PC.DEL/680/25
3 July 2025

ENGLISH only

United States Mission to the OSCE

Malign Activity in the OSCE Region

As delivered by Chargé d'Affaires Katherine Brucker
to the Permanent Council, Vienna
July 3, 2025

As we and many participating States agreed during the June 25-26 Annual Security Review Conference (ASRC), the OSCE faces new and emerging threats to our region's security from internal and external sources across all three dimensions. We thank Japan and Israel for making that point so clearly in their ASRC statements, and for highlighting the importance of OSCE partner country cooperation to help us identify appropriate responses. We also thank the Chair and the Troika for their solid commitment to revitalize and strengthen the organization to respond to new threats and to maintain the organization's relevance over the next 50 years.

A May 21, 2025, report from the MERICS and Rhodium Group found that Chinese direct investment in Europe rose in 2024 for the first time in seven years. Many of these investments are commercially motivated—but not all. Beijing's track record shows that investments are often designed to foster political leverage.

In many cases, these investments allow state-sponsored cyber actors to conduct widespread espionage. For instance, Germany has reported repeated cyber incidents against its leading firms, and in the United Kingdom, Beijing-linked hackers targeted members of Parliament. Authorities in several European countries have uncovered attempts by Beijing to use academic partnerships and fake LinkedIn profiles to recruit spies and harvest sensitive research. Finally, this May a Czech government report found that Chinese state-backed cyber actors targeted strategic Czech institutions, including the Czech Ministry of Foreign Affairs, in a sustained campaign to undermine national security—underscoring the urgent need for enhanced cyber resilience across the OSCE region.

Chinese malicious cyber activity is a persistent threat to U.S. national security. The United States is dedicated to countering the Chinese Communist Party's (CCP) malicious cyber activity against U.S. government, private sector, and critical infrastructure networks to help protect American citizens, businesses, and industries. Beijing's tactics often blur the line between commerce and coercion.

China has taken steps to position itself inside U.S. critical infrastructure. Its recent access to U.S. telecommunication systems shows both the capability and intent to target key networks in a crisis or armed conflict. The scope and scale of these incidents should be of concern to all

states given their potential impact on our collective security. The United States is committed to investing in our industrial base and ensuring a future rooted in secure technology and innovation, rather than untrusted technology from China or concerning products and services from other authoritarian states.

Beijing's tactics undermine sovereignty, disrupt markets, and threaten democratic governance. They are a systemic challenge to the values enshrined in the Helsinki Final Act.

Several participating States have felt the consequences of non-transparent and low-quality Chinese investment. In Montenegro, a near billion-dollar Belt and Road Initiative for a highway, funded by the Export-Import Bank of China that equaled nearly a quarter of Montenegro's national GDP and built by a Chinese corporation, threatened Montenegro with unsustainable debt and left vital infrastructure potentially subject to foreign seizure. In Serbia, the collapse of a railway station canopy, part of a CCP-led upgrade under the Belt and Road rail project, killed 16 people. As Secretary Rubio summed up: "China doesn't do humanitarian aid. China does predatory lending." The lesson to be learned is buyer beware. You get what you pay for. When price quotes sound too good to be true, they usually are.

China also exports surveillance infrastructure. Chinese manufactured solar inverters, widely installed in European power grids, were recently found to contain unauthorized communication modules capable of data exfiltration. These products—sold as green energy solutions—pose real risks to our digital and physical infrastructure.

The CCP's malign tactics extend to direct coercion. Illegal "police stations" operating in OSCE states, including Germany, the Netherlands, the United States, and Canada, reportedly surveilled and intimidated members of diaspora communities. These actions violate national sovereignty and fundamental freedoms.

At the June 27 Special Economic and Environmental Committee meeting, we discussed Beijing's growing use of "shadow fleets" to obscure sanctions violations and conceal vessel ownership. These opaque maritime operations—now operating near OSCE coastlines—undermine transparency and pose risks to the environment and undersea cables that are critical infrastructure and vital to global communications, national security, and prosperity.

Madam Chair, we urge participating States to take coordinated action. We should use this organization to coordinate concrete, implementable steps to protect critical infrastructure and our borders, strengthen procurement processes, promote supply chain transparency, and elevate scrutiny of CCP-linked infrastructure projects. Economic coercion is not commerce. The time to respond is now.

###