OSCE Security Days

A Human Rights-Centred Approach to Technology and Security

8 NOVEMBER, HOFBURG, VIENNA

Concept Note

At the most recent OSCE Summit in Astana (now Nur-Sultan) in 2010, participating States reiterated that human rights and fundamental freedoms are inalienable, expressing their conviction that "the inherent dignity of the individual is at the core of comprehensive security." OSCE participating States have long recognized that respect for human rights, fundamental freedoms and the rule of law is intrinsic to any successful approach to countering contemporary threats and addressing challenges to security and stability in the OSCE area.

For example, efforts to combat terrorism and related phenomena such as violent extremism and radicalization that lead to terrorism (VERLT) and various forms of organized crime, including trafficking in human beings and in illicit goods can only be successful and sustainable if compliant with their commitments to protect human rights.

Global attention is now focused on the role of new technologies and technological developments enabled by computerization and digitalization – sometimes characterized as the "Fourth Industrial Revolution." Driven by largely privately owned ICT industry, these may have profound implications, both positive and negative, for all aspects of security, including the human dimension.

On the positive side, for example:

- Tools enabled by digitalization can provide participating States and other responsible actors with means to enhance comprehensive security at all levels and serve to foster dialogue and understanding both within and among OSCE participating States.
- State authorities can use such tools, for example, for better policing, border monitoring, intelligence-gathering, victim identification, analysis, facilitating citizen participation, awareness-raising, education, data protection, and secure communications.
- The accessibility of modern technologies enables State and non-state actors to easily share information and take action for positive purposes, including to promote democracy, human rights, transparency and accountability as well as formal and non-formal education, co-operation across frontiers, , and networking to increase economic opportunities.

Among negative implications:

- Any technology can be misused or exploited by terrorists, traffickers, child abusers or other criminals to carry out and conceal their malign activities.

- Abuse of technological tools by state actors – such as excessive, unjustified or disproportionate surveillance, data collection and profiling – can result in violations of human rights and fundamental freedoms, including due process guarantees, freedom of thought, conscience and religion or belief, freedom of opinion, freedom of expression and information, freedom of assembly and association, and the right to equality before the law as well as the right to respect for private and family life.
- Complex issues can also arise when State and non-state actors use new technologies in ways which are discriminatory and abusive, which violate privacy, or which restrict freedom of expression or when new technologies are used for misinformation campaigns, which, at times, can undermine democratic processes.

This is not the first time that a technological leap forward affects security and human rights. What is different in the 21st century is that the newest technological tools available both to states and non-state actors – including instruments such as big data analysis, targeted messaging, biometrics, artificial intelligence or unmanned aerial vehicles – are changing with such speed and power that neither their positive nor negative implications are fully understood or easily managed.

Future technological developments promise to make it even more difficult to assess and properly oversee the development, deployment, and use of technology, whether through existing legal and human rights frameworks or through new guidelines or self-regulatory mechanisms to be developed. Moreover, as development processes and methodologies are not necessarily transparent, relevant actors may face challenges in gaining access to data that allows for oversight of technology-enabled decisions.

The OSCE Security Day will discuss challenges faced by participating States in connection with the design and use of new technologies, including for the purposes of countering security threats, with a focus on ensuring respect for human rights and fundamental freedoms. The discussion will address how States can best implement a comprehensive approach to security when employing technological tools and how such tools can be used to enhance a human rights-centred approach to security. Participants will also be encouraged to consider gender aspects of these issues, including the differences in the technology-related threat environment and the specific impacts of various technological tools on women and men. Appropriate attention will also be given to the role of youth in implementing a human-rights centred approach to security.

As a comprehensive security organization that addresses all dimensions of security across a wide geographic area, the OSCE is uniquely well placed to look at current and emerging issues facing legislators and other policy-makers, state institutions (particularly in the security sector), commercial entities, civil society, academia and other actors in determining how technologies should be used to counter contemporary threats and address new challenges while respecting human rights for all, as well as how technology can be used to promote democracy and human rights, thus strengthening security.

Objectives and expected outcomes

The Security Day will focus on four main objectives:

1) **reviewing and assessing how new and emerging technologies can be developed and employed for positive purposes**, including to promote and advance democracy, human

rights, transparency, accountability and accessibility; to contribute to the fight against transnational threats; and to address other contemporary social, economic or human security challenges such as violence against women and trafficking in human beings;

2) **examining risks inherent in the development and use of such technologies**, including ways they may be exploited with ill-intended purposes and ways in which their use by states and non-state actors may have negative human rights implications;
3) considering how participating States (and perhaps private parties such as NGOs) can implement a gender-sensitive and **human rights-centred approach to addressing implications of new technologies** and rapid technological developments such as machine learning;
4) **identifying lessons learned, best practices, future perspectives and recommendations**, showcasing good examples of how the OSCE and others are using technology to combat threats to security in a human rights-centred way; discussing how technology could evolve in ways that present new opportunities rather than focusing only on challenges.