ADDRESS BY MAKIS VORIDIS,

CHAIR OF THE OSCE PA AD HOC COMMITTEE ON COUNTERING TERRORISM

International Conference: Digital Resilience of a Democratic State

Session 4: The Threat of Cyber-Terrorism in the OSCE Area

Lisbon, 8 May 2018

Check against delivery.

Dear Moderator,

Honorable Guests,

Ladies and Gentlemen,

To begin with, I would like to commend the Portuguese Parliament for hosting this important event and for giving me the opportunity to address you in my capacity as Chair of the OSCE Parliamentary Assembly's Ad Hoc Committee on Countering Terrorism. Let me also thank Prosecutor Verdelho and Ambassador Mira Gomes for their thought-provoking presentations and insights on the Portuguese experience.

Before telling you more about the work of our Committee, I would like to share some views about the complex challenges that we are facing in countering cyber-terrorism in the OSCE region and how we, as parliamentarians, can help to address them.

Digitalization and information technologies have become indispensable tools in our everyday life, where using them is not a matter of choice, but a necessity. The 2018 Global Digital report reveals that over four billion people around the world use the internet. In addition, more than three billion people use social media, with nine in ten of those users accessing their chosen platforms via mobile devices. Finally, the reported total value of e-commerce in 2017 reached almost US$ 1.5 trillion. This data shows how our community is quickly transforming into a fully digital society, with important security implications.

Against this backdrop, it is self-evident why risks related to cyber-terrorism are growing exponentially: last year, for instance, the WannaCry attack impacted more than 10,000 organizations, including major hospitals and companies, in 150 countries around the world. In addition, we have all witnessed how Daesh/ISIL and other criminal organizations have used the

web to disseminate their radical ideologies and spread fear in our societies. Finally, the recent Cambridge Analytica scandal, one of the biggest data breaches in history, while not being a cyber-terrorism attack itself, should give us a wake-up call: it proved that public opinion can be easily manipulated online. Skilled terrorists could use similar methods to recruit individuals who feel disenfranchised or alienated from society.

As the politically motivated use of computers and information technology to cause severe disruption and widespread fear, cyber-terrorism usually refers to:

- The direct hacking and disruption of critical online networks, and;
- The use of the internet and of social media platforms to foster violent extremism and radicalization, as well as to directly recruit terrorists.

These might appear just as some additional definitions, but definitions in our line of work do matter. In fact, without a clear understanding of what we are looking at, we can't fully focus our efforts and be effective. Unfortunately, the global legal framework to address these challenges is still minimal. For example, while the Council of Europe (Budapest) Convention on Cybercrime is certainly a step in the right direction when it comes to promoting legislative harmonization, investigative techniques and international co-operation, its reach is "only" regional and its content could benefit from some "updating" (signed in 2001). Clearly, there is an urgent need to fill in this vacuum with global instruments which adequately reflect the latest cyber threats.

Allow me now to highlight some challenging areas where action is urgently required.

First: to address cyber-terrorism more comprehensively, it is paramount to broaden the array of stakeholders involved and include relevant counterparts from the cyber/ICT sector. A powerful tool in this context is the creation of strong public-private partnerships (PPPs), as structured coordination with ICT companies is paramount to better understand and properly address the technological challenges we are facing.

Two cases in point are the Global Internet Forum to Counter Terrorism (GIFCT), which includes major companies such as Google and Facebook, and the Tech Against Terrorism platform. While the GIFCT is working on technological solutions to help thwart terrorists' use of the internet, the second platform aims at building capacity for smaller ICT companies on the issue. This is particularly important: as also reported by the UN Counter Terrorism Committee, smaller companies, with less resources, are much more vulnerable to terrorist organizations because they have no means to control how their platforms are used. However, such channels are no less powerful, or less reaching.

Second: it is important that we do not compromise our fundamental freedoms while safeguarding the security of the citizens. When looking at online terrorist propaganda, meeting both objectives requires new thinking on what is the content to ban, as well as on how to ban it. Again, without a clearer understanding of what can be considered terrorist propaganda, even in its more subtle forms, we often lack the capacity to adopt comprehensive strategies to counter

terrorists online. Critical support should also come from individuals: some countries have established online platforms where citizens may easily report to authorities any materials promoting terrorism, or suspected to do so.

Third: there is a need to strengthen information sharing channels at local, national, regional and international levels. This is to ensure regular and reliable exchange of operational data aimed at enhancing counter-terrorism preventive and response mechanisms. For instance, it is key to develop and fully integrate our databases to facilitate timely exchanges among key stakeholders, including under the guidance of international bodies such as INTERPOL.

Moreover, we should regularly train our security providers on the latest cyber-terrorism trends and enable them to quickly collect information and evidence on-line while respecting fundamental freedoms. The current efforts of the European Union to expedite cross-border access to evidence in criminal matters are encouraging. Ultimately, whilst addressing terrorism on a political level remains important, States need to seek more technical expertise on the issue and get, so to say, their hands deeper in the pie.

Ladies and gentlemen,

Moving to the specific role that parliamentarians, as representatives of the people, should play in responding to these challenges, I would focus on three elements:

The first is our policy-making function - We should, first and foremost, promote effective policies to bridge loopholes in our national counter-terrorism frameworks and develop targeted strategies to respond to cyber-terrorism in a human rights-compliant manner.

The second is oversight - We must support the work of our governments, law enforcement and intelligence services and bring specific topics concerning cyber terrorism more regularly into parliamentary sessions and question times, thereby promoting the timely implementation of existing counter-terrorism frameworks.

The third is our aptitude to bring States closer to their citizens. In this context, we must not only strengthen the inclusion of civil society in counter-terrorism efforts, but also promote transparency of our counter-terrorism efforts to generate greater public confidence. Citizens must be reassured that States will protect their personal data.

Building on these assets and in response to a precise call from our citizens, in 2017 the OSCE PA created the Ad Hoc Committee on Countering Terrorism to bring more focus to its counter-terrorism work. We are currently striving to identify the most pressing policy-legal loopholes and forge strategic partnerships to best contribute to global counter-terrorism efforts, also by leveraging on our comparative advantages. In the long run, we aim to add value through strategic guidance and by engaging in targeted initiatives to bring a stronger parliamentary perspective in the field. For instance, we are considering ways to engage our national parliaments in the implementation of existing international frameworks on border security and information sharing.

The Committee, currently comprising 12 members from 12 participating States, has been quite active since its creation, in particular by taking part in international counter-terrorism events and field visits. Our work will continue in the coming months with the participation in more expert events - including the OSCE-wide counter terrorism conference in Rome starting this Thursday - the organization of a field visit to Bosnia and Herzegovina in June, and the drafting of a resolution to be presented at our Annual Session in Berlin in July.

Ladies and gentlemen,

If the world-wide-web brings about many risks, it also carries plenty of opportunities, and the best way to fight cyber-related threats is the appropriate use of cyberspace itself. Interestingly enough, the word cyber derives from a Greek verb meaning "to steer". Terrorists are using the opportunities offered by the internet to target vulnerable infrastructures and individuals, steering public opinion towards their flawed narratives. In response, we should redouble our efforts to protect our critical infrastructures and promote a constructive engagement of all segments of our society online. We should promote the values of integration, openness, non-discrimination, resilience and development, including through social media campaigns with ICT companies, political parties, religious leaders, local communities and schools.

In conclusion, let me reiterate that Parliaments, and international parliamentary fora such as the OSCE PA, are well placed to address the growing and evolving challenges stemming from cyber terrorism. As parliamentarians, we are ready to assume such a responsibility and shall spare no efforts in lending our contribution.

I now look forward to engaging in a productive discussion. Thank you!