PC.DEL/1320/21
1 September 2021

ENGLISH only

**United States Mission to the OSCE**

# Annual Security Review Conference

## Working Session II: Transnational Threats: Current and Future Trends in the OSCE Area and Beyond

As delivered by Chargé d'Affaires, a.i. Courtney Austrian,
September 1, 2021

In the face of an unprecedented transnational threat—the pandemic—OSCE participating States worked hand-in-hand to share resources and expertise. Through international collaboration, we are beating one of the greatest health challenges the world has ever faced. That willingness to work together must also be applied to tackling the transnational threats we address in the OSCE's First Dimension—organized crime, violent extremism and terrorism, illicit trafficking, and malicious cyber activities. A successful approach includes partners across the globe and at all levels, civil society and private businesses. The OSCE has proven its ability to gather and coordinate stakeholders to take effective and sustainable action. This is the right place to discuss ways ahead.

The United States welcomed consensus on the *Declaration on Strengthening Cooperation in Countering Transnational Organized Crime* at the Tirana OSCE Ministerial Council last year. Our focus must now be on its implementation at both national and international levels. Transnational organized crime and the corruption that facilitates it have hampered our pandemic response by siphoning public and private resources from much-needed emergency relief. To prevent transnational organized crime and associated corruption from undermining our pandemic recovery, we must meet our obligations in the United Nations *Convention against Transnational Organized Crime* and United Nations *Convention against Corruption*, for which the OSCE has long advocated and which we have helped participating States to implement. Notably, we need a multi-pronged approach. OSCE institutions and field missions help develop legislation to support fair, effective, independent, and responsive judicial systems. That is extremely important but it is not sufficient if we are to be effective against transnational organized crime and associated corruption. We also need highly trained prosecutors. We need advanced training for police and other investigators. These are the people who must gather the evidence that can bring criminals to justice. To get there we need to help participating States design effective whole-of-government approaches. Transnational criminals traffic to make a profit, whether that involves trafficking in people, natural resources and wildlife, cultural property, drugs, or weapons. This is a quintessential cross-dimensional, multi-pronged threat with pathways and perpetrators that are hard to identify, track, and investigate without effective strategies for sharing information government-wide.

The OSCE's work on cross-dimensional capacity-building in those areas provides a solid foundation for expanded efforts. Notably, the Organization's close collaboration with law enforcement agencies and civil society has helped to develop a culture of accountability.

We applaud the OSCE's workshops to strengthen civil society involvement in the social re-use of assets confiscated from organized crime.

The pandemic accelerated the digitalization of our societies and exposed our reliance on information communication technologies. Debilitating malicious cyber activities in my country, notably the SolarWinds hack last year that targeted U.S. government and non-governmental networks and the ransomware incident that disrupted the Colonial Pipeline networks, put cybersecurity at the forefront of the agenda of U.S. government leaders. The ability to maintain networks that are secure, reliable, and resilient is essential to national security.

The United States is committed to working with other countries and private sector partners to respect existing consensus, non-binding norms of responsible State behavior in cyberspace. In fact, in January we utilized the OSCE Communications Network, pursuant to the OSCE Cyber Confidence Building-Measures (CBMs) 13 and 16, to share accurate and timely information regarding the SolarWinds hack. We also advised participating States of the detection and mitigation resources being made available by the United States government. That was the first time CBM 13 was used. We hope our initiative encourages other participating States to make use of it, as we all committed to do in multiple FSC Decisions. Utilizing the OSCE's cyber CBMs can reduce mistrust and tensions and enhance interstate cooperation and stability.

For violent extremists and terrorists, both domestic and international, the pandemic was more of an opportunity than a threat. With many more people working and socializing online, terrorist recruiters stoked public fears and disseminated disinformation online to radicalize and recruit to violence. Domestic violent extremism, including racially or ethnically motivated violent extremism (REMVE), is a serious concern that requires close attention. Many of these violent extremists, particularly those who promote the superiority of the white race, have transnational connections, including online. The best weapon in our counterterrorism fight is our collective will to act and a common commitment to protect our people. We are working through our partnerships with governments, civil society, the private sector, and international organizations to counter the narratives of racially or ethnically motivated violent extremists while upholding freedom of expression.

With regard to the threat from foreign terrorist fighters, we support fellow participating States' efforts to repatriate, rehabilitate, and prosecute these fighters and associated family members. This will help prevent a resurgence of ISIS in Iraq and Syria, hold individuals accountable for their crimes, and prevent the further radicalization to violence, including of thousands of children held in the Internally Displaced Persons camps.
We welcome the OSCE's continued work on countering use of the Internet for terrorist purposes, which was addressed this year in a Security Committee meeting, a dedicated webinar, and at the annual OSCE-wide Counterterrorism Conference.

The OSCE has been a steadfast partner in our collective counterterrorism efforts and has a vital role to play. We applaud the work of the Secretariat's *Action Against Terrorism Unit* which recognizes the importance of whole-of-society and whole-of-government approaches, while respecting human rights and the rule of law.

The pandemic proved we can work across borders in addressing a shared threat. The same resolve must be applied to expanding our ability to address organized crime, illicit trafficking, violent extremism and radicalization that leads to terrorism, and malicious cyber activity. These challenges require coordinated action including a wide array of partners from all levels of society and government. However, any and all actions must be in line with our commitments to protect and advance human rights and fundamental freedoms. Efforts to counter transnational threats that do not respect human rights and fundamental freedoms ultimately foster conditions that enable these threats to proliferate.

Thank you, Mr. Chair.