PC.DEL/616/24
17 May 2024

ENGLISH only

EUROPEAN UNION

OSCE Permanent Council 1473
Vienna, 16 May 2024

EU Statement on the Russian Federation's malign activities and interference in the OSCE region

1. The European Union and its Member States, together with international partners, strongly condemn the malicious cyber campaign conducted by the Russia-controlled Advanced Persistent Threat Actor 28 (APT28) against Germany and Czechia. On 6th May, Germany has shared publicly its assessment on APT28 compromise of various e-mail accounts of the German Social Democratic Party executive. At the same time, Czechia announced its institutions were also target of this cyber campaign. State institutions, agencies and entities in Member States, including in Poland, Lithuania, Slovakia and Sweden were targeted by the same threat actor in the past. In 2020, the EU imposed sanctions on individuals and entities responsible for the APT28 attacks targeting the German Federal Parliament in 2015.
2. The malicious cyber campaign shows Russia's continuous pattern of irresponsible behaviour in cyberspace, targeting democratic institutions, government entities and critical infrastructure providers across the European Union and beyond.
3. This type of behaviour is contrary to the OSCE commitments agreed by all participating states on cyber security, as well as UN norms of responsible state behaviour in cyberspace, such as impairing the use and operation of critical infrastructure. Disregarding international security and stability, Russia has repeatedly leveraged APT28 to conduct malicious cyber activities against the EU and its Member States, and international partners, most notably Ukraine.

4. At the same time, Russia is waging its unprovoked, unjustifiable and illegal war of aggression against Ukraine not only on the battlefield, but also in the information space. More specifically, Russia's information manipulation and interference, including disinformation campaigns, against Ukraine began long before the onset of Russia's full-scale invasion of February 2022. Since at least 2014, the Russian state-controlled media ecosystem has been propagating a series of sham pretexts and false claims, seeking to undermine Ukraine's sovereignty and territorial integrity and to prepare the ground for full-scale invasion and military aggression against Ukraine. Internationally, the main aims of this "information war" have been to falsely justify Russia's war of aggression against Ukraine, deflect responsibility for the global consequences of its war of aggression, and undermine international support for Ukraine. As documented in the EEAS Reports on Foreign Information Manipulation and Interference (FIMI) Threats, official social media accounts of Russia's diplomatic representations have been used as amplifiers of disinformation narratives. Domestically, Russia's information manipulation has been aimed primarily at sustaining public support for its war of aggression against Ukraine and stifling any opposition to it, including by an unprecedented wave of repression against Russia's own citizens.
5. Russia's conduct and rhetoric demonstrate a consistent pattern of aggressive behaviour toward its neighbours and other OSCE participating States, employing conventional, cyber and hybrid threat methods. Russia must uphold its international obligations and commitments and stop its state-controlled disinformation and other malign activities, including attempts at subversion, coercion and intimidation.
6. We reiterate our firm support for the independence, sovereignty, and territorial integrity of the Republic of Moldova and Georgia within their internationally recognised borders. We will continue to provide all relevant support to the Republic of Moldova and Georgia in addressing the challenges they face also as a consequence of Russia's war of aggression against Ukraine, and to strengthen their resilience in the face of destabilising activities by Russia.
7. The EU will not tolerate activities that aim to degrade our critical infrastructure, weaken societal cohesion and influence democratic processes, mindful of this year's elections in the EU and in more than 60 countries around the world.

8. With its comprehensive concept of security and in partnership with relevant international actors, the OSCE can contribute to enhancing resilience to cyber threats, countering disinformation campaigns, and addressing hybrid threats, ultimately promoting security and stability in the OSCE region.
9. The EU is determined to make use of the full spectrum of measures to prevent, deter and respond to Russia's malicious behaviour in cyberspace and other destabilising activities. The EU's Strategic Compass, adopted in March 2022, sets out a plan of action for strengthening the EU's security and defence policy by 2030, aiming to enhance the EU's resilience to internal and external threats, including cyberattacks, disinformation campaigns, and hybrid threats. To this end, the EU has set up dedicated toolboxes to address hybrid threats and FIMI, and developed the Cyber Diplomacy Toolbox.
10. We will continue to cooperate with our international partners to promote an open, free, stable and secure cyberspace.

The Candidate Countries NORTH MACEDONIA*, MONTENEGRO*, ALBANIA*, UKRAINE, the REPUBLIC OF MOLDOVA, BOSNIA and HERZEGOVINA*, and GEORGIA, the EFTA countries ICELAND, LIECHTENSTEIN and NORWAY, members of the European Economic Area, as well as SAN MARINO align themselves with this statement.

* North Macedonia, Montenegro, Albania, and Bosnia and Herzegovina continue to be part of the Stabilisation and Association Process.