**Organization for Security and Co-operation in Europe**

**Secretary General's Security Days**

**A human rights-centred approach to technology and security**

**Opening remarks**

**Secretary General Thomas Greminger**

***8 November 2019***

Commissioner Mijatović,
Ambassador Boháč,
Director Gísladóttir,
Excellencies,
Ladies and Gentlemen,

Good morning!

Welcome to this Security Days event on a human rights-centred approach to technology and security. I am very pleased to see such a diverse group of participants drawn from not only the OSCE family but also our partners in other international organizations, civil society, business and academia.

So thank you all for coming!

We chose this topic because of the Slovak Chairmanship's focus on the Fourth Industrial Revolution. Also, a number of ambassadors suggested that we look at issues related to the human dimension of security.

The digital domain is now at the forefront of debates about human rights, democracy and security. We also noticed the growing impact of technology on the work of OSCE executive structures: for better or for worse.

So it seemed logical to take a closer look at the implications of new technologies for human rights and security.

As a result, and in close consultation with the Institutions and the Parliamentary Assembly, as well as with different units in the Secretariat, we have put together an interesting programme. We will look at the benefits and risks of technology, taking a human rights-centred approach to rapid technological change. We will also discuss what lessons we can take away from this for the OSCE's work.

Younger generations are increasingly paying attention to new technologies. At the OSCE Perspectives 20-30 Youth Forum in Bratislava last week, I witnessed how young participants discussed the advantages that new technologies can bring but also the potential risks they might pose to security in the OSCE area. I am delighted that one of those experts, Katarina Kertysova, will participate in the final panel this afternoon.

Colleagues,

Security Days is designed to be different than most OSCE meetings here in the Hofburg. It should be more inter-active and provocative, and because of that, it should bring new ideas to our work. I encourage you to take part actively – to ask questions, to share experiences, and to provide suggestions.

The success of this event depends to a great extent on the quality of our speakers and moderators. The good news is that we have a great line up today!

I would like to thank, in advance, all our panellists and moderators who have accepted to speak today. We look forward to hearing from you.

Special thanks to Commisioner Mijatovic, the former OSCE Representative on Freedom of the Media and currently the Council of Europe's Commissioner for Human Rights. Welcome back, Dunja!

Ladies and gentlemen,

The topic that we are discussing today is all around us.

Just look at the impact of the Internet, smartphones, and fingerprint or facial recognition software on our lives, our societies and our work.

But do we understand the potential implications of artificial intelligence and big data? Or how the collection of massive amounts of personal data could impact us? How do we take advantage of technology to enhance security while safeguarding human rights and human dignity?

What is the appropriate role of the OSCE in addressing these issues, based on our comprehensive security concept and our co-operative approach to promoting security across all three dimensions?

While these topics are relatively fresh for the OSCE, some may be surprised to learn about the wide range of activities that different parts of the Organization are already engaged in that relate to the impact of technology on human rights and security.

Allow me to highlight a few.

Criminals are often the first-movers when it comes to technical innovation.

For example, technology is being misused by human traffickers to recruit, control, and exploit their victims. They not only communicate through the Dark Web, but also use publicly available applications employing encryption to carry out illicit activity. Cryptocurrencies, for instance, allow criminals to move money anonymously.

Terrorist groups are using the Internet to recruit followers, finance their activities, disseminate propaganda, and incite people to commit acts of terrorism.

Cyber attacks threaten critical infrastructure, and can jeopardize privacy and data protection.

But technology can be – and is being – used to fight crime. Also in the OSCE.

Just in the past few months, the TNTD's Strategic Police Matters Unit (SPMU) organized a conference in close co-operation with the Slovak Chairmanship and the Austrian Federal Ministry of the Interior on "Crime in the Digital Age". The SPMU also supported the Chairmanship in organizing the Annual Police Experts' Meeting to focus on the use of artificial intelligence in policing.

Or look at anti-trafficking efforts. Data aggregation and analysis, blockchain for traceability, artificial intelligence, facial recognition, and monitoring trafficking routes are all examples of our tech against trafficking programme. We will hear more about the OSCE's work in this area later today.

Technology can also be used to counter terrorism and to improve border management.

For example, biometric systems integrate checks against watch-lists and databases in order to compare the traveller's biometric information against known criminals or terrorists. The OSCE plays a role by helping participating States to collect and share biometric data as mandated by UN Security Council Resolution 2396.

We also support participating States in developing national capacities to counter the use of the Internet for terrorist purposes, while keeping in mind our commitments to freedom of expression and freedom of the media.

Regarding arms control efforts, participating States use the technologies provided by our OSCE Conflict Prevention Centre to reduce the risk of conflict. Specifically, information is routinely exchanged via the OSCE Communications Network to increase transparency and to build predictability and trust. Recently, States have also taken it upon themselves to approve the use of the CommsNet to exchange information pertaining to Cyber Security Confidence-Building Measures.

We should also not forget the second dimension.

At a time of fast-moving digital transformation, we need to take into account both human capital and human rights – to minimize the risk of a digital divide. The Milan Ministerial Council decision on human capital development in the digital era gives us something to build on.

Technology can also help to reduce risks to the economy and the environment. A newly designed project of the OCEEA aims to increase the capacity of participating States to use innovative open data tools and new digital technologies. They can enable governments and civil society to implement open data national commitments. Moreover, OCEEA has developed an OSCE E-learning Platform that now hosts the first online training course on Good Governance and Anti-Corruption and it will soon also add a Virtual Competency and Training Centre for the Protection of Critical Energy Networks. The Centre offers online-based trainings and risk assessments and a common platform for energy professionals and related stakeholders throughout the OSCE area. This illustrates a potential area of growth for the OSCE: namely capacity-building through on-line tools.

One final example to mention is the way technology is contributing to the effectiveness of our field operations. The Special Monitoring Mission to Ukraine is a great example.

Since October 2014, the SMM has increasingly used technology to enhance its ability to monitor developments in eastern Ukraine: through satellite imagery, UAVs and fixed surveillance camera systems. This technology has given the Mission access where it has been restricted, enabled monitoring at night, and reduced risks to our monitors. This is a good example of how technology enhances security and thus supports the Mission's efforts at facilitating responses to ease the humanitarian consequences of the violent conflict. We will hear more about technology in OSCE field operations in session one.

Ladies and gentlemen,

While the web can be a dark space, it can also be a safe space. OSCE Institutions are also working to that end.

ODIHR supports civil society partners seeking greater security. I am very glad that the Director of ODIHR, Ingibjorg Gisladottir, is with us today: we look forward to your remarks in a few minutes.

The Representative on Freedom of the Media has focused special attention on safety of journalists and particularly of female journalists online.

And the High Commissioner on National Minorities offers guidance on how to create, nurture, and develop the role of the media and information technologies for conflict prevention.

The OSCE PA is also doing important work on technology issues, including a recent resolution about digitalization as an advantage for gender policies, sponsored by Stefana Miladonovic, the Special Rapporteur on the Digital Agenda. I am delighted that you joined us today, Stefana.

It is indeed very troubling that online forms of violence against women are becoming increasingly common, particularly with the use of social media platforms and other technical applications. A recent study by the OSCE on the well-being and safety of women reveals a disturbing picture of online violence against women and cyber stalking.

So, colleagues, there are many interesting topics for us to look at today – as illustrated by the icons that you see on the screen.

The questions include:

What are the risks, and what are the opportunities?

Who are the key players and what kinds of partnerships are necessary to cope effectively with developments that originate largely in the private sector?

How can the OSCE adapt to the rapid development of technology in a way that upholds our commonly agreed principles, and that furthers the common commitment of our participating States to promote human rights and comprehensive security? This will require innovation and co-operation.

In that spirit, I look forward to a thought-provoking and forward-looking exchange of views.

In concluding, I would like to remind everyone that Security Days are dependent on the voluntary contributions of participating States. This event would – quite literally – not be possible without the support of the Czech Republic and the Netherlands, as well as in-kind contributions from Estonia, Canada, Sweden and Germany. So thank you very much and thank you all for your attention.