19th *ALLIANCE AGAINST TRAFFICKING IN PERSONS* Conference
Using Technology to Combat Trafficking in Human Beings: Turning a Liability into an Asset
8-9 April, 2019

Excellencies,

Let me start by thanking the OSCE for inviting me to the 19th Alliance against Trafficking in Persons Conference. I particularly appreciate the opportunity to participate in this year's conference as the topic of Technology plays an ever-increasing role in our private and professional life's. Human trafficking is no exception in this development.

*Many technological developments, can easily be misused - in our case to facilitate trafficking in human beings - but we should not ignore that they can also be used in positive ways by various actors dealing with combatting human trafficking to fight this heinous crime. I believe this conference is a great chance for all of us gain insight & experience how to effectively combat this new form of human trafficking**. [PP 1]***

First of all, I would like to present some facts about human trafficking in Austria. We noted that in 2018 as well as in previous years, sexual exploitation was the most common form of trafficking, occurring in over 70% of the completed police investigations in this area. **[PP 2]**

In 2018, as well as in previous years, the recognized victims of sexual exploitation and cross-border prostitution were almost exclusively female. **[PP 3]**

A majority of recognized victims of sexual exploitation were also third-country nationals, meaning nationals from outside of the European Union. The main country of origin was Nigeria with 124 victims, followed by China with 33 victims. Therefore, we placed special emphasis on cooperation with Nigeria and China. **[Also PP 3]**

Nevertheless, we assume that many cases remain unreported and therefore the data collected doesn't necessarily reflect the complete picture of the situation.

For this conference, probably the most interesting fact is that the vast majority of trafficking incidents in Austria also involve technology and the Internet. The most recent data of 2017 shows that the perpetrators used online infrastructures in 74% of all investigations**. [PP 4]**

Over the past few years, Austria has detected the following major types of misuse of technology by traffickers:

- **Recruiting [PP 5]**
  - ⇨ We know that the so called "lover boy method" is one of the most common ways perpetrators use to recruit their victims. More and more human traffickers get in touch with the potential victims over the internet and various social media platforms by adding and liking their personal accounts. In order to lure them to go abroad and to be able to exploit them, they charm their victims with fake love stories and promises. This method is often used when a perpetrator wants to sexually exploit girls and women as prostitutes.

- **Advertising [also PP 5]**
  - ⇨ Even if advertising sounds self-explaining, let me give you one example: In Austria, some years ago, several women from South-East Europe were forced to check in as regular clients into hotels and subsequently had to hand over the access key-card to another person. As everything appeared normal and the hotel employees didn't ask any questions, the perpetrators advertised the victims for sexual services at various pornographic websites to potential clients who were located nearby. This was achieved by showing ads only to IP-addresses[1] that were located within a certain predefined geographical area. The client got further information by clicking on the ads and a meeting for the handover of the hotel key card was arranged.

    For me, this method is a prime example of how the internet facilitates human exploitation.

[1] Internet Protocol address (IP address) is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication.

- **Surveilling and giving instructions to the victims [also PP 5]**
  - ⇨ It is almost standard procedure that perpetrators control their victims by using technology. With today's technology it's very easy to locate a certain mobile phone remotely or video-control a certain room or door-access system remotely. *It's also convenient for a perpetrator to communicate with the victim via a messenger service tool instead of simply talking to them over the phone.*

    Open source messenger tools are all Data- and not speech based, they are typically end-to-end encrypted and for law enforcement, it is much harder to interfere this kind of communication than a simple phone call. Additionally, if the perpetrator deems it necessary, he can easily threaten the victim, but also clients of the victim, with the publication of certain pictures or chat-protocols he received over time. By doing so, the perpetrator may gain additional revenue or the cooperation of the victim and the client of the victim.

- **Communication between the perpetrators [also PP 5]**
  - ⇨ As for the communication between perpetrator and victim, we also experience that the communication between perpetrators shifted to open source messenger tools. They are cheaper but most importantly much harder for law enforcement to track than phone calls.

Apart from these already quite established types of misuse, we have identified a few new trends I also want to share with you: [PP 6]

- using NFC-Codes[2] (a Mobile phone-based system used mostly for payment solutions) to take over full control of the payment transaction between the customer and the victim.
  - ⇨ Systems like Apple Pay, which are launched right now in Austria, are monitored closely by law enforcement concerning their implications in human trafficking situations.

[2] Near Field Communication (dt. Nahfeldkommunikation, abgekürzt NFC)

- transferring profits by use of Bitcoins, other virtual means of payment and prepaid credit cards. **[also PP 6]**

    - ⇨ Even if digital currencies like Bitcoin are much talked about, Austrian law enforcement learned that simple prepaid cards are used much more frequently as a digital payment option.

- organizing accommodation (online ads, chat forums and emails are used to find flats and "jobs" for exploitation): **[also PP 6]**
    - ⇨ The use of various accommodation-sharing platforms is also investigated by Austrian police from a human trafficking perspective. It is important to create an understanding in Austrian society, that these technological platforms can be used for criminal activities like Human Trafficking and that a potential host is aware of what to do and what the legal implications are if he becomes part of a human trafficking investigation.

By examining the prior trends and numbers, the question arises: what are the major enablers that allow traffickers to misuse technology in those kinds of ways? [PP 7]

In recent years, the use of the Internet and social media created more complex criminal processes. The legislation and judicial practice do not always timely respond to technological changes, resulting in legal gaps and the general difficulty of gathering legal evidence, which makes it difficult to prosecute most types of cyber-crime.

It's just a matter of fact, that every state can only react with new laws and regulations to a technological development after it has been developed, tested and put into use. Therefore everything we do in the legislative sector is always – at least – one step behind the technological development.

However, even though this new ways of misusing technology seem to be a full-scale problem, Austria is very optimistic to find ways on how to prevent, combat and prosecute these new ways of human trafficking. We have taken already serious steps, particularly with regard to the international aspect of the challenge.

On an operational level, creating the Joint Operational Office (JOO) against Human Smuggling and Human Trafficking within the Federal Bureau for Criminal Investigations, gave our abilities for international cooperation a substantial push. **[PP 8]**

Let me give you two examples about what the JOO can do in cooperation with other states:

  - *In May 2017 six investigators from China supported the JOO in investigations against Chinese offender groups.*

  - *In December 2017, an operational working meeting took place in Abuja, Nigeria. In addition to discussing the further common approach with (National Agency on the Prohibition of Trafficking in Persons) the team also met with the European Liaison Officer in Nigeria for migration and human trafficking, with representatives of the Nigerian Ministry of Justice and Nigerian Foreign Ministry.*

Creating a Joint Operational Office, which includes law enforcement officials from various states from different continents, does not sound very "technological" of first-hand, but the added value must not be underestimated.

By ensuring that officials from various states, who have all access to their national data bases, sitting next to each other in a Joint Operational Office, a lot of red tape can be cut. Investigation proceedings can easily be simplified, by just talking to each other, informing each other about national results and cross-referencing results with the database of the colleague sitting on the other side of the table.

Last but not least, I would like to share our lessons learned from the past and I allow myself to make comments that could be useful in the future: **[PP 9]**

- Training, research and more involvement are the first steps to end misuse of technology
  - ⇨ A few weeks ago a conference named "*How to cope with the misuse of modern technology*" took place in the Ministry of the Interior in Vienna. Relevant stakeholders from all over Europe joined this event including Air BnB Europe and Facebook Europe Senior Executives. These platforms hold crucial positions in the context of misusing online services for criminal processes such as human trafficking.

The event was a successful example of implementing new ways of improvement to deal effectively with these modern technological techniques.

- It is essential to cooperate not only with Human Trafficking related bodies, but to create knowledge about Human Trafficking within organizations dealing with cyber crimes and banking regulations.

  A close cooperation with Financial Intelligence Units from state agencies or private actors typically help to identify financial transactions that may involve tax evasion, money laundering or some other criminal activity such as payments for victims of Human Trafficking.

  ⇨ *To give you an example: public-private cooperation, I would like to mention the close and essential cooperation between the Financial Intelligence Unit of Western Union and law enforcement. If there are certain suspicious transactions registered by Western Union, the police can use and benefit from this transaction data, which might lead to the core of criminal structures.*

- *Given the sophistication of the technology used by traffickers, States should attempt to ensure that their laws are up to date and can address these issues*
- Understand that just because you don’t see trafficking on your streets, doesn’t mean it isn’t happening; there is a robust online system of exploitation!

Thank you all very much!