's Internet Hotline Center - managed by Japan's National Police Agency and in collaboration with the INHOPE network,[10] the center receives reports from internet users, which they will then collaborate with website administrators to remove such illegal contents.

Harmful Information on the Internet



Concerning the private sector's perspectives, raising the industry standards **can start with implementing simple features and safety measures** which help reduce abuse when enacted. Speakers gave the examples of setting up strong account creation criteria for users in social media and communication platforms; enabling age verification mechanisms or mechanisms to prevent the re-uploading of the same illicit and abuse materials to the adult service / dating websites once removed; including safety by design defaults for users under 18 years old on social media platforms, which automatically help with, for example, default activation of privacy settings for discoverability data collection, and geo location being turned off, etc.

[10] INHOPE is made up of 46 hotlines around the world that operate in all EU member states, Russia, South Africa, North & South America, Asia, Australia and New Zealand. They support hotlines and their partner organisations through training, best practices, quality assurance and staff welfare. More information at https://www.inhope.org/EN

Speakers stressed the need for policymakers and law enforcement agencies to **collaborate with the technology industry, child development experts, parents, survivors of online sexual exploitation to draft and develop policies**, safeguarding mechanisms and good business practices for the tech sector, especially those operating and providing online platforms and communication apps and tools. Furthermore, speakers emphasized that relying on complaints from the population might not be the most effective approach - many survivors reportedly did not come forward to disclose their abuse, partly due to the fear of being re-targeted by traffickers or revictimized in the justice and testimonial process. In addition to enabling an environment where victim testimony is not required / needed for case investigation and prosecution, speakers advocated for **a systematic promotion of proactively initiating inspections and investigation** by the enforcement entities as distinct from the reliance on complaints to trigger enforcement action.

Recommendations:

1. Collaborate with the technology industry, child development experts, parents, law enforcement, survivors of online sexual exploitation to draft and develop policies, safeguarding and reporting mechanisms and good business practices for the tech sector, especially those operating and providing online platforms and communication apps and tools;

2. Draft and enact policies which require greater accountability and liability from online platforms and developers/users of digital tools;

3. Mandate the online, social media platforms and service providers to implement reporting, grievance and support mechanisms and channels in their platforms, services and tools, which allow users to report on illicit, non-consensual and abuse materials, as well as to get proper support in time when faced with / placed in an abusive situation;

4. Promote a systematic approach of proactively initiating inspections and investigation by the enforcement entities as distinct from the reliance on public complaints to trigger enforcement action;

5. Develop policies and frameworks which enable victim-less investigation and prosecution, to prevent survivors from being re-victimised by recalling / having to give testimonials on their past abuse and trauma.

CLOSING REMARKS

Closing remarks were delivered by **Mr. Valiant Richey**, OSCE Special Representative and Co-ordinator for Combating Trafficking in Human Beings.

The Special Representative highlighted that, while each country has its own nuances to this problem, its own country-specific challenges, counterstrategies, and approaches, there is a **broad similarity in the nature, characteristics, and trends of the issue** across the OSCE and the OSCE Asian Partners for Co-operation from the roundtable discussions. This reminds us that **when we have common problems, we can develop common solutions**. Furthermore, given the transnational and border-less nature of tech-facilitated trafficking in human beings, **multilateral and multistakeholder collaborations are required** and needed to develop such solutions and counter-approaches.

The Special Representative reiterated the importance of **data driven policy development and operational programmes and activities**. The discussions gave a good general overview of the digital and social platforms and tools, and of the nature of the challenge and how traffickers operate. However, this information should be further tested, explored and used to develop informed and evidence-based policies and counter-strategies and efforts.

The Special Representative urged governments and policymakers to **strengthen policies oriented towards the private sector**. In the context of trafficking for labour exploitation and due diligence laws, there has been evidence that suggests that **voluntary compliance does not work on a large scale**. Countries are therefore encouraged to start engaging and **collaborating with the private sector** at the national level, while ensuring mandatory compliance with those provisions.

The Special Representative questioned if legislations and policies should be based on whether companies had had prior knowledge of specific instances of violations and abuse within the services and platforms which they offer and operate. Only holding online platforms and service providers accountable for their knowing of specific instances is arguably problematic, as with this, **we might incentivize** the lack of knowledge and more importantly, **incentivise the lack of meaningful content moderation** from the tech sector.

The Special Representative highlighted the **need to incentivize rigorous content moderation**. Self-regulation by these platforms has been proven to not be efficiently working. Preventive protections should be mandated to prevent negligence.

Finally, the Special Representative urged countries and law enforcement agencies to move beyond the case-based perspective at the national and international level **to a market-based perspective**, where the overall market and demand side are carefully addressed to tackle the problem at its roots.

The Special Representative offered his Office's support and technical assistance to the participating States and Asian Partners for Co-operation in responding to the call for action and in designing and implementing effective strategies to prosecute traffickers and deliver justice to victims.

OSCE Secretariat
Office of the Special Representative and Co-ordinator
for Combating Trafficking in Human Beings
Wallnerstrasse 6
A-1010 Vienna, Austria

E-mail: info-cthb@osce.org

Organization for Security and
Co-operation in Europe