The OSCE Secretariat bears no responsibility for the content of this document and circulates it without altering its content. The distribution by OSCE Conference Services of this document is without prejudice to OSCE decisions, as set out in documents agreed by OSCE participating States.

PC.DEL/979/24
26 July 2024

ENGLISH only

EUROPEAN UNION

OSCE Permanent Council No. 1484
Vienna, 25 July 2024

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

1. The European Union and its Member States strongly condemn the sharp increase in Russian hybrid activities across Europe and beyond, including foreign information manipulation and interference (FIMI), disinformation, malicious cyber activities, intimidation, coercion, subversion, sabotage, and the instrumentalisation of migrants. Since launching its full-scale invasion of Ukraine, Russia has intensified its hybrid campaign with new active operations on European soil.

2. The latest EEAS Report on FIMI of January 2024 exemplifies how foreign information manipulation and interference is used as a strategic policy and tool as part of Russia’s ongoing war of aggression against Ukraine with a negative impact beyond Ukraine’s borders. Ukraine remains the country that is most targeted. Domestically, Russia’s information manipulation has 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.

3. Within the European Union, Russian information manipulation has taken advantage of increased social media penetration and AI-assisted operations. Russia has developed in particular so-called “Doppelgänger” manipulation campaigns, in which websites and social media profiles were created to pretend to be authentic news outlets. In addition, pro-Kremlin platforms are not only trying to undermine the information environment inside the European Union, but also to distort the image of the EU and its policies across the Middle East, Western Balkans, Africa, Latin America, and Asia.

4. Russia's conduct and rhetoric demonstrate a consistent pattern of aggressive behaviour toward its neighbours and other OSCE participating States, including by employing hybrid methods. Russia must stop its state-controlled disinformation and other hybrid and malign activities and uphold its international obligations and commitments.

5. Hybrid threats pose a serious challenge to our collective security. The EU will not tolerate activities that aim to weaken societal cohesion and influence democratic processes. The EU and its Member States are determined to make use of the full spectrum of the EU's instruments to prevent, deter and respond to Russia's malicious behaviour and to invest further in situational awareness, societal and democratic resilience, foreign policy instruments, and regulatory tools. As part of the EU's security and defence strategy, the EU has put in place measures and dedicated toolboxes to detect, address, deter and respond to hybrid threats, FIMI, and cyberattacks. Notably, the Cyber Diplomacy Toolbox sets forth a complete spectrum of measures to counter cyber threats, including the possibility to impose sanctions for malicious activities directed against EU Member States, third countries or international organisations. Last month, six individuals were added to the EU sanctions list for malicious cyber activities against EU Member States and Ukraine.

6. With regard to malicious cyber activities, the EU will continue to strengthen its cooperation with international partners to promote an open, free, stable and secure cyberspace, and increase global cyber resilience, including through cyber dialogues and cyber capacity-building projects with third countries. We have significantly stepped up our cyber support to Ukraine since the beginning of Russia's war of aggression and remain firmly committed to strengthening Ukraine's resilience capabilities against cyberattacks and disruptions of critical infrastructure. Moreover, in the framework of last week's third EU-Ukraine Cyber Dialogue, the two sides agreed to enhance exchanges on situational awareness and cyber risks and strengthen their partnership in international fora in support of the UN framework of responsible state behaviour in cyberspace. The EU will also

continue political and capacity-building support to its Western Balkan partners. Activities of the EU-funded comprehensive regional cybersecurity programme in 2024 are focusing on four components: 1. Cyber governance and awareness, 2. Legal framework, cyber norms and diplomacy, 3. Risk management, and 4. CERT capacities.

7. In addition, exposing the tactics, techniques and procedures of malign foreign actors to our citizens is one of the best instruments to counter all sorts of disinformation. Through utilising the EUvsDisinfo platform, which has the world’s largest publicly available database of pro-Kremlin disinformation cases, we seek to limit the impact of Russian attacks on our societies. We also work closely with academia, civil society, the tech industry, and international partners to better understand and counter FIMI.

8. The EU also actively supports the development of international principles and norms to address FIMI, including disinformation, by promoting responsible state behaviour in the online environment and the commitment to refrain from using the Internet or online platforms to undermine human rights, universal values, democratic processes, and institutions. The EU is determined to engage with all partners to advance this goal, including within the OSCE.

The Candidate Countries NORTH MACEDONIA*, MONTENEGRO*, ALBANIA*, UKRAINE, the REPUBLIC OF MOLDOVA and BOSNIA and HERZEGOVINA*, the EFTA countries ICELAND, LIECHTENSTEIN and NORWAY, members of the European Economic Area, as well as ANDORRA and 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.