SUMMARY REPORT

A Human Rights-Centred Approach to Technology and Security

Vienna, 8 November 2019

Overview and Introduction

On 8 November 2019, the Organization for Security and Co-operation in Europe (OSCE) organized a Security Days expert roundtable on "A Human Rights-Centred Approach to Technology and Development" at the Hofburg Palace in Vienna. More than 150 participants from across the OSCE area engaged in an interactive discussion that highlighted 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 addressed 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 also considered 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. Speakers also focused on the role of youth in implementing a human-rights centred approach to security.

At the end of a productive day, OSCE Secretary General Thomas Greminger expressed satisfaction that the Security Days event had contributed to wide-ranging discussion of important topics of clear relevance to the OSCE and its participating States. The Secretary General offered five general observations and five suggestions cited in the final section of this report, which summarizes the

extensive discussions at the event and the suggestions that emerged from them, with the aim of stimulating possible follow up.

This report provides background information drawn from the Concept Note that was available to participants in the Security Day, a synopsis of each session's discussion, and a summary based on the Secretary General's final wrap-up. Further information about OSCE Security Days is available at https://www.osce.org/sg/secdays *further details about the 8 November 2019 event, including videos of the entire proceedings, are available at:* https://www.osce.org/secdays/2019/human-rights-technology-and-security.

Background

At the last OSCE Summit in Astana (now Nur-Sultan) in 2010, OSCE 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 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 information and communications technology (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 may 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.

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.

The Security Day focused 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 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.

Welcome and Keynote Remarks: The human dimension in the digital era

The **opening remarks** highlighted the fact that **digital technologies can be employed both to protect and promote human rights and to undermine and violate them**. Choices made by human beings about the use of new technologies will always be decisive. Social media, emerging technologies and innovative digital tools offer potential benefits for democracy and human rights, to enable freedom of assembly, to build capacities in such areas as human rights monitoring and digital security, to track and trace hates crimes and to promote tolerance and non-discrimination.

At the same time, **abuses of new technologies** to facilitate trafficking in human beings and encourage terrorism, to spread disinformation and hatred, and to perpetrate violence against women **present serious cause for concern**. OSCE participating States are increasingly using new technologies such as biometrics, electronic surveillance, and mass information collection to fight serious crime and terrorism and to manage borders. Yet the same technologies are used in some cases alongside anti-terrorism legislation to suppress human rights defenders, harass and silence political opposition, and repress the civil and political rights of citizens. The Director of the OSCE Office for Democratic Institutions and Human Rights (ODIHR) described how her institution is developing innovative, mobile-based tools to reach human rights defenders and build their capacity on topics such as human rights monitoring and digital security. She also explained how ODIHR contributes to an enabling environment in which human rights defenders can feel safer and can more effectively help the people whose rights they defend, for example by using a purpose-built online digital tool that enables civil society to record and monitor hate crimes and hate incidents. ODIHR also continues to employ digital tools to strengthen election observation processes and enhance cyber security where digital means are used in elections.

It was emphasized that **the Fourth Industrial Revolution**, with its technological innovations flowing from digitalization, **has combined with globalization to profoundly reshape economic systems**. The OSCE has begun to discuss digital transformation and its impact on the labour market, including the potential for economic disruptions to undermine stability.

Given the OSCE's mission to promote sustainable economic growth and foster international economic co-operation to counter security challenges connected with digital transformation, Italy, as OSCE Chair in 2018, focused on the topic **of digital transformation and its influence on the development on human capital in the OSCE area** which resulted in a decision at the Ministerial Council in Milan. As

Chair in 2019, Slovakia built on this theme by focusing on the opportunities and challenges of digital transformation and how to **make new technologies safer.**

A priority is to strengthen cooperation in research and science to foster green and sustainable growth, to address growing privacy and security risks, and to harness efficiency gains that come with emerging technologies in the environmental and energy fields.

It was stressed that **different parts of the Organization are already engaged in many activities that relate to the impact of technology on human rights and security**. Recent examples have included major events focusing on **crime in the digital age** and the use of **artificial intelligence (AI) in policing**, and how the OSCE helps participating States to use technology such as **biometric systems to counter terrorism and to improve border management**. Data aggregation and analysis, blockchain for traceability, artificial intelligence, facial recognition, and monitoring trafficking routes are all examples of OSCE's work to support the use of **technology against trafficking in human beings**.

The OSCE helps participating States in developing national capacities to counter the use of the Internet for terrorist purposes, consistent with commitments to freedom of expression and of the media. In the arms control field, participating States use technologies provided by the OSCE to reduce the risk of conflict. The OSCE Special Monitoring Mission to Ukraine increasingly uses technology to enhance its ability to monitor developments in eastern Ukraine: satellite imagery, UAVs and fixed surveillance camera systems have given the Mission access where it has been restricted, enabled monitoring at night, and reduced risks to monitors, and facilitated responses to ease the humanitarian consequences of the violent conflict.

Technology can help reduce risks to the economy and the environment. A newly designed project aims to increase the capacity of participating States to use innovative open data tools and new digital technologies. An OSCE e-learning platform hosts an online training course on good governance and anti-corruption and will soon also add a Virtual Competency and Training Centre for the Protection of Critical Energy Networks, illustrating the potential of capacity-building through on-line tools.

In her **keynote speech,** Dunja Mijatović, Commissioner for Human Rights, Council of Europe, cautioned that technological development can be an **accelerator of such negative phenomena as aggressive nationalism and terrorism**, fomenting new tensions and polarization, and elevating their ability to undermine security and the democratic fabric of our society. **Technology creates new opportunities** in such fields as health care and employment, and even to strengthen human rights protection, **but it can also be turned against users, and restrict people's rights**.

Large amounts of **personal data is collected and are used to profile us**. Another alarming phenomenon is the **relationship between technology companies and state security** agencies, which has become closer in response to terrorist threats and attacks. States have **increased surveillance** and used it to **silence criticism, restrict free assembly, "snoop" into private life, or control individual**s or minorities.

Regarding AI, **there is evidence that women, older people, minority groups, people with disabilities, LGBTI and economically disadvantaged persons particularly suffer from discrimination through biased algorithms**.

Digital technologies are often used to manipulate public opinion. Disinformation, incitement to hatred and violence have been propagated by tricking the algorithms of some social media platforms. This has contributed to instilling fear and pushing the frames of anti-democratic movements and parties.

Attention was drawn to the **Recommendation on Artificial Intelligence** that the Commissioner for Human Rights of the Council of Europe (CoE) published in May 2019, based on existing standards to help guide member states to maximize the potential of AI systems and prevent or mitigate the negative impact they may have on people's lives and rights, focusing on **10 areas of action**. One such area relates to the **obligation of governments to ensure that business enterprises abide by human rights** standards, to ensure that private companies which design, develop or use AI systems do not violate human rights standards.

Conclusions and recommendations:

- The OSCE should engage with technology companies to make sure that their tools enhance human security and human rights rather than undermine them, and that men and women benefit equally from this.
- It is in the interest of all states to come to agreement about the use of the digital space, like a "rulebook" to decrease the risk of conflict and improve conditions for peace and security. OSCE human dimension commitments provide a frame that can be built on.

- Digital technologies are reaching further into society and economy with more connectivity, further integration with everyday life activities, and less privacy. This will demand a response from all stakeholders.
- OSCE is well placed to address the opportunities and security challenges connected with digital transformation and help the participating States to find ways to increase cooperation in this area from the perspective of all dimensions including the human dimension.
- OSCE participating States should work together to enhance digital governance, to promote guidelines for the ethical and socially beneficial use of emerging ICT in our societies, to promote safer and more inclusive technologies, and to integrate a gender perspective to generate a positive impact on society.
- Ensuring that technological development works for and not against human rights, democracy and the rule of law is one of the biggest tasks that States must face.
- States should reinforce their monitoring of human rights compliance by AI systems and act anytime there is an infringement of these rights. They should strengthen independent oversight and empower national human rights structures to engage in this field.
- It is crucial to keep human control and human liability in relation to AI. More generally, digital transformation should be human-centric or human-oriented.
- The May 2019 **Recommendation on Artificial Intelligence** by the CoE Commissioner for Human Rights can help guide states to maximize the potential of AI systems and prevent or mitigate the negative impact they may have on people's lives and rights.
- States should promote digital literacy among the population, and in particular in schools, in order to help people understand how the digital world works and recognize when it harms.

Technology for Security

The first thematic session focused on positive uses of technology to promote security. Attention was drawn to the recent decision by the President of the **OSCE Parliamentary Assembly** to appoint a **Special Rapporteur on the Digital Agenda**. In her introduction, the first incumbent of this new post, Stefana Miladinovic, said that she will work as a "pioneer" in addressing these issues with a focus on the potential of the Fourth Industrial Revolution and digital transformation to provide positive benefits, including for public services and fighting human rights violations.

It was noted that **lessons learned from the uses and misuses of technology in the context of trafficking in persons could be applied** in other areas of endeavor. **Trafficking violates rights of numerous persons and constitutes a security threat**, a great source of insecurity and a phenomenon that thrives in conflict. While there is a tendency to glorify "fun" tech tools to combat trafficking – with over 300 tools available – trafficking continues with an estimated 25 million victims and less than one-tenth of one percent of traffickers are prosecuted. An example of good practice for combating child trafficking is a chat bot developed to talk to online predators until they can be arrested. **Real-world experience poses challenges**, such as the need to address tensions among different rights (freedom of expression versus freedom from online harassment).

While technology companies emphasize positive uses of their products, they also recognize **that new challenges and nefarious uses of technology are emerging.** These include fields like trafficking, election security, and the need to protect freedom of expression. Sometimes companies have tools not available to law enforcement, but they do not have authority to prosecute criminals. **Companies recognize that they have responsibilities, but need to balance pressures** from both law enforcement and civil society.

Global companies also face **tensions among different values in different regions**; they might be comfortable adopting proactive measures in one jurisdiction but not in another. At the same time, certain companies will always be willing to develop technologies that governments want (without regard, for example, of human rights or privacy concerns). **Responsible companies would like to see more regulation in fields like AI** and facial recognition to prevent "creepy" or intrusive uses of such technology. To counter election interference, **companies are working to identify how bad actors attack democratic practices** and contribute with new protocols and programmes for electoral bodies. Recognizing that technology platforms exacerbated the ChristChurch tragedy, many have joined the "ChristChurch call" to take down certain content.

The session provided a forum for demonstrating how **the OSCE Special Monitoring Mission to Ukraine (SMM) has developed its technological capacity since 2014 to become "a living embodiment of using technology for security."** Despite the modest size of the Organization, the OSCE is now a leader in using cameras, UAVs, and a technical monitoring centre to compile information every day, all day about the state of ceasefire implementation. The SMM uses imagery not only to monitor and record ceasefire violations and the location of heavy weapons but also to raise awareness, for humanitarian purposes and ultimately improve the lives of people in Ukraine. It was pointed out that **data on such issues as the location of mines should be able to inform post-conflict rehabilitation** "when the guns fall silent." The SMM thus demonstrates how technology can benefit the OSCE's work in the field.

One participant emphasized that **ethical questions always arise about the uses and possible limitations on the use of technology**. While the technologies now under discussion are new and more powerful than anything previously developed, we continue to face the same "old questions" about what human beings are doing with technology and how far they may limit its use. Another participant

pointed out in this context that the challenges are not new but the scale in cyberspace is new, as we see "how horrible things can be, on a much greater scale."

Conclusions and recommendations:

- There is good potential for synergy among efforts undertaken by the OSCE Chairs, the OSCE Parliamentary Assembly and the OSCE Secretariat to highlight and foster positive uses of technology to promote security and economic prosperity.
- The SMM uses imagery not only to monitor and record ceasefire violations and the location of heavy weapons but also to raise awareness, for humanitarian purposes and ultimately improve the lives of people in Ukraine.
- More should be done to capture, learn and share lessons from the SMM's experience of using technology.
- States and international organizations should build trust and partnerships with the private sector, civil society and law enforcement in order to use technology for such positive purposes as to combat trafficking in human beings.
- OSCE has a fundamental role in developing the policy responses to such challenges as identifying how to best use technology to combat trafficking.
- Technology companies face challenges in balancing pressures from law enforcement and civil society; responsible companies would welcome well-intentioned regulation in fields like AI and uses of facial recognition software.
- While the OSCE is already using technology for capacity building, it should continuously identify, invest in, and deploy new technologies to do this work even more effectively.

Risks of Technology

The second thematic session focused on the **key risks and challenges of emerging technology** for all dimensions of security. From a human rights perspective, despite the huge opportunities that new technologies present for the exercise of rights and freedoms, **challenges include the potential use of the same technologies to target human rights defenders by surveillance, for Internet blocking and filtering as well as censorship** practiced in some participating States. Among issues addressed by the Human Dimension Committee of the OSCE Permanent Council are **disinformation and propaganda, preventing online violence against women with tech, and the need for citizens to have enhanced access** to information.

Non-governmental experts identified various risks that may be associated with the use of new technologies. These include the risk that accounts may inadvertently be compromised and then abused by a third party. Other risks relate to the fact that **technology is developed by humans who may invest it with their own biases**; this is a potential problem with machine learning tools, designed to aid recruitment processes, which may foster discrimination because of the way that algorithms are written.

Another category of risks relates to **deliberate misuse of data** collected through the use of technology, for example to keep tabs on critics of the government in power. Such risks are particularly prevalent in the fields of privacy and free speech; for example, expanding CCTV surveillance combined with facial recognition software (for the purposes of deterring common crimes or countering terrorism) can infringe on personal privacy. Such tools, which are being used increasingly in a number of states, could allow for mass surveillance or manipulation, as the actions of every citizen would be transparent to the government.

Technologies deployed in "liberal" states may be abused elsewhere; an example is the legislation in one participating State on voluntarily removing illegal content from social media by tech companies using automated content moderation tools which has been copied by some authoritarian states.

Several speakers identified **risks associated with AI tools relying on algorithms**, due in part to the absence of transparency about their development and the difficulty that many people face in understanding them. Questions were raised about how evidence developed with such tools might be handled by courts, whether governments are able to assess the risks of relying on algorithms, and

what unintended consequences there might be. It was suggested that "**human rights due diligence" may be needed** to foresee possible consequences of using new tools.

With regard to the risk of disinformation and propaganda, speakers identified media diversity and education as important elements in building resilience of citizens.

Conclusions and recommendations

- States should not only refrain from practices which contravene human rights, but also take positive steps to provide space for civil society engagement.
- New technologies should have human rights protections built-in by design.
- Catch-all use of facial recognition should be avoided.
- It is not necessary to reinvent the wheel but rather to apply the existing human rights framework. Standards exist which should be applied to technology issues.
- There is no common agreement about the extent to which new standards are needed, even among and within civil society; openness and transparency are key.
- In considering new initiatives and legislation, it is important to look at the existing human rights framework and undertake broad consultations, including with civil society.

A human rights-centred approach to rapid technological change

The third thematic session considered the fundamental challenge of developing **policy approaches to fast-paced innovation** and change. It was noted that political systems bear responsibility for defending human rights but that "politics are catching up after the facts," as technology development follows the logic of "move fast and break things."

It was observed that states, institutions and individuals are now delegating decisions that are very "human" to algorithms and machines. The question raised by such developments is how the state may react to make sure these decisions are for benefit of human beings. **Concerns arise when decisions made by algorithms are not transparent to individuals.**

Various international organizations have stepped in to help. As highlighted in the keynote address, for example, the Council of Europe's Commissioner for Human Rights has developed recommendations for states to consider the implications for human rights whenever deploying AI and algorithms. The OECD's AI Principles are also relevant as an example of the ways that the international community is starting to fulfil this positive obligation. The United Nations is contributing to this work in a number of ways. For example, the UN's Guiding Principles on Business and Human Rights were unanimously endorsed by the UN Human Rights Council in 2011 as a set of non-binding standards to be applied voluntarily by ICT and other companies.

Significant work is being done in this field by various special procedures of the UN Human Rights Council with support from the UN Office of the High Commissioner for Human Rights (OHCHR) in cooperation with the private sector. Specific UN mandate holders, such as the Special Rapporteur on Freedom of Expression, are looking at challenges that new technologies raise in a human rights context. Other mandate holders looking at particular technology issues include the Special Rapporteurs on Cultural Rights, on Extreme Poverty, on Freedom of Assembly and Association, and on Racism. Another often overlooked area requiring a human rights-centred approach is the work of technical standard-setting bodies.

It was observed that **governments and traditional institutions are not sufficiently prepared to address many of the developments which are largely in the hands of huge monopolies**. The result is that "innovations made in Silicon Valley may end up the European Court" [of Human Rights] in Strasbourg. It was suggested that one must return to the basic framework of ensuring respect for fundamental rights but also that it is necessary to adapt policies and development regulations which are based on interdisciplinary research. Given the challenge of developing appropriate regulations that would be implemented over an extended period of years and of determining how certain technologies are going to affect the lives of individuals, the possibility of **considering moratoriums on certain technologies** was raised.

With regard to freedom of expression, it was noted that the existing standard contained **in Article 19 of the International Covenant on Civil and Political Rights is sufficiently broad** to cover "any means of communication" with appropriately narrow grounds for any limitations. It was suggested that research on such challenges as disinformation is quite incomplete and that contemporary discussions focus too much on possible restrictions rather than the importance of sustainability of journalists and journalism in the social media era. It was also suggested that **states have a positive obligation to ensure pluralism and diversity online** through the use of such tools as competition authorities, vertical "unbundling" of services, and oversight of content moderation practices employed by social media companies. The **use of new technologies by governments to target human rights defenders and independent journalists was cited as a significant problem** in some countries.

With regard to determining whether particular online content should be removed, it was emphasized that **any judgement about alleged illegality of content must be subject to judicial oversight**. Different issues arise when companies remove content from their platform (citing community standards, for

example, in removing pornography); while not a strictly legal issue, such practices raise questions about consistency of approaches and transparency that emphasize the need to have stronger guarantees for users on the "de facto public square." Specific **challenges arise when content is removed not by humans but by AI-driven technology.** Non-governmental activists focus in this context on the need for improving accountability systems and for independent oversight of what companies are doing, including judicial oversight but also through such mechanisms as "social media councils."

The importance of **data protection impact assessments** was highlighted in the context of government efforts to employ new technical tools, including facial recognition, to increase security and deter crime. The **combination of video and facial recognition technologies was described as a significant challenge**, in particular when such technology was not developed under a human rights-centred approach or with concern about basic privacy principles. AI expertise and more research would be necessary to determine how to get more benefit instead of harm from deploying such tools.

A **scenario involving the introduction of autonomous self-driving vehicles in an urban environment** was used to identify human rights issues associated with such a technological change. Panellists highlighted the importance of **transparent public discussion involving civil society** and other stakeholders on the need for the technology and its **possible impact on human rights** as well as issues relating to **legal liabilities**, impact on **employment and economic life**, **non-discrimination and equality**, **climate change, and sustainability**. It was suggested that the deployment and impact of technological innovations should be considered in the context of their possible role in promoting or hindering implementation of the **Sustainable Development Goals**.

Conclusions and recommendations

- The UN Guiding Principles on Business and Human Rights provide a framework for dealing with many issues raised by new technologies.
- Many international organizations including the UN Office of the High Commissioner for Human Rights (OHCHR) and the Council of Europe are considering how to ensure a human rights-centred approach to technology issues.
- Much work is being done by the special procedures of the UN Human Rights Council with the support of OHCHR in cooperation with the private sector.
- The need for a human rights-based approach to the work of technical standard-setting bodies is crucial but often overlooked.
- A holistic approach is needed when deploying human rights-compliant technologies, including consideration of what this means for developers

Lessons learned, best practices and future perspectives

The fourth and final thematic session provided a platform for discussion of some **ways in which technology is being used to promote security and well-being along with future perspectives**. The session included a particular focus on the way that new technologies affect **youth and gender equality.**

A specific example presented to the participants was the PREVIEW system used by the German Federal Foreign Office to analyze open-source data to improve early warning capacities. The tool contributes to predictions of terrorist attacks and violent conflicts, also helping to identify hot areas in conflicts at even the very local level through heat maps. The promise of such a tool is that it has the **potential for data-driven analysis to contribute not only to crisis management but also to crisis and conflict prevention**. In considering risks, it was acknowledged that the usefulness of such a tool will be dependent in part on the reliability of the raw data that is entered into it. Another risk is that some might believe that such a tool would "run by itself" and provide answers to complex analytical problems, rather than serving as a planning tool. It was stressed that the **PREVIEW** tool provides just **one of the sources to inform decision-making, to be used carefully and in combination with qualitative analysis.**

From the perspective of a leading Russian technology company, it was explained that **AI and robotics are important emerging technologies with huge potential to improve everyday lives**. Like any new or emerging technologies, it was acknowledged that AI and robots could be also used for nefarious purposes. While **AI therefore needs to be regulated** to deal with such risks as bias and discrimination, it was argued, **modern societies should proceed with implementation in order to reap substantial benefits for improving human lives**. A review of the current situation suggests that AI is already subject to regulation at four levels: ethical rules; self-regulation by key players in the tech industry (including a major consortium involving Microsoft, Apple, Facebook, and Google – known as the "Partnership for AI" – and a newly-created Russian "AI Alliance"); national regulation; and supra-national regulation. **National AI development plans or strategies are in place in more than 35 countries.** Supra-national regulation efforts are underway or under discussion in multiple forums including the European Union, the Council of Europe, the United Nations, the G20, UNESCO and the Organisation for Economic Cooperation and Development (OECD). At least 136 different multilateral "rules and principles" are already on the table. The view was expressed that the **OSCE could play a role in facilitating discussion of critical**

issues, perhaps in conjunction with the academic world and specifically with involvement of the OSCE Network of Think-Tanks and Academic Institutions.

Participants in the session received a detailed briefing on the technology-related work of the Core Group of Experts in the OSCE Perspectives 20-30 Youth initiative, which produced a comprehensive paper on the future of European security to be presented to the OSCE Ministerial Council Meeting in Bratislava. The section of this paper on new technologies urges the OSCE to consider **ethical guidelines for the use of AI, to address issues that relate to autonomous weapons systems, to share good practices and convene dialogue on technology issues, and to facilitate exchanges between smart cities.** A youth expert observed that national education systems are not often ready to respond to disruptive technologies. Among awareness-raising and educational challenges are the need to create broader understanding about the human rights implications of new technologies and more generally to **improve digital literacy and computer skills**. These tasks imply the need for **life-long learning**, taking into account that training on technology issues may be needed by members of the older generation in particular.

Looking at the specific implications of rapid technological development for different age groups, it was noted that **youth and older people tend to use tech in different ways**. Youth typically use social media as their main sources of news and information, and are deemed to be most vulnerable to manipulation. These challenges can be compounded among groups that lack sufficient technical skills and particularly among those with limited critical thinking skills. Youth are targeted also by extremists for recruitment.

Reflecting on the ways in which **new technologies may have different impacts on women and men**, it was noted that women constitute only about 20 to 30 percent of experts on new technologies. Special efforts are needed to include women, particularly in coding and other functions where bias may be introduced into programmes and algorithms. There are positive examples including organized groups of women in AI that have helped women advance, and Slovakia was cited as an example of empowering women in the IT sector. The need to demystify the sector and encourage more engagement by women was nevertheless underlined.

Conclusions and recommendations

- Quantitative data detection and analysis models can improve prediction capabilities regarding developments that may affect security and thus provide a basis for conflict prevention.
- Care must be taken to avoid over-reliance on quantitative or technological solutions, to the exclusion of qualitative assessments by human analysts.
- Regulation of AI and robotics are needed to ensure that humans reap benefits from them.
- There is much ongoing work to regulate AI and robotics at four levels: ethical guidelines or principles, self-regulation, national regulation and supra-national regulation.

- More than 35 countries in the world now have national AI strategies; virtually every international body is now working on these issues, and OSCE might play a role in facilitating discussions on the impact of technology on human rights and security.
- Women are under-represented in the new technology sector; special efforts are needed to include women, particularly in coding and other functions where bias may be introduced into programmes and algorithms.
- Different age groups use tech differently. Youth are most vulnerable to manipulation, but at the same time can profit most from new using new technologies.
- Tech can serve as tool for empowerment and youth activism.
- Public procurement can drive innovation, to promote use of technologies and applications that are secure, private and ethical.

Closing remarks by Thomas Greminger, Secretary General of the OSCE

In his concluding remarks, OSCE Secretary General Thomas Greminger expressed satisfaction that the Security Days roundtable had contributed to a broad ranging discussion of important topics of clear relevance to the OSCE and its participating States.

The Secretary General offered five general observations and five suggestions summarized below. He wrapped up the Security Days event by expressing gratitude to all the speakers and moderators as well as to those participating States that contributed financially to the event.

Summary

Observations:

- This is a big and complex topic, and it will probably get bigger and more complex in the future. In terms of security and human rights, tech is both part of the problem and part of the solution. Therefore, it is something that the OSCE needs to focus on.
- It cuts across most of the work that the OSCE does. And it transcends borders. So there must be joined-up responses.
- The OSCE, with its comprehensive approach to security, is well-suited to deal with the impact of technology on human rights and security.
- The impact of digitalization and technology on security is greater than the topic of this Security Days event. It also relates to the first dimension, eg. lethal autonomous weapons systems, or the malicious use of new technologies by terrorist and criminal networks. It also relates to the second dimension of the OSCE's work in terms of human capital, the impact of automation, critical infrastructure, and green technology – to name a few examples.
- In a digital age, we need to keep the focus on human beings: to ensure that people are empowered and protected rather than put at risk, made to feel insecure, or become victims of a digital divide. And we need to ensure that humans maintain control over, and are accountable for, increasingly autonomous forms of artificial intelligence technologies.

Suggestions

- First, concerning norms and guidelines, it is clear that others (like the UN and the Council of Europe) are well ahead of the OSCE. The OSCE should not duplicate these efforts, but should follow – and learn from – relevant debates, reports and outputs of these organizations. At the same time, there are certain topics where the OSCE has a clear role and comparative advantage based on its experience. It should therefore provide guidance, for example in relation to cyber CBMs, gender equality, tolerance and non-discrimination as well as national minorities, media freedom and democratic governance.

- Second, the OSCE should focus more on how technology can help participating States implement their commitments, to counter security threats in a way that ensures respect for human rights and fundamental freedoms. Examples mentioned during the Security Day include tech against trafficking, the use of biometrics to better manage borders and prevent terrorism, as well as a growing range of tools to

fight cyber-crime. The OSCE should continue its work in this area – to build capacity, share knowledge, and strengthen networks.

- Third, the OSCE should help States deal with the challenges and opportunities that arise because of technological change. This is relevant for all three dimensions of the OSCE's work: including, for example, the impact of cyber attacks, violent extremism and hate crimes on the Internet, technology as an enabler of organized crime, threats to critical infrastructure, digital transformation and the workforce, how social media are transforming political participation.

- Fourth, technology should be used more effectively to make the OSCE more 'fit for purpose'. This includes:

  - Using technology to enhance efficiency, information and work flow, as well as security;

  - Smart technology in field activities and mediation. And smart use of the information that we gather;

  - Technology for training: both in terms of greater use of on-line tools, as well as ensuring staff have the necessary skills and knowledge;

  - And technology for communication – internal, and in communicating with the public.

  - All of this will require sufficient financial, human and intellectual resources.

- Fifth, ensuring a human rights-centred approach to technology and security requires partnerships. As a UN report put it, we need "digital cooperation" in an age of "digital interdependence". The OSCE should therefore build on this Security Day: to involve all parts of the OSCE – participating States, executive structures, and the Parliamentary Assembly – together with partner organizations, the private sector, civil society, youth, and the media. Because of the nature of this topic, we need to take a "systems" approach, and to enhance benign networks against malign ones. Since security and human rights are at the core of the OSCE, the Organization is well-placed to provide a platform for such conversations, and to facilitate networking and dialogue.

ANNEX 1

Agenda and Guiding Questions

09:00 – 09:45 *Registration and welcome coffee*

09:45 – 10:45 **Welcome and Keynote remarks: *The human dimension in the digital era***

Thomas Greminger, OSCE Secretary General

Ambassador Radomír Boháč, Permanent Representative of Slovakia to the OSCE, Chair of the OSCE Permanent Council

Ingibjörg Sólrún Gísladóttir, Director, OSCE Office for Democratic Institutions and Human Rights

Dunja Mijatović, Commissioner for Human Rights, Council of Europe

10:45 – 12:00 **Session 1: *Technology for security***

Moderator: Ambassador Luis Cuesta Civís (Spain), Chair of OSCE Security Committee

Stefana Miladinovic, Special Rapporteur on Digital Agenda, OSCE Parliamentary Assembly; Member of Parliament of the Republic of Serbia

Valiant Richey, Special Representative and Coordinator of OSCE Activities for Combating Trafficking in Human Beings (OSR/CTHB)

Jeremy Rollison, Director of EU Government Affairs, Microsoft

David Campion, Operational Support Officer, Conflict Prevention Centre, OSCE Secretariat

Questions that may be addressed:

- How can individuals, civil society organizations, academia and the private sector make effective use of new technological tools to enhance the exercise of fundamental human rights? To foster citizen participation and improved compliance with OSCE human dimension commitments?

- What are the opportunities created by new technologies for an improvement of international co-operation in tracking, apprehending and gathering evidence for combating

terrorism, trafficking, other forms of organized crime, or cyber-crime and how are they being developed/implemented to reinforce the applicable human rights framework?

- How can these technological tools be used to prevent and counter phenomena such as intolerance and discrimination, disinformation, abuse, harassment, and VERLT, while at the same time respecting human rights and fundamental freedoms, including the rights to freedom of movement, freedoms of opinion, expression and association, equality and non-discrimination, as well as the right to privacy?

- How can States promote the development and use of human-rights based technological tools and provide them to the general public?

- How can a positive role be played by public-private partnerships between state authorities and the private sector (business community, industry)?

- How can media, information and communication, and the technologies which enable them, sustain spaces for inclusive and pluralistic deliberation and facilitate integration of diverse societies?

12:00 – 12:15 Coffee Break

12:15 – 13:30 Session 2: *Risks of Technology*

Moderator: Georgia Holmer, Adviser, Action against Terrorism Unit, Transnational Threats Department, OSCE Secretariat

Ambassador Ivo Šrámek, Permanent Representative of the Czech Republic to the OSCE, Chair of the OSCE Human Dimension Committee and of the Forum for Security Co-operation (FSC)

Melody Patry, Advocacy Director, Access Now

Jacob Mchangama, founder and director of Justitia, Copenhagen

Questions that may be addressed:

- What are the main risks that new and emerging technologies will be used, by States or non-State actors, intentionally or inadvertently in ways which negatively affect the exercise of human rights and fundamental freedoms? How can OSCE participating States counter these risks?

- What new challenges confront states implementing existing OSCE human dimension commitments while countering security threats in an era of rapid technological change? Do

we need to consider independent oversight and rules for transparency in the use of machine-learning technologies?

- What are the main risks, including for privacy and data protection, of new and emerging technologies enabling the gathering, storing, processing and sharing of data and information in the name of security – including for policing and border control, surveillance and monitoring of public spaces (online and offline)?

- What data exist about the ways that terrorists and other criminals or those spreading hatred, intolerance, disinformation, and violent extremism that can lead to terrorism may be exploiting new technologies to further their aims?

13:30 – 14:30 ***Lunch***

14:30 – 15:45 **Session 3:** ***A human rights-centred approach to rapid technological change***

Moderator: David Mark, Human Rights Adviser, OSCE ODIHR

Karmen Turk, Partner, law firm TRINITI; Lecturer in the University of Tartu, Estonia

Barbora Bukovska, Senior Director for Law and Policy, Article 19

Djordje Krivokapic, Assistant Professor, Faculty of Organizational Sciences, Belgrade; Ethics Consultant

Beatriz Balbin, Chief, Special Procedures Branch, Office of the United Nations High Commissioner for Human Rights

Questions that may be addressed:

- Drawing on the OSCE's experience in capacity building as well as in providing guidance on legislative frameworks and policy approaches in such sectors as law enforcement and good governance, how can participating States ensure that the use of new technologies will promote human rights and fundamental freedoms and enhance comprehensive security? How can co-operation among States be enhanced?
- What is the role of national policy and international co-operation in establishing standards, regulating practices by private entities, and/or encouraging self-regulation where appropriate? What steps are necessary to guarantee that civil society is able to contribute to the dialogue on these issues and play an appropriate role in a "whole-of-society" approach to the formulation, implementation, review and oversight of relevant policies?
- The UN Guiding Principles on Business and Human Rights highlight the ICT industry's responsibility to respect human rights. What challenges arise for the ICT sector to avoid

being involved in harm to individuals' human rights if states are unwilling or unable to implement their human rights commitments?

15:45 – 16:00 *Coffee break*

16:00 – 17:00 **Session 4:** ***Lessons learned, best practices and future perspectives***

Moderator: Doug Wake, Senior Expert, Strategic Policy Support Unit, Office of the OSCE Secretary General

Marian Weimann, Desk Officer, Division for Early Warning, Strategic Perspective, Conflict Analysis and Center for International Peace Operations, Federal Foreign Office, Germany

Andrey Neznamov, Executive Director, Regulation of Robotics and Artificial Intelligence, Sberbank JSC

Katarina Kertysova , Member of the Core Group of Experts, OSCE Perspectives 20-30 Initiative

The final session will showcase good examples of how the OSCE and others are using technology to combat threats to security and address other challenges in a human rights-centred way. The discussion could furthermore address how technology could evolve in ways that present new challenges and opportunities.

17:00 – 17:30 **Conclusion:** Thomas Greminger, OSCE Secretary General