OSCE PA President George Tsereteli

Address to the Lisbon Conferences of the OSCE Parliamentary Assembly

Digital Resilience of a Democratic State

Assembly of the Republic of Portugal, Lisbon

8 May 2018

Check against delivery.

First of all, I'd like to thank the Assembly of the Republic of Portugal for organizing this conference, which is both timely and important.

In this era dominated by debates about fake news, cybersecurity, online radicalization, and data protection, it is essential that we come together to discuss these issues.

In the OSCE Parliamentary Assembly, we have been increasingly focused on cybersecurity for the past decade. We adopted our first resolution on the topic in 2008, identifying cyber threats as some of the most serious security challenges of our time. Over the past ten years, these challenges have only grown.

Our Members will recall that during our latest Autumn Meeting in Andorra, we discussed how cyber threats can jeopardize the way of life of modern societies and the whole of civilization.

In our increasingly digital world, armed conflicts are not the only breeding ground for threats against governments and citizens. In cyberspace, we see new challenges emerging and old challenges evolving.

Whether the issue is child sexual exploitation, terrorist recruitment, or crimes such as identity theft and fraud, the internet offers new opportunities for criminals and extremists. We must respond effectively and ensure that the response is proportionate.

Currently, there are policies being pursued by the United States and European Union to relax international rules for cross-border law enforcement investigations of cybercrime. While these rule changes might be well-intentioned, what we don't want is a race to the bottom of weaker privacy protections around the globe.

While addressing these problems, in other words, we must always uphold the highest standards of respect for fundamental freedoms.

Recognizing the essential role of co-operation between governments to cope with modern security risks, we should revise existing legal frameworks and harmonize relevant legislation to make international co-operation more effective and efficient. All actors and stakeholders must search, in good faith, for solutions based on international law in a way that does not infringe on freedom of information or individual privacy.

Although governments often see cybercrime through the lens of threats to state security – whether the protection of digital infrastructure or ensuring the protection of state secrets – our citizens are no less vulnerable to cybercrime and breaches of their personal data. We saw recently the damage done by the Cambridge Analytica data breach, which affected millions of Facebook users.

These people had their personal data collected and inappropriately sold to politicians to advance political agendas and careers. The scandal raised important legal and ethical questions about the nature of privacy in a digital age. For example, what are the implications for democracy when extremely detailed personal data can be used by skilled political operatives to influence public opinion?

While Facebook has been in the spotlight, this sweeping data collection is an issue throughout cyberspace. This raises the fundamental question of whether internet users should expect any privacy protections at all.

After all, technology is not good or bad in and of itself. It all depends on the people who use it.

When intimate and detailed knowledge of citizens' views can be collected and sold to the highest bidder, citizens become prime targets for fake news campaigns and propaganda. This, in turn, can have dire consequences for the functioning of democracy.

There has been much speculation that recent elections have also been the target of cyberattacks. Whether electoral outcomes have been affected or not is a matter of debate, but what is not a matter of debate is that this possibility is troubling. And even if past elections have been secure, there is no reason to assume that future elections will remain secure, so we must make every effort in protecting our electoral systems from hacking.

I hope that in this forum, we can exchange best practices, develop confidence-building measures, and find the most effective ways to build resilient democracies that protect against cyber threats while also protecting freedom of information and personal privacy.

British novelist Phyllis Bottome once said: "There are two ways of meeting difficulties: you alter the difficulties, or you alter yourself to meet them."

I think we can all agree that technology has offered great advances for our civilization. It has helped to connect the world, share knowledge, promote commerce, and to advance democratic development.

Take for example our own Parliamentary Assembly, where we are now all connected through our smartphones, and able to share and gather information as fast as ever. In this era of digital diplomacy, we should realize that the internet can also help solve foreign policy problems.

Dear colleagues and friends,

What we now must do is make sure that this technology is secure so that the challenges of the digital age are managed in a way that ensures both security and liberty.

It is up to us to make sure that modern technology remains a useful servant and not a dangerous master.

I once again thank the Assembly of Portugal for organizing this important conference, and I look forward to exploring these topics in greater detail with you all.

Thank you.