

# OSCE ROUNDTABLE REPORT

© olly - Fotolia.com  
#36136663

VIENNA, AUSTRIA  
9-10 NOVEMBER 2020

Leveraging Innovation and Technology to Address 21<sup>st</sup>  
Century Security Challenges and Crises across the OSCE  
and Asian Partners for Co-operation.



## ANALYSIS

Discussion and analysis of the complex challenges currently being faced, as well as sharing best practice and innovative approaches.

LEVERAGING TECHNOLOGIES



## ENGAGEMENT

Opportunities for engaging with experts and building your network for enhancing international co-operation and collaboration.

STRENGTHENING CO-OPERATION

## ABOUT TNTD BSMU

The Border Security and Management Unit of the OSCE Transnational Threats Department supports OSCE participating States and Partners for Co-operation to address emerging border security risks and challenges.

# REPORT

*Leveraging Innovation and Technology to Address 21st Century Security Challenges and Crises across the OSCE and Asian Partners for Co-operation.*

Analysis of the complex security challenges, currently being faced, as well as sharing best practices and innovative approaches was the focus of the OSCE roundtable discussion. The event titled “Leveraging innovation and technology to address 21st century security challenges and crises across the OSCE and Asian Partners for Co-operation” was held on 09 and 10 November 2020 online and in Vienna. Organized by the OSCE Border Security and Management Unit/ Transnational Threats Department, the Slovak Chair of the OSCE Asian Partners for Co-operation Group, the OSCE Border Management Staff College, and the OSCE External Co-operation Section, the discussion gathered some 180 participants from the OSCE region and beyond. This roundtable discussion was the first of its kind and was held in the context of the 25th anniversary of the OSCE Asian Partnership for Co-operation. (<https://www.osce.org/secretariat/469806>).

## IMPACT OF COVID-19 PANDEMIC ON TRAFFICKING IN HUMAN BEINGS - SHARING INNOVATIVE PRACTICES OF PREVENTING AND COMBATING HUMAN TRAFFICKING ACROSS THE OSCE AND ASIAN PARTNERS FOR CO-OPERATION

**Trafficking in human beings is one of the most pressing and complex crimes in the OSCE participating States and Asian Partners for Co-operation. Human trafficking, whether for sexual or labour exploitation, is a very complex crime to detect in ‘normal’ times. The coronavirus pandemic made the investigation of human trafficking cases even more challenging pushing victims further from possible detection and assistance. The complexity of obstacles associated with combating this crime means that anti-trafficking actors have to adopt innovative measures in order to effectively overcome them. During this session, the participants discussed how new technology tools could prevent and counter human trafficking by detecting both offenders and victims. The panel elaborated on how co-operation among OSCE pS and Asian PFC on countering human trafficking can amplify shared expertise on addressing this major security threat.**

**Moderator:** Mr. Valiant Richey, OSCE Special Representative and Co-ordinator for Combating Trafficking in Human Beings

- Ms. Noriko Kishida-Kiyotani, Programme Manager, International Organization for Migration (IOM) Tokyo, Japan
- Mr. Steve McGlynn, Minister-Counsellor Geneva, Department of Home Affairs, National Resilience and Cyber Security Group, International Policy Division, Australia
- Mr. Nenad Naca, Team Leader – AP Phoenix (THB), European Migrant Smuggling Centre (EMSC), EUROPOL
- Mr. Mohammad Amran Sahak, Customs Department, Afghanistan

## SUMMARY - MR VALIANT RICHEY

The impact of COVID19 and its intersection with THB has had a disproportionate effect on the most vulnerable. Victims of trafficking find themselves increasingly with fewer options for survival and simultaneously less protection because of closure of services.

The impacts include a surge in online exploitation and enforced criminality and an increase in child labour and child marriage.



Before COVID only one trafficker for every 2300 victims was being prosecuted, this figure is expected to grow substantially in the coming months and years.

The pandemic is not a time to turn away from combating human trafficking, but a time to invest in its prevention and eradication. As borders remain closed and movements restricted due to the pandemic traffickers have moved online to secure their revenue secure greater anonymity and subsequently enhance their impunity.

In a comparative report from just four countries, researchers concluded that technology has become the single greatest facilitator of the commercial sex trade and all of the countries observed. However, the report was undertaken 13 years ago.

Europol concludes that the online advertisement of sexual services is an increasing phenomenon relating to trafficking of human beings for sexual exploitation, with children being advertised as adults.

In Southeast Asia online platforms, facilitating live streaming of children are associated with an increase in child trafficking, resulting in an estimated three to \$20 billion a year in profit.

In Austria, the internet was used as the most common criminal infrastructure by perpetrators in 74% of human trafficking cases.

Initial reports from countries measuring online exploitation increases from a year ago:

- Australia 50%
- Canada 81%
- United States 109%
- Philippines 300%

OSCE has documented over 300 technology tools that can assist law enforcement civil society and policymakers in combatting THB

**References:** Leveraging Innovation to Fight Trafficking and Human Beings - [https://www.osce.org/files/f/documents/9/6/455206\\_0.pdf](https://www.osce.org/files/f/documents/9/6/455206_0.pdf)

## JAPANESE CONTEXT - MS. NORIKO KISHIDA-KIYOTANI

The number of migrant workers has more than tripled in the past 10 years. COVID19 has led to a disproportionate loss of jobs amongst the migrant community making them more desperate and vulnerable.

70% of THB victims in Japan are foreigners. Victims of THB in Japan are predominantly females from Southeast Asia brought to Japan for sexual exploitation. Currently, there is no clear indication of increase or decrease or human trafficking cases reported in 2020.

### Good practices of Coordination

IoM has been provided technical support to Japanese Airlines (ANA) since 2018. In 2019 ANA established a reporting system to Japanese immigration of suspected trafficking victims. All crew have been trained on the system.

*Immigration and Police identify victims without determining perpetrators (victim identification is independent) and refer them to supporting agencies such as designated shelters and the IOM.*

### Conclusion

The capacity to detect/identify/refer victims could be expanded. For instance:

- Labour standard inspection offices
- Industries employing migrant workers such as hotels and airlines





Before the next Japanese national action plan revision expected in 2021, studies on the impact of pandemic or human trafficking could be useful. Coordination with various sectors need to enhance the significant tree to eliminate human trafficking in Japan.

## AUSTRALIAN CONTEXT - MR STEVE MCGLYNN

THB is a crime that transcends borders. THB crime that will evolve to the to the form of most convenient to the perpetrator and offers the least risk profile. Online and social media platforms offers criminals important tools, especially encrypted communications.

The Australian Government worked in partnership with industry stakeholders, in the development of regulation and a framework for cooperation. The government has worked directly with ISP and social media outlets and other information holders. The idea that is industry works with government on a voluntary basis, but this backed by regulation.

*"We call it a technical assistance requests and in essence, it was a request that detailed the person or if you like the entity from which we are going to get the information from but also the actual information that will seeking to obtain from them."*

Legislation defines that requests any must be:

- Reasonable and proportionate
- Practicable and technically feasible
- Not subject to civil liability

A process exists where government engages with the operator to fashion the 'request' in a way that they can answer, leading to a coordinated and cooperative approach. But key to success is that industry would not be subject to civil liability.

Where industry feels unable to cooperate on a voluntary basis, regulation exists to require cooperation.

This takes the form of a Technical Assistance Notice and Technical Capability Notice:

- A Technical Assistance Notice works in similar terms to a 'Request' where certain information is required.
- A Technical Capability Notice is where the operator is required to provide the technical capability to access the information.

Protections for the operator are provided by its costs negotiator, for any costs incurred and that the provider must not be required to build or implement a systemic weakness or vulnerability into their system (a so called backdoor).

This applies not just to networks or facilities in Australia, but services that operated in Australia, had end users in Australia were manufactured supplied, installed, maintained. It should be noted that only three requests in a 12 month period, they have not as yet had to issue a notice.

This supports the idea of a successful cooperative and collaborative framework and the idea that the 'Notice' has such a high threshold that it can only be used in certain circumstances.



The Impact of COVID-19 on serious and organised crime and THB in the EU - COVID-19 outbreak and Europol response:

More people online due to restrictions has triggered sharp increase in online abuse.

Opportunities for increased exploitation of victims.

Exploiters may abuse victim in more hidden locations.

Victims may be forced to switch activity to criminal acts.

Tightening of the debt bondage of victims towards their exploiters due to the restrictions during COVID-19.

**Push factors** - increase of online activities of potential victims

**Pull factors** - Cheap Labour demand's

- Miners are very active on Internet and therefore at higher risk than before.

The impact of COVID-19 on THB for the purposes of sexual and Labour exploitation:

### **Sexual exploitation**

The prolonged closure of the establishments offering legal sex work and may increase victims vulnerability. The pool for new clients online is much greater, so victims are more likely to be exposed to be exploiting online.

### **Labour exploitation**

The restrictions on travel and the closure of borders complicated seasonal workers especially in the agricultural sector, but there is still huge demand for cheap labour, especially in unregulated industries.

### **The impact of the digital era on trafficking in human beings**

Even before COVID19 there was a trend towards the digitalisation of human trafficking because it enables increased anonymity, encrypted communications, and offers a wider audience of victims as well as clients.

Geographical displacement, meaning exploiters do not have to be in the same location as victims, but have tools for remote supervision, such as real time monitoring for example GPS localization and built in video cameras in smart phones.

### **Reducing chances of detection**

Social media enables access to knew potential victims and develop new strategies based on personal data and blackmail. New technologies have emerged that enabled new opportunities for the movement of illicit profits, whilst maintaining a low profile. Criminal networks are moving towards digital wallets, virtual banking services and virtual currencies.

### **How can law enforcement leverage technologies and innovation to tackle THB?**

If it is true that technology offers multiple benefits to criminal networks, it also provides law enforcement with tools to investigate and find leads:

#### **Digital footprints**

- The dedication of investigators to find ways to trace criminals' digital footprints with the purpose to use them in judicial proceedings
- Using their own advantage against them identity, structures of OCG, locations, roles, assets.

#### **Online Evidence**

- Different sources of evidence for example.
- Financial transactions made by the criminal to manage the proceeds.
- From uploading contents.
- Online advertisements.



The criminal may have destroyed everything on their computer or taken all the precautions on their own computer, but it is possible to find evidence via the victim's devices, and track their movements and contacts via their cell phones.

#### **Challenges for THB analysts:**

- Increase of big data
- The ever-changing model of business that criminals utilise, adapting to the development of technologies
- Adapting to new circumstances eg COVID-19 pandemic

#### **Ways Forward**

- Need for empowered and increased capabilities and improved legislative tools.
- A better use of digital evidence and footprints in the prosecutions and legal proceedings.
- More functional cooperation between law enforcement agencies and the private sector.

*If the legislative and policy framework would be amended, this would allow a more functional cooperation between law enforcement agencies and the private sector.*

International and regional cooperation is vital to tackle THB

*Fighting the THB is not only for the police or law enforcement. But if we want to eradicate it, as we are all dedicated to do, then we all have to engage in this fight. All sectors, private and government have to be involved equally to fight THB.*

Lots of opportunities for the financial sector to help in the fight against THB

*Most people think that financial institutions only hold data about a financial transactions. This is not true, they have a lot of data regarding the where people live, about the ATM machines they're using etc. So imagine if all this data could be used to recognize indicators and then proactively to identify labour exploitation. For example, at one address there are 20 people living and all 20 working for one company. They are all paid on one day and all the monies is transferred the next day. This could be an indicator of labour exploitation.*

#### **VALIANT RICHEY**

*I share precisely your analysis that this could be a game changer in the fight. The OSCE my office last year put out a paper called following the money, which in fact does exactly what you were just talking about. Highlights the number of indicators for identifying trafficking and also discusses frameworks for cooperation so we very much share your analysis. It can be useful not only to identify perpetrators identify victims, but also then seize assets which can then be used to support the recovery of victims.*

See Following the Money: Compendium of Resources and Step-by-step Guide to Financial Investigations Into Trafficking in Human Beings - <https://www.osce.org/cthb/438323>

#### **CUSTOMS DEPARTMENT OF AFGHANISTAN - MOHAMMAD AMRAN SAHAK**

- Afghanistan is a source transit and destination country for men, women and children's who are mostly subjected to forced labour and sex trade trafficking.
- Human trafficking is second only to drug trafficking in profitability
- Unemployment, poverty and war fuels trade.

#### **Routes for smuggling trafficking people from Afghanistan to Europe**

People are being transported from Afghanistan to Pakistan. From Pakistan people are further transported illegally to Iran, from Iran to Turkey then on to Bulgaria to Greece.



### **Actions undertaken by Afghan government to combat human trafficking**

Afghan government established a Commission on combating human trafficking in 2014. The Commission is comprised of 16 members from government agencies and non-government organisations and has raised the seriousness of the crime and the penalties.

106 human trafficking networks have been identified and dismantled by the National Security Agency

### **Recommendations on prevention of human trafficking in Afghanistan**

- Develop and enforce comprehensive and inclusive national strategy tracked strategies on prevention of human trafficking men women and children
- Conduct advocacy and prevention campaigns against child abuse, domestic violence, sale of children and forced marriage
- Engage extensively with media (TV and radio in particular) and journalists in prevention efforts of human trafficking.
- Further enhance border security and management by providing capacity building initiatives to border and customs officers on victims identification and their referral.
- Promote regional cooperation in countering human trafficking particularly with Iran and Pakistan on repatriation of victims, exchange of information, as well as extradition of perpetrators.

Highlighted were the risks undertaken by victims

The roles of conflict and poverty.

The role of domestic violence as a push factor

More subtle forms of recruitment for example fake romance

Trafficking routes often follow very closely migration routes

## Q&A

### **What segments of the private sector can help us?**

- Tech companies really need to consider preventing the misuse of their platforms
- They can be proactive in their initiatives by building tools or devoting resources to the effort to combat trafficking



# REPORT

*Leveraging Innovation and Technology to Address 21st Century Security Challenges and Crises across the OSCE and Asian Partners for Co-operation.*

## ENHANCING REGIONAL AND INTERNATIONAL SECURITY CO-OPERATION BY SHARING GOOD PRACTICES AND INNOVATIVE APPROACHES TO COMBAT TERRORISM IN THE OSCE AND ASIAN PARTNERS FOR CO-OPERATION.

**The panel analysed good practices, innovative tools, as well as viable mechanisms enhancing international co-operation against terrorism in the OSCE and Asian Pfc. This session underlined the importance of building a broader community network to support the prevention of violent extremism and radicalization that lead to terrorism (VERLT) and enhanced multi-agency co-ordination, including with actors beyond law enforcement and criminal justice institutions. Discussions explored how the OSCE and Asian Pfc can achieve better leverage on capacity-building programmers to effectively combat terrorism related threats. Additionally, the panel elaborated on effective mechanisms of preventing and countering the use of Internet for terrorist purposes.**

**Moderator:** Ms. Georgia Holmer, Head, Transnational Threats Department/Action Against Terrorism Unit, OSCE Secretariat

- Mr. Otabek Rashidov, Programme Officer, Transnational Threats Department/Action Against Terrorism Unit, OSCE Secretariat
- Dr. Matteo Vergani, Senior Lecturer in Sociology and Senior Research Fellow at the Alfred Deakin Institute for Citizenship and Globalisation, Australia
- Mr. Izuru Sugawara, President of Overseas Security and Crisis Management Association (OSCMA) a non-profit organization and Crisis Management Advisor to several Japanese corporations and JICA (Japan International Cooperation Agency)
- Ms. Alexandra Antoniadis, Deputy Head of Unit, European Commission, Directorate-General for Migration and Home Affairs, Law Enforcement and Security, Unit on Prevention of Radicalization
- Mr. Jisoo Han, Chief of Foreign Affairs Security Section of the Foreign Affairs Bureau, Korean National Police Agency, Republic of South Korea
- Mr. Muhammad Idrees, Independent expert, Afghanistan

## CHAIRPERSON - GEORGIA HOMER - HEADS OF ACTION AGAINST TERRORISM UNIT TRANSNATIONAL THREATS DEPARTMENT

One of the overarching themes of this roundtable today is the complexity of the security threats we face. This is particularly manifested in the realm of preventing encountering terrorism and violent extremism.

The COVID pandemic rapidly changing technology and shifting geopolitics have had a real impact on trends and transnational threats.

Violent extremist movements and terrorist organizations of all types are attempting to capitalize on the vulnerability fear and uncertainty that is generated by the pandemic to advance their objectives.



## MR. OTABEK RASHIDOV, OSCE

Violent extremists and terrorists groups are increasingly using dark web encrypted channels and anonymous sharing portals to mobilize resources train land records radicalized and insight others.

Following the outbreak of the pandemic made it evident that violent extremist organizations are seeking to capitalize on the global crisis and are rapidly to adapting to the changing circumstances. For instance by continuing to move their equipment online. There is a growing trend that terrorist networks are turning to more closed decentralized encrypted systems providing extra layers of security and anonymity.

Terrorist networks actually conduct actively financial transactions in digital world, including through crypto currencies.

We also should not underestimate the increasing possibility of the use of ICT and artificial intelligence by terrorists to advance their agenda.

### CTUI - Countering Terrorist Use of the Internet

OSCE provides support to the participating states to improve the efficiency on their nationally force to prevent and counter the use of the Internet for terrorist purposes,

Practical work in this area has several key objectives:

- Advancing the key human rights issues tied to Internet regulation with special emphasis on the need for a clear definition of terrorism, issues of data and privacy protection, fundamental freedoms of expression, religion etc.
- Fostering public private partnerships for information sharing
- Building the capacity of law enforcement and judicial actors to ensure that online investigations and prosecutions using digital evidence is conducted within the rule of law
- Promoting digital citizenship and Internet literacy to help build resilience to the influence of violent extremist groups.

### OSCE E-Learning Course (Launched May)

[https://elearning.osce.org/courses?search\\_query=counter-terrorism](https://elearning.osce.org/courses?search_query=counter-terrorism)

The E learning course is available in the English and rational languages and divided into two modules

- Module One - Explored and provides real world example. So how violent extremists and terrorists misuse the Internet.
- Module Two - How to effectively respond to these challenges in a human rights compliance and gender mainstream manner, drawing on the guidance developed on the topic, including the GCS 31 and policy to get on preventing and countering violent extremism and terrorism online.

### National Tabletop Exercises (NTTX's)

- Moderated scenario based discussions on CTUI - three days
- Participants decision makers, law enforcement, civil society, media, academia, youth and the private sector
- Major objective to produce **Actionable Policy Responses** and recommendations a pay (APRR) the keyword is "ACTIONABLE"
- APRR's are then put forward to the policymakers for **integration into grand strategies / NAP on CT**

Moderated discussions take into account context specific gender dynamics

*Within the intelligence and research communities that the gender blind approaches to countering violent extremism activities risks negative consequences in terms of failing or to detect individuals engaged in violent extremism.*

During tabletop exercises best practice guide books are extensively used.



NTTX's Develop to Actionable Policy Responses and Recommendations:

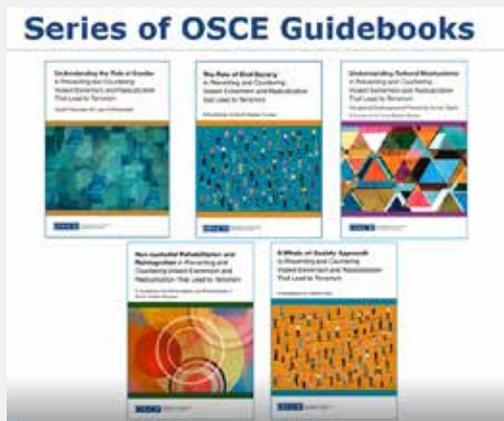
- Legal frameworks
- Public private partnerships collaboration with the global ICT industry and developing capacities of key stakeholders
- Preventing through strategic communication development of counter and alternative narratives and educational programmes

The second component is about the strengthening the prevention related work through Strategic Communications development of contract tentative narratives and educational programs.

This project is called the **Leaders Against Intolerance and Violent Extremism**.

This project addresses issues related to online dimensions of radicalization to violence as well as effective ways of involving the internet in its prevention.

OSCE Produced a Series of Guidebooks



### Future Plans – Electronic Evidence

Future plans include issues related to improving the effectiveness of the investigation of cyber enabled terrorist offenses and emphasizing the need to develop the capacity of national criminal justice to obtain electronic evidence to ensure the right individuals is persecuted and those who perpetrated serious offenses are brought to justice.

The UNODC and the OSCE are working on train the trainer programmes based on the UNODC *Practical Guide for Requesting Electronic Evidence Across Borders* - [https://sherloc.unodc.org/cld/secured/18-05840\\_Practical\\_Guide\\_Electronic\\_Evidence\\_ebook.pdf](https://sherloc.unodc.org/cld/secured/18-05840_Practical_Guide_Electronic_Evidence_ebook.pdf)

The OSCE will also launch a new initiative for digital citizenship and media literacy.

This new initiative will facilitate regional awareness campaigns to promote the message was the importance of critical thinking around all types of media and our ability to engage positively critically and compassionately in the digital environment to practice a form of social participation that is respectful of human rights and dignity through the responsible use of technology.

### Key points:

- Striking the right balance between the possibilities offered by modern technological solutions and their potential impact on societies
- Holistic balanced gender mainstreamed and self reflected approach to applying technology in addressing terrorism and violent extremism
- Transparency
- Cooperation



## DR MATTEO VERGANI, THE SOUTH EAST ASIAN NETWORK OF CIVIL SOCIETY ORGANISATIONS - SEAN-CSO - WORKING TOGETHER AGAINST VIOLENT EXTREMISM

Sharing and analysing the experience of the Southeast Asian network of civil society organisations, SEAN-CSO is a network of like-minded organizations and people. It comes from the 2015 Sydney Countering Violent Extremism Summit and as endorsed by regional governments and it is funded by the Australian Government

*The main focus of the network is to share knowledge and best practice to build capacities, especially on specific topics such as evaluation or of CD activities or research fundraising and mentoring.*

It has the members with different skill sets and some more experts can mentor more junior members. The organisation has over 60 members across five main states Indonesia, Malaysia, Philippines, Thailand and Australia but also some members from Singapore, Myanmar and Bangladesh

### **SEAN-CSO has three tiers of members:**

#### **Practitioners**

Local NGOs, international NGOs, religious organisations coma social enterprises, small businesses.

#### **Researchers**

Academics, research institutes and think tanks

#### **Government (observers)**

Local government, national government, law enforcement

As civil society organisation the strategy was created and endorsed by the membership.

### **The groups activities include:**

**Research** - an annual capacity gap analysis of the needs and gaps in countering violent extremism and counterterrorism in the region. USIP paper will be published soon.

Face to face meetings (regional and country workshops, two to four per year) on specific topics, for example impact evaluation training, financial stability etc) according to strategy. A pilot funding scheme is also available for members.

**Interactive training online** (in local languages). For example, 'Hate Speech' is important for Malaysia. So, training covered how Hate Speech shaped the political environment and the risk of violence and conflict in the country. Another example is about teaching community members and practitioners to recognize early warnings or risk factors of violent extremism and how to address those.

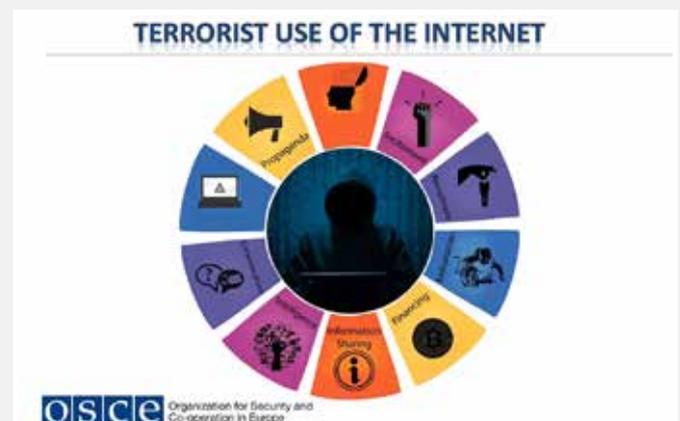
Toolkits (evaluation, fundraising). For example, impact evaluations of city programs about identifying sources of funding alternative sources of funding so financial sustainability.

*There are challenges of a paradigm shift to digital delivery with a proliferation of content. Everyone is moving things online. The UN called this an infodemic. This leads to a duplication of effort. For practitioners is really hard to locate relevant materials content understand what is important and what is not important and understand what is a quality training and what is not a quality training.*

### **Future direction**

*For next year the organisation will be consolidating high quality knowledge and making it available for local SEAN- CSO members. Adapting, translating, ranking existing materials, selecting the training online available, which is good training, which is redundant.*

This will include building a clear and easy to access online library of existing content for lifting capacities and skills in countering violent extremism, and consolidating research knowledge into practical toolkits.



## MR IZURU SUGAWARA , PRESIDENT OF THE OVERSEAS SECURITY AND CRISIS MANAGEMENT ASSOCIATION

### Enhancing security awareness Japan's efforts

Because of the lack of experience in terrorism and extremist violence in Japan for the last two decades. Most Japanese are not aware of the threats and more and more Japanese suffered every year abroad. Therefore, focus was on how to raise the security awareness of Japanese, Japanese traveling abroad.

The Ministry of Foreign Affairs of Japan (MOFA) establish the Council on security measures for International Cooperation Project, which conducted fundamental review of security measures related to international cooperation.

### Key Recommendations

1. Collection and analysis of threat information and the strengthening of information sharing
2. Rules, regulations and code of conduct
3. Strengthening security measures and enhancing security awareness training
4. Improvement of response capability

Especially emphasised was the importance of training and education for overseas travellers.

Japanese government mainly, MOFA and JICA, attach great importance on enhancing security awareness by developing different tools and measures.

'Tabi-Regi' is an information distribution system for Japanese who travel abroad for short periods of less than three months.

By registering travel dates, accommodation, contact information, etc overseas travellers can receive the latest overseas safety and security information, alerts in the event of an emergency and receive emergency contact by emails and SMS in the event of an emergency.

MOFA implemented large scale promotional activities to promote to increase users of the system.

*Many large companies are increased the number of registrants by integrating Tabi-Regi into the air tick ticket reservation process for overseas business trips.*

MOFA enhanced security awareness and public engagement by promoting the system through the use of popular comic books and youtube videos. MOFA have also been creating security awareness by producing Awareness Quizzes online and on international flights.

JICA obliges contracted companies and organisations to receive security awareness lecture as a condition for overseas trips. Lectures and training are also open to any organisations that wants to business with JICA.

### JICA has strengthened cooperation and networking with international organizations

*It is extremely important to share the know-how of security measures, exchange information and risk analysis with international organizations or original organization that are making similar efforts*

Promotion of public private cooperation - Private organisations and companies welcome and cooperate with the efforts of the Ministry of Foreign Affairs and JICA to help create momentum.

The effects of the Coronavirus pandemic have worsened the global economy and increased the risk of social unrest

*It is therefore more likely than ever that multiple crises such as terrorism under a pandemic, political instability and terrorism at the same time will occur. It is recognized by our community that it is necessary to develop new efforts to raise people security awareness.*



## MS ALEXANDRA ANTONIADIS , DEPUTY HEAD OF THE UNIT ON PREVENTION RADICALIZATION AT THE EUROPEAN COMMISSION

The EU has a supportive role. It is primarily the Member States that are responsible for a countering Terrorism and preventing radicalization, leading to violent extremism and terrorism.

But it has increasingly Member States recognize the added value of action at the EU level to pool expertise and experiences exchange best practices also developed joint capabilities, a better joint can common understanding foster Collaboration.

*The EU approach is based on the firm believe that security measures alone will never protect us from terrorist attacks*

The EU advocates a bottom-up approach.

Reach out to collaborate with those that are most closely and more immediately involved in in the matter. For example, teachers, social workers, mental health officials, and community leaders as much as police officers, prison guards and intelligence officers., to be able to detect and prevent the process of radicalization, and the pathway to violence as early as early as possible.

Embedded in this approach is not only a security focus, preventing attacks from happening, but it is embedded in a broader policy perspective that we need to prevent the growing polarization and society. We need to strengthen social cohesion inclusion and integration. These are all integral parts of an overall approach and we need to foster active citizenship democratic values and fundamental rights.

### The Commission created the Radicalization Awareness Network in 2011

This is a network of first line practitioners, not only NGOs, but everybody that is dealing with vulnerable or radicalized people. It is a platform for exchange, but it's also an incubator for innovative solutions, concrete guidance and policy recommendations.

It now has a network of connecting over 5000 practitioners, it has organized hundreds of events from study visits to workshops to bigger conferences. It provides a closer interaction between practitioners, policymakers and researchers.

It has produced practical guidance on:

- How to deal with returning terrorist fighters.
- How to rehabilitate them.
- What we do with those radicalised in prison and released terrorist fighters.
- Evaluation of exit programmes

There's also guidance on more structural changes:

- How to set up multi agency cooperation models
- How local authorities and can be helped to develop a strategy or action plan
- How to set up a helpline for concerned families
- What to do with information sharing in a multi-agency setting; who can share what information, with whom, and under which conditions.

*We are also looking at the impact of corvid, what does that mean for the radicalization process. We see a resurgence of terrorists and extremist propaganda, conspiracy theories disinformation campaigns, and how is that impacting on radicalization pathways*

Also, very important is the increase in violence right wing extremism, both off and online. We have and we continue to be obviously concerned about Islamist extremism, but we see also the need to follow more closely violent right-wing extremism and we have been looking into that more closely.



## The Internet

The Commission follows a broad and diversified approach with voluntary measures with the industry, but also legislative proposals

The launched the EU internet forum in 2015 bringing together the big platforms with member states and Europol to work together to ensure that terrorist propaganda is taken down swiftly, but also to reduce the impact of such terrorist propaganda, by promoting and developing alternative and counter narratives.

*This corporation has grown over the years. I think it has been a blueprint example for other initiatives that started later on, like the Global Internet Forum to Counter Terrorism - [www.gifct.org](http://www.gifct.org)*

The launched civil society Empowerment Program, with the purpose to support civil society organizations in developing their own narratives to either provide an alternative to the extremist propaganda or to counter it. Programmes will be evaluated for effectiveness.

### Proposed legislation to take down terrorist content

Set down clear rules for both our Member States and the industry to take down terrorist content, which has been identified by the competent authorities. As complying with the definition of terrorist content.

*We need a clear and strict definition of what is terrorist content, incitement to carry out terrorist attacks material that and promotes and explains how to carry out terrorist attacks and to train people to recruit people. All this is defined in our proposal as terrorist content, which needs to be taken down within one hour after having been assessed previously by the competent authorities.*

Proposed regulation to provide safeguards to protect freedom of speech. So, there are complaint procedures, judicial redress, transparency and accountability.

## MR. JISOON HAN, KOREAN NATIONAL POLICE AGENCY, FOREIGN AFFAIRS BUREAU, FOREIGN AFFAIRS SECURITY SECTION CHIEF

### Counter terrorism efforts of the Korean National Police

*Context: Korea has yet to suffer a terrorist attack.*

However, in January 2019 UN Security Council report on ISIS and al Qaeda warned that hundreds of Uzbeks had been attempting to enter South Korea. In November 2015 an Indonesian overstayer was arrested for suspected links to a terrorist group. This is why prevention is an integral part of the counterterrorism efforts of Korean National Police Agency (KPNA)

The terrorism prevention activities consists of four phases during all these phases:

1. Collection of terrorism related intelligence from various sources including foreign affairs police officers in the field all cooperation with national intelligence service and other related government agencies.
2. Analysts in the foreign affairs Intelligence Division thoroughly assess the reliability of the intelligence by the standard of reasonable doubt.
3. Investigation teams seek to gather concrete evidence and try to apply the Counter Terrorism Act or the Terrorism Financing Prohibitionist Act, these laws are the backbone of our activities.
4. The suspect is indited based on the investigation results or deport the suspect in cooperation with the Ministry of Justice Immigration Service.



## Background information on emerging terrorism financing issues in Korea.

According to the report issued by the UN Security Council. In January 2019 some Uzbek migrant workers in South Korea were reported to be a source of financing for the travel of extremists to the Syrian Arab Republic. Some of the foreign workers in Korea are allegedly friends or relatives to a foreign terrorist fighters in the conflict zone and transfer funds for them. This method of fundraising usually involves the transfer of funds from multiple unrelated individuals to a single entity or individual in another foreign country that particular entity or individual subsequently delivers the funds to the ultimate recipient in the conflict zone via informal remittance channels such as Hawala.

In all these cases the Korean Police foreign affairs counterterrorism teams. Had been thoroughly analyzing intelligence gathered on each subject monitoring their movements and trying to formulate the most effective and appropriate strategy for each case. Through CT teams proactive counterterrorism intelligence activities, the KNPA were able to present the perpetrators in time prevent them from remitting more funds to a terrorist group and bring them to justice.

## MUHAMMAD IDREES

### Current Trends of Violent Extremism and Radicalization That Lead To Terrorism (VERLT) in Afghanistan and the Region

Two examples of 'Best Practise' of bottom up campaigns.

#### United States Institute of Peace, peace education program at the Nangarhar University

**The Problem** - Many of the students who are engaged in day established their connections with ISIS and the Taliban.

The University started peace building approaches within the university campuses and also in their community. One aspect of the program was to establish the **Peace Clubs**, and these clubs were engaged in the in the activities, for example, delivering the message of peace, of conflict resolution and peace building training and some other extra curricular activities like blood donation and book donation.

Another aspect of the program was the Youth Peace Journal in which the students share write poems, articles, essays, interview and role models in their communities.

After the program was launched it slowly within the campus to changed the minds of the students and convinced them that it's not that violence is not the only way are not the only way to achieve their objectives and dreams.

*Both the book donation and blood donation campaigns have been very successful in turning the youth away from radicalism.*

#### People's Peace Movement

Started in 2018. This involved a group of young people getting together, they travelled across the country demanding a ceasefire this is a non violent movement demanding an end to the war. The movement spread across the country and attracted people from different ethnicities.

The movement was had impact because it appears neutral and has mobilised the youth.

#### Recommendations on how to combat the problem of radicalization in violent extremism

Strengthening the institutions and eradicating of corruption

- Capacity building of local governments
- Designing and implementing of proper youth policies
- Exchanging visits of students faculties academics, researchers and writers
- Recruitment of educated Imams in the mosques
- Cooperation between Central Asia and Afghanistan in border management drug trafficking and trafficking in human beings



# REPORT

Leveraging Innovation and Technology to Address 21st Century Security Challenges and Crises across the OSCE and Asian Partners for Co-operation.

## STRENGTHENING AND ADVANCING INTERNATIONAL CO-OPERATION IN BORDER SECURITY AND MANAGEMENT DURING CRISES

**This session assessed how well prepared border agencies were in dealing with the current health crisis and will provide guidelines for a more efficient crisis response and contingency planning. The session focused on enhancing the base-level co-operation between border agencies, customs services, sanitary agencies and other security sector actors in a systematic manner. It touched upon Integrated Border Management (IBM) and its focus on international co-operation as a viable tool for early warning and risk assessment.**

**Moderator:** Mr. Jonathan Holland, Director, OSCE Border Management Staff College, Dushanbe

- Mr. Scott Lacey, Australian Border Force/Aviation Traveller NSW, Australia
- Ms Upinya Boonruangnam, Police Major / Inspector of Foreign Affairs Division, Foreign Affairs Division, Royal Thai Police, Thailand
- Mr. Mohammad Amran Sahak, Customs Department, Afghanistan
- Mr Savvas Chrysoulidis, Major/MPSOTC Instructor, Hellenic National Defence General Staff / MPSOTC (NATO PFP) Training Division, Greece
- Mr. Erdenetugs Erdenebat, Foreign Relations Officer, Ministry of Justice and Home Affairs of Mongolia, Mongolia Immigration Agency, Mongolia
- Ms. Gerrit Zach, Associate Project Officer, Conflict Prevention Center (CPC), OSCE Secretariat

### MR. SCOTT LACEY, AUSTRALIAN BORDER FORCE/AVIATION TRAVELLER NSW, AUSTRALIA

**Australia's COVID-19 response** - How to ensure effective and efficient interagency cooperation across both state and federal levels in response to an unprecedented pandemic.

The National cabinet held a meeting between our Prime Minister and the relevant state and territory heads to ensure that there's a collaborative and cooperative approach across all state and federal jurisdictions to ensure a concerted response to the COVID-19 threat.

Australia's response to the COVID-19 pandemic have seen an unprecedented level of Corporation from state and federal law enforcement defence and health agencies.

*In response to something that we've never done before, putting people into hotel quarantine, dealing with a pandemic and how effective and efficiently it has all come together, even from the first day. I strongly believe that part of this cooperation was the direct benefit of previous exercises and scenarios that my agency had ran with the state. We were able to connect and cooperate and work together collaboratively right from the start of this response. So, I would encourage you in your agencies to run exercises, to run interagency desktop initiatives and cooperative exercises such as this, because they create a system of communication, a system of cooperation between agencies. So, when we do need a quick responses to a crisis, we can do so effectively.*



## Australia's arrival and entry travel restrictions

- In response to the COVID-19 pandemic entry to Australia is restricted to Australian citizens and permanent residents
- Temporary visa holders require an exemption to enter Australia
- On the 24th of March Prime Minister of Australia announced a travel restriction on Australian citizens and permanent residents departing Australia
- Australian citizens and permanent residents require an exemption or must meet an exemption category to depart

## Introduction of hotel quarantine

- All incoming passengers are arriving in Australia we're to quarantine in a hotel for 14 days – They were tested twice in that hotel period. The programme was run by state agencies supported by ABF at the point over entry.

Part of effective interagency cooperation is the establishment of interagency command centres.

*I strongly believe the establishment of these command centres where officers from different agencies can be co-located within the one centre to ensure effective communication between agencies*

## International and regional cooperation

Located within the Pacific, with many close Pacific island neighbour nations, that had very low COVID-19.

Australia put in place enhanced health screening for all passengers flying to Pacific island nations.

Further discussions with other countries with low rates are likely to progress to develop quarantine free travel arrangement within certain bubbles to ensure economic recovery.

*The COVID-19 crisis is so unprecedented, it's impossible for us to adequately prepare for. The best preparation we can have within our agencies, is to ensure we have agencies that are resilient agile, responsive and readily adaptable to ensure that any crisis, whether it's a pandemic, terrorism, a natural disaster, any crisis that occurs, how agencies can stand up responses quickly and work collaboratively and cooperatively together.*

**Jonathan Holland:** Stressed the absolute importance of regular training and exercises between different agencies. Also, embedded officers from different agencies in joint command centers. The more closely that you train with colleagues from other agencies, it simply becomes second nature. And when we are called into action for any real life incident, whether it's a pandemic, whether it's a terrorist attack. The closer you work together and train together, it becomes second nature. The last thing you need in the middle of any incident is bumping into people from different agencies for the first time that you've never worked with, you don't know their procedures and processes.

MS UPINYA BOONRUANGNAM, POLICE MAJOR / INSPECTOR OF FOREIGN AFFAIRS DIVISION, FOREIGN AFFAIRS DIVISION, ROYAL THAI POLICE, THAILAND

## Thailand banned all inbound and outbound flights

Some foreigners continued to enter with non-immigrant visas like businessman, people with family in Thailand and students.

## Thailand created a Special Tourist Visa (STV)

This was designed mainly for those who want to make long stays. They are allowed to enter and stay up to nine months. These visas are subject to embassy checks. These visitors are subject to 14 days quarantine upon entry.



## **APPS: Advanced Passenger Processing Service**

Airlines send passenger information and crew information and flight information, before the aircraft depart from arrive to our transit through any international airport in Thailand to verify the Traveller can travel into our depart from Thailand.

### **Benefits**

#### **Government Agencies**

- Increase security passenger processing you line reduce time of passenger processing
- Passive passenger information is accurate
- Receiving passengers list in advance
- Managing time and resources

#### **Airlines**

- Save cost on rejected passenger
- Customers feel more confident
- Prevent terrorists on board

#### **Passengers**

- Safely travel
- Speed up the process at the immigration checkpoint

### **Biometrics**

There are 200 biometric scanners installed in 170 borders, including airports, seaports and land border crossings.

### **Challenges and conclusion**

As the country starts to open up, the special tourist visa is one that we concern about because criminals may seek to enter the country via this means along with more regular passport imposters.

Thailand is one of the busiest ports of entry in the world. Technology in the form of APPS and biometrics is vital to control our busy borders.

## **MR. MOHAMMAD AMRAN SAHAK, CUSTOMS DEPARTMENT, AFGHANISTAN**

### **Modern Technologies to Address Security Challenges in Afghanistan**

**Background:** Afghanistan is a landlocked and war torn country in a period of transition, which requires assistance and support of the international community to tackle the situation. The current security issues are insufficient cooperation with the international community, a volatile security situation with insurgencies and terrorist networks across the country, infiltration by neighbours in the internal affairs of the country and skirmishes at the border.

With the help of international partners and donors technology deployed so far includes:

- Deploying scanners to control illicit trafficking of goods and also biometric systems
- Deployment of smart cameras and digital scales ensure national revenues and taxes are accumulated

In 2006 the government implemented the ASYCUDA system to prevent legal activities at customs and to facilitate trade.

The security agencies have deployed K-9 units- specially trained dogs for drug detection, arms and explosives goods.



## Security Agency operations

- Security agencies patrol in the cities 24/7 being equipped with small technical devices (scanners, sniper rifles, dogs, cameras and others)
- Security agencies are engaged in fighting insurgents and terrorists
- Security agencies are engaged to stop the infiltration of neighbours via large open borders
- Security agencies are dealing with smuggling and human trafficking
- Security agencies are confronting the menace of contraband and illicit trafficking of goods

Modern technologies are being used to counter smuggling and trafficking which includes gold, drugs, money laundering, terrorists and rebels, weapons and human trafficking.

## Recommendations

- It is essential to increase the use of modern technology in preventing and countering terrorism
- Modern technology can prevent corruption at the border as well as smuggling and other illicit activities at the border
- Donors support in the acquisition of modern technology to be used by security agencies is instrumental under current security circumstances
- Better and enhanced security cooperation with the neighbouring countries in order to improve regional security

*We are currently working on an IBM strategy with a neighbouring countries, supported by European Union and it will be implemented around the end of 2020*

MR SAVVAS CHRYSOULIDIS, MAJOR/MPSOTC INSTRUCTOR, HELLENIC NATIONAL DEFENCE GENERAL STAFF / MPSOTC - NATO PFP - TRAINING DIVISION, GREECE

## Soft Power and Cooperative Approaches On Border Security, A Critical Link To International Security

Since the end of the cold war and the terrorist attack on the USA 2001 we have entered a new threat agenda, where the main victims are not States but individuals. This new threat agenda includes organised crime, criminal gangs, misgoverning, epidemics, terrorism, failed states, natural hazards, poverty, overpopulation, economic mismanagement, failed states, irregular migration.

### Soft and Hard Power Contexts

**Hard power** is the exercise of influence through coercion relying on tactics like military force payments and economic sanctions

**Soft power** uses attraction and persuasion to change minds and influence behaviour its sources includes culture, political values and positive global engagement

In the new threat environment is dealt with by soft power and a good exemplifier of that is the OSCE.

The OSCE has a comprehensive approach to security that encompasses is not only politico-military, economic and environmental, but also human dimension aspects.



## Causes of Soft Powers Promotion in Border Security

- Impact of globalisation on the ability of states to accumulate and employ hard power
- The distinction between old and new security concepts, and the changing nature of military warfare
- The rise of non-state actors in the conduct of international relations such as, private military companies, NGOs, private sector and civil society
- The impact of the technological revolution in international relations
- The democratisation of the media on the interpretation and expression of foreign policy goals and strategies

## Collective border security

Collective border security means multilateral and the bilateral agreements about the trafficking about the list interact and how we can address these threats. It includes forums for the exchange of knowledge, the exchange of information.

## Recommendations

### Collective Border Security:

Establish which countries around the world have the desire but not the funds, proper equipment and training for collective security.

*For example, we visited the Tajikistan/Afghanistan border, where the Japanese government had given the budget in order to buy in mobile X-Ray Machine in order to scan the trucks, this is how a country can give funds to another country that has the desire but is economical too weak to have the proper equipment.*

Threat should be addressed at the source and a 24/7 early warning system to be in place which all states should have the ability to access and communicate with and with each other.

The first step in this direction is a forum for discussion under the UN or the OSCE to address solutions beneficial for all states.

### Military Role:

Military has a border role mainly in surveillance and providing a second line enforcement if there is an escalation. Military personnel to participate in joint training like OSCE/BMSC, as well as in discussion forums, conferences and other security activities.

Activities to change mindsets for both to military and law enforcement staff for acceptance of this role. Review of military personnel participation and duties and develop a legal framework to implement these changes where needed.

### Border Security Soft Power Index:

Introduction a soft power index SPI on border security and it will become possible to process and qualify data which can be used to produce graphs reports studies analysis at local regional and global level.

Identical identification of weak border areas and the capability to measure and improve them.

Create awareness of the border security situation for both the authorities and individuals. Promoting resilience and the capability to monitor the degree of changes when actions occur.

### Training and Education:

*The most important tool in promoting soft power is training and education.*



Centralised control and evaluation from one responsible body for providing training and education. With a decentralised training and education delivery i.e. train the trainers

Creation of a common database where unclassified training and education material related to border management and security is uploaded and shared.

Training and education should match the job description and be mandatory and continuous for relevant personnel.

### **New Technologies:**

Create connections with industry and universities Defined new methods equipment and technological solutions.

International organisations should fund the implementation of API/PNR in countries that want it but cannot afford it.

Satellite and IT capabilities must be promoted and implemented in border security, for example (EU SatCen provides data information and intelligence but only two EU member states).

### **Role of Mass and Social Media in Border Security:**

Public affairs offices should be created in each Border Agency it should be manned by media experts. Personnel should participate in media awareness seminars and core courses in order to handle ongoing situations in a proper manner.

At the strategic level of communication, use social media and new media to promote the work of the border agencies to gain public understanding and empathy.

### **Border challenges:**

New and old threats require states to find the balance between soft power and hard power i.e. smart power.

We should not allow criminals to threaten the rights of individuals in the name of security.

Modern threats appear in new contexts and criminals are better prepared than ever before to take advantage of all the new systems on weaknesses. That means acting more effectively and then disconnected world.

It becomes increasingly complex to succeed, whilst trying to maintain the balance between open and secure borders.

Overall soft power and a cooperative approach seem to be more effective in the contemporary international security environment than the use of hard power.

The use of soft power for border challenges are low cost solutions, that provide long term results and are sustainable.

MS. GERRIT ZACH, ASSOCIATE PROJECT OFFICER, CONFLICT PREVENTION CENTER - CPC - OSCE SECRETARIAT

### **Security Sector Governance and Reform and Border Security Management**

**A working definition** - The security sector governance is subject to the same standards of good governance as any other public sector.

What do we mean by good governance?

#### **Key principles:**

##### **Accountability and Transparency**

*Any border policing needs to be subject to democratic oversight and governance, as are all other security agencies which have right to use force.*



There needs to be specific accountability mechanisms but at the same time have sufficient authority for the role. Internal and external oversight, legislative oversight, but also a community dimension.

### **Gender Responsive Human Rights and Rule of Law**

Border management is gender responsive human rights compliant.

### **Inclusive and Holistic Approach**

*A key part in any security sector good governance is really about this inclusive approach. Basically, taking into account into linkages between various actors. Using a whole of government of response and having intra and inter agency and response mechanisms in place. This is ultimately what this is about. Having information flows on at least three different levels, vertically from border units in a ministry, to the units working on the border posts, horizontal cooperation among all services really operating at the border, but also international cooperation between agencies involved in border issues in different countries.*

### **SSG/R Principles**

Political will and national ownership are critical to achieving progress and reform

A holistic approach to SSG/R is essential. When supporting reforms in one part of the security sector, it is imperative to reflect how this may affect, or require changes in other parts of the sector

SSG/R obligations and commitments on border related issues

The OSCE border security and management concept provides the political framework for cooperation. Recognising that border security and management is a matter of national sovereignty and responsibility of states, the concept provides grounds to the participating states to seek and receive assistance from the OSCE based on identified priorities, for example, the development of comprehensive national border management strategies, thereby supporting national SSG/R processes.

The concept calls upon the participating states and gives recommendations to promote interagency cooperation between their border services, customs authorities, agencies issuing travel documents and visas, and law enforcement and migration agencies, as well as other competent national structures.

### **COVID-19 Challenges**

- State of emergency is issued
- Closing of borders increase impersonal diploid two entry points via land sea and air
- Additional tasks for the security sector, due to the crisis nature of the response there was inevitably less oversight
- TNTD: more interagency cooperation information sharing needed.  
*There is a need for having this in place, so that it is ready for any crisis situation.*
- ODIHR: effectiveness of the response to the pandemic has been determined above all by the level of trust



# REPORT

*Leveraging Innovation and Technology to Address 21st Century Security Challenges and Crises across the OSCE and Asian Partners for Co-operation.*

## LEVERAGING TECHNOLOGY IN ADDRESSING TRANSNATIONAL SECURITY THREATS AND CRISES IN THE OSCE PS AND ASIAN PFC.

**During this session, the panel explored the possibilities of using and combining the existing and new technologies (Biometrics, API/PNR Systems, e-passports, automated border gates, national and international databases) in an effort to facilitate cross-border movement and prevent transnational crimes and terrorism. The participants also discussed protection of human rights and fundamental freedoms in development and application of the listed technologies. Additionally, the participants explored best ways of leveraging modern technologies in dealing with crises similar to the current one triggered by COVID-19.**

**Moderator:** Mr. Cameron Walter, Associate Programme Officer, Border Security and Management Unit/Transnational Threats Department (BSMU/TNTD), OSCE Secretariat

- Mr. Andrew Priestley, Director, Agile Borders and OSCE external expert on API/PNR
- Mr. Junichi Sakaki, Adviser for Panasonic System Solutions, Japan, Chair of Japan ePassport technical committee, Head of ISO/IEC JTC1 SC17/WG3/TF4
- Ms. Mona Koehler-Schindler, ODIHR, Associate Human Rights Officer on Anti-Terrorism Issues
- Ms. Christiane DerMarkar, ICAO Traveller Identification Programme (TRIP) Technical Officer
- Ms. Arsineh Danielians, Senior Migration Officer, Department of Home Affairs, Australia

## MR. ANDREW PRIESTLEY, DIRECTOR, AGILE BORDERS AND OSCE EXTERNAL EXPERT ON API/PNR

### API and PNR - obligations and benefits in times of crisis

The UN Security Council resolutions 2178, 2396 and 2482 mandates the collection and use of Advanced Passenger Information (API).

*There are many reasons why you should want to do this rather than because you have to do this*

#### Passenger Information - Advanced Passenger Information

- Information about travellers data from travel document (Name, DoB, Nationality, Flight)
- Sent to governments at close of check-in
- Used to facilitate border control and combat irregular migration
- Approximately 75 countries require API

#### Passenger Information- Passenger Name Record

- Information about the reservation
- Rich data set
- Available before close of checking.
- Very useful for risk profiling
- Many countries want to use PNR



*The PNR file is started as soon as the flight is booked, which could be up to a year in advance. This can include information about baggage and information about other flights that are booked on the same reservation. So, you can start to see that from a border management and intelligence perspective, this data set could be much more useful than just a little bit of information about the traveller.*

*The number of governments that want to use PNR versus the number of governments that can use PNR is very different. There are only a handful of governments around the world who are actively using PNR. The high level of data protection required is a barrier to using PNR for most countries.*

Invaluable for countering terrorism, irregular migration, human trafficking and the facilitation of border management.

### **Benefits**

Historically border agencies have necessarily been reactive; a traveller presents themselves at the border in an airport, and then the border official makes a decision on that traveller, after they've arrived.

API allows border agencies to be more proactive. To plan and use available resources efficiently, for example, target individuals of interest immediately upon arrival whilst expediting the onward journey of low risk passengers.

API enables risk profiling of travellers based on their journey, rather than individual based, which is a more ethical way of profiling.

### **Use of API and PNR in current and future pandemic's**

API provides the origin of a flight and usually the origin of a connecting flight, So that you know if a flight is arriving from a high risk area

PNR provides the full journey history if made on the same reservation. Provides the details of all flights made of the same booking and people travelling within the same group.

### **What about information from other modes of transport?**

API and PNR are defined data sets which includes things like magic baggage, seat number, flight number.

Whilst these elements may not be available from ferry crossings and maritime traffic, other data elements like car licence plates may be. For passengers travelling by bus or coach, it would be known exactly what other passengers were travelling with them on that vehicle.

Whilst it is fairly straight forward acquiring API and PNR information from airlines, acquiring similar data from road a maritime operators needs consideration.

MR. JUNICHI SAKAKI, ADVISER FOR PANASONIC SYSTEM SOLUTIONS, JAPAN, CHAIR OF JAPAN EPASSPORT TECHNICAL COMMITTEE, HEAD OF ISO/IEC JTC1 SC17/WG3/TF4

### **Passports and Biometrics in Japan**

#### **Passport issuance**

#### **Study on Morphing Countermeasures**

- The threat of impostor by using two person image morphing
- Morphing detection/Direct facial capturing

#### **Preliminary Survey for Digital Travel Credentials (DTC)**

- ICAO DTC TR will be published in 2020
- Study for future possibility



## Border control - Automated facial recognition gate

There are seven airports and 203 autogates in Japan, without pre-registration using IC chip and facial image. These gates save space and transactions are faster. 80% of travellers in Japan are using autogates.

## Airport E-airport project

Using one ID (facial token) allowing automatic check-in, self baggage check-in, automatic boarding gate - Binding the facial image and the e-ticket.

## Morphing

Moving attack is becoming a realistic challenge for enrolment and border control and moving detection techniques are not mature.

## Integration of automatic process (airline border control etc)

For the seamless process the auto gate systems should work together.

## DTC

ICAO DTC standard will be published soon. It will enable faster transactions and good for the use of smartphone apps', and include full passport data, facial image with API and PNR data and can be transferred to the destination country before departure. Easy to link two IATA On-ID programme.

## COVID-19

Exchange health information: We need to standardise health information

Travel history check

We need to implement contactless travel

## JOHANNES HEILLER - HUMAN RIGHTS ADVISOR OSCE/ODIHR

### OSCE comprehensive concept of security

Countering security threats affectively requires efforts in all three OSCE dimensions (1) Politico-military (2) economic and environmental (3) and the human dimension.

*Security/counter terrorism and human rights are not competing objectives and are in fact mutually reinforcing*

Border Security and management has an inherent impact on human rights and combined with data driven technology the human rights concerns are amplified. Increased border security, including and the counterterrorism context must not come at the expense of human rights.

*At the core of the OSCE's comprehensive concept of security is exactly that, that sustainable security really requires protecting human rights. A lack of respect for human rights does not create more security but it actually undermines our security and this obviously also applies in the border security contracts, we should never forget about that.*

### Key rights in the border context:

- Freedom of movement - including the right to leave any country including his or her own and the right to enter one zone country
- The right to seek and enjoy asylum
- Equality and non-discrimination
- The right to privacy - including the protection of personal data - gateway right.
- Certain rights can be restricted but only within strictly defined parameters



## Human rights challenges related to API and PNR

- Interference with the right to privacy
- Excessive data collection and retention
- Protection of sensitive data
- Unlawful sharing of data
- Potential implications for other rights

*Data collection must have a clear legal basis with appropriate safeguards in legislation and data collection must be minimized to what is necessary and proportionate and it must not be discriminatory.*

Retention storage of PR data. If API and PNR data are repurposed to use in track and trace systems and/or health data is also collected and stored it raises many legal and ethical questions that will need to be addressed.

Human rights challenges related to the collection storage and usage of biometric data:

- Bias in facial recognition/ risks of discrimination - the impact of gender and skin colour on accuracy rates
- Collection and retention of biometric data (fingerprint facial recognition images)
- Impact of unlawful sharing of biometric data

*There are studies which have shown that depending on the ethnicity of the person, whose images are checked, there is a higher error rate.*

*And many systems have more difficulty in identifying women than men and in particular, women with a darker tone of skin. So again, there is a risk of discrimination here which we need to be very, very careful about.*

## Algorithmic Data

It is important to emphasize that algorithms and algorithmic decision making is not neutral and bias can be introduced at the programming level. There is a need to be very careful to ensure that we're not perpetuating discrimination.

**Human rights challenges related to watch lists, databases and other information sharing for border security:**

- Wrongful inclusion on watchlists the listing
- Abuse of watchlists and International alert systems
- Lack of remedy

## Conclusions and Recommendations

Put in place solid legislative frameworks that regulate the use of new technologies at borders and provide strong human rights safeguards

Establish effective oversight mechanisms regular, monitoring and independent review, as well as effective remedies for those whose rights may be affected

While states have the primary obligation to respect and protect human rights, private business enterprises developing, operating and selling such technologies also have human rights responsibilities, to which they need to be held accountable

Conduct thorough human rights impact assessments prior to deployment of any new technology and at regular intervals in its operation

Ensure border guards using new technology systems receive adequate human rights training and are sensitised to potential bias



## ICAO TRIP and the tools to Facilitate Cross Border Movement and Prevent Transnational Crimes and Terrorism

Three facilitation programmes: Annex 9, ICAO TRIP strategy and ICAO PTSD

**Annex 9 – Facilitation:** the regulatory framework and contains all the standards and recommended practices concerning the ICAO TRIP strategy.

Facilitation is the efficient management of border control processes to expedite clearance (of aircraft passengers, crew, baggage, cargo) and prevent unnecessary delays, so as to maintain both the security and efficiency of air transport operation.

### Announcement

*28 February 2021, A new amendment to Annex 9 - Amendment 28 contains new standards and Recommended practises in relation to Passenger Name Record (PNR) and makes it mandatory for states to implement PNR*

### Doc 9303: International specifications for Machine Readable Travel Documents (MRTD's)

*There will be a new addition up Doc 9303, published by the middle of 2021. It will contain updates but will also contain and you section on visible digital seals*

It is mandatory for all states issue a machine-readable travel document that has incorporating standardized format for the visual zone and machine readable zone.

Standardized format it facilitates inspection by airline and government officials, which results in clearance of low risk traffic, and problem cases are more readily identified.

### ePassport or Biometric Passport

Biometrics will help to solve identity fraud, lookalikes and imposters. Biometrics will not prove identity but seals identity to a document. Once linked it is very difficult to tamper with a document or change it.

*Improper validation of an ePassport leads to a false sense of security.*

### ePassport Benefits:

- Facilitates travel
- Enables automation
- Increases security

*But these benefits can only be properly realized and trusted if you verify the applied digital signature which requires the appropriate public keys*

### ePassport Public Key Database (PKD)

Having a public key infrastructure at national level is essential for properly taking advantage of an ePassport.

ICAO PKD database stores all the certificate so States that participate can upload their certificates and allow other states to download them for the validation.





### Recommended Physical and Digital Matching at Borders

- The use of Automated Border Controls (ABC's) gates as a means of verifying and authenticating a passport and enhancing security and cross border movement to facilitate the clearance of passenger
- Use of ePassports
- Use of Biometrics
- Validation of ePassports via the PKD

### KEY TAKEAWAYS

Across both days clear themes emerged, the need for ever closer international and regional co-operation being the most widely shared. Closely aligned with this is the sharing

good practices. The impact of the digital platforms and social media was identified as one of the major challenges and the need to develop the legal framework to meet this challenge and the technologies to tackle it.

#### Key Recommendations

1. Collection and analysis of threat information and the strengthening of information sharing
2. Rules, regulations and code of conduct
3. Strengthening security measures and enhancing security awareness training
4. Improvement of response capability

