Russia's war on Ukraine: The digital dimension

While Russia deploys cyber warfare and disinformation strategies in its war on Ukraine, social platforms, and telecommunication, media and internet operators are playing an important role in relaying information on the war and shaping public opinion. The EU has taken a number of immediate, practical, measures to support Ukraine, and is contemplating further action to build the resilience of its communications infrastructures, strengthen cybersecurity and counter disinformation.

State of play

Russia's military aggression has largely destroyed and destabilised Ukraine's communications infrastructure. This has been accompanied by hybrid threats, including massive disinformation campaigns and cybersecurity attacks. The work done by the EU's East StratCom Task Force, set up to address Russia's disinformation campaigns, shows that, since 2014, over 13 500 cases of disinformation (nearly 40 % of all cases identified) have targeted Ukraine. In recent weeks, the pro-Kremlin disinformation narrative on the situation in Ukraine has been gaining momentum; it includes a misrepresentation of the role of the North Atlantic Treaty Organization (NATO), and claims that the West is imposing censorship through state institutions and privately-owned social-media companies. Furthermore, Ukraine has suffered a string of cyber attacks in recent weeks, and concerns are also rising with regard to cyber strikes targeting the EU. The European Central Bank has gone so far as to warn European financial institutions of the risk of retaliatory Russian cyber attacks. Faced with these exceptional circumstances, the EU has acted to support Ukraine, and is exploring the need to adopt additional measures to foster the resilience of the communications infrastructure, strengthen cybersecurity and counter disinformation.

The **global submarine cable network** is the internet's 'backbone'. Over 95 % of international telecommunications are provided through undersea cables, transmitting vast amounts of data across oceans. The vulnerabilities of this infrastructure are long documented. Some experts warn that, in the context of Russia's war on Ukraine, hostile action could be taken to damage or destroy physical internet infrastructure (such as undersea cables) that could disrupt global internet traffic and the flow of government and citizen communications, with serious economic consequences.

EU response

- **Boosting communications infrastructure resilience**. Keeping Ukraine's telecommunications services operational is critical to ensure normal functioning of the Ukrainian government, as well as to relieve the humanitarian crisis. Some European telecom companies have taken voluntary measures, such as offering free international calls to Ukraine, distributing SIM cards to refugees, and providing free Wi-Fi at refugee camps. In addition, the French Presidency of the Council of the EU will coordinate the efforts of private-sector companies in the Member States to provide Ukraine with IT equipment. The EU may also intensify its efforts to back the Ukrainian authorities by means of the €25 million EU project to support Ukraine's digital transformation agreed in 2020, and the investment schemes under the Global Gateway strategy to finance digital infrastructure.
- **Banning Russian propaganda on its war on Ukraine**. Combating war propaganda and disinformation is a particularly pressing issue in Russia's war. The Council decided on 2 March 2022 to suspend the broadcasting activities of Sputnik and Russia Today taking place in or directed at the EU until the aggression towards Ukraine ends and Russia and its associated outlets cease to conduct disinformation and information manipulation actions against the EU and its Member States. This extraordinary measure, which was immediately and directly applicable in all EU Member States, restricts the access of the main Russian state-controlled media outlets to the European media market. Furthermore, following the Commission's call,

Author: Tambiama Madiega, Members' Research Service
PE 729.317 – March 2022

European media regulators have agreed to strengthen their cooperation in establishing a taskforce that will focus on foreign disinformation in the context of the situation in Ukraine.

- **Strengthening the EU anti-disinformation toolbox**. The Ukraine crisis is fostering a debate on how to fend off foreign interference and disinformation more effectively. There are already proposals to increase East StratCom Task Force funding and extend the EU's rapid alert system on disinformation to cover Ukraine and other interested parties. Moreover, on 8 March 2022, EU ministers called on tech firms (online platforms, internet service providers and social media companies) to take additional voluntary measures to combat online disinformation and information manipulation. The Ukrainian situation is also likely to steer EU lawmakers towards strengthening the EU's online media framework in the pending digital services act and other initiatives under the democracy action plan, and in the European media freedom act due to be adopted in the third quarter of 2022.
- **Supporting Ukraine's fight against cyber threats**. In the wake of Russia's invasion of Ukraine, and following on from the EU/Ukraine cyber dialogue launched in June 2021, the EU Foreign Affairs Council announced on 21 February 2022 that the EU would do more to help Ukraine defend itself against cyber attacks. A Cyber Rapid Response Team composed of EU experts has been deployed to that end.
- **Bolstering EU cybersecurity capacities**. The situation in Ukraine has also prompted the EU to reflect on how to complement its current framework to counter hybrid threats, and accelerate the pace of European cooperation to address cybersecurity challenges more effectively. On 24 January 2022, the Council of the EU called on the Commission to strengthen the EU's resilience and ability to fight back against cyber attacks. Further initiatives to ensure resilience of electronic communications infrastructure and networks in Europe have been announced, including more cooperation at operational level, a future cyber resilience act, and the establishment of a cybersecurity emergency response fund.
- **Limiting Russia's access to dual-use technologies**. The EU sanctions adopted on 25 February 2022 intend, not least, to limit Russia's access to crucial advanced technology. Dual-use technologies – namely those that can be used for both peaceful and military objectives – such as semiconductors or cutting-edge technologies, radio communication technology and crypto-assets, must not be sold or otherwise supplied for use in Russia or to a Russian entity.

European Parliament position

The Parliament has long supported EU initiatives to regulate digital platforms and reinforce EU capacities to tackle disinformation and cyber threats. At its extraordinary session on 1 March 2022, it adopted a resolution, condemning the use of information warfare by Russian authorities, state media and proxies 'to create division with denigrating content and false narratives' about the EU. The resolution called on the Commission and the European External Action Service to enhance alternative online Russian-language information on the unfolding developments to counter disinformation. It welcomed the ban on Russia Today and Sputnik in the EU, and reiterated the calls on Google and YouTube to remove war propaganda accounts. Furthermore, it called for the EU and the Member States to terminate the software licences for military and civilian equipment in Russia and Belarus, more specifically those used for communication and satellite navigation. Finally, the resolution called for full use of the EU cyber sanctions regime against individuals, entities and bodies responsible or involved in the various cyber attacks targeting Ukraine, and for action to support Ukraine and Eastern partner countries in improving their resilience against possible Russian attacks. On 9 March 2022, the Parliament's plenary adopted the final report of its Special Committee on Foreign Interference in all Democratic Processes in the EU, including Disinformation (INGE), urging the Commission to propose a more coordinated European strategy to counter operations by foreign governments using disinformation. The report recommends the setting up of a European centre to tackle interference threats, and stronger measures to address disinformation on online platforms. It also calls for new counter- and deterrence measures to ensure cybersecurity and resilience against cyber attacks, and to protect critical infrastructure and strategic sectors.