Joint letter by DIGITALEUROPE and its member associations on the war in Ukraine

How to protect Europe and its allies from cyber threats and give threatened states safe connectivity

Dear Ministers,

The continent of Europe is experiencing the biggest conventional war since World War II. However, the reality of the 21st century shows that we cannot underestimate the importance of cyber warfare. Research shows that cyberattacks on Ukraine have ramped up in recent weeks and months, weakening its critical infrastructure and the functioning of its society. Furthermore, connectivity is fundamental for Ukraine and its citizens.

Our members in the region are already providing support, both humanitarian and ICT-related. Many companies are donating time, money and expertise to support Ukrainian citizens and organisations, and to protect them from cyber-attacks. We fully support measures that the EU and its allies are taking in order to stop Russia's aggression, **and call on ministers to step up its immediate cybersecurity support.**

The EU must also use this as a wake-up call. Now is the time to commit the necessary resources, and to build up Europe's digital shield to protect our citizens and our allies like Ukraine. Cyber knows no borders and talent is scarce – let us bolster our cyber security together.

During the Informal Telecommunications Ministerial on 8-9 March, we urge you to take the following points into account:

1. **Ministers should commit to joint EU action on cybersecurity**. For example, in the NIS2 Directive, currently in trilogues, the EU should have a common approach to listing critical entities and there should be a single point to help companies notify and respond to cyber incidents. We need a united and transparent legislative framework, and to avoid fragmentation into 27 nations.
2. **EU and NATO collaboration on cybersecurity and emerging technologies is essential for our collective security.**

3. **Ministers should ask the Commission to develop a new Digital Decade target on cybersecurity.** For example, the EU should propose a package to help to immediately train 200,000 cyber security experts (the number of experts Europe lacks today) and develop a long-term plan to train 1,500,000 cybersecurity specialists by 2030 to fill future demand.
4. **Member States should reassess their recovery and resilience plans and invest more in cybersecurity.** We are concerned by the lack of funding allocated to cybersecurity in the current plans.
5. **Ministers should accelerate the set-up of the Cybersecurity Competence Centre in Bucharest and give it significantly more resources** in order to do its work.
6. **Ministers should renew their focus on cybersecurity training and digital education in the public education system**. Cybersecurity training should be on all school curricula.
7. **Ministers should make sure that all legislation under discussion is helping and not hindering cybersecurity efforts.** For example, machine learning and device data are essential to identifying new cyberthreats. We must make sure the new AI Act and ongoing ePrivacy talks bolster our cyber defences and do not weaken them.
8. **Ministers should consider how to facilitate communications to and from those in Ukraine and the victims fleeing the country**. **Strong and safe connectivity for our European friends is of crucial strategic importance.** Many operators have already waived roaming charges and offered free calls and texts between Ukraine and the EU on their own initiative.
9. **Setting international cybersecurity standards should be a priority, first and foremost in the EU-US Trade and Technology Council.** This is an area where we can and should move quickly.

Only by being united can we prepare ourselves for the new realities. We also need to get our own house in order to be able to adequately provide support to our allies and friends like Ukraine, which has deep ties with the European ICT community and has served as major hub for ICT and cybersecurity in the region.

Signed:

- **DIGITALEUROPE**
- **AAVIT** (Czech Republic)
- **Abelia** (Norway)
- **AFNUM** (France)
- **AGEFE** (Portugal)
- **Agoria** (Belgium)
- **Ametic** (Spain)
- **ANIS** (Romania)
- **Anitec-Assinform** (Italy)
- **APSI** (Luxembourg)

- **ATIC** (Moldova)
- **bitkom** (Germany)
- **CITEA** (Cyprus)
- **Dansk Erhverv** (Denmark)
- **DI Digital** (Denmark)
- **Digital Turkey Platform** (Turkey)
- **ECID** (Turkey)
- **Fiar** (Netherlands)
- **GZS** (Slovenia)
- **HGK** (Croatia)
- **INFOBALT** (Lithuania)
- **ITAS** (Slovakia)
- **ITL** (Estonia)
- **IVSZ** (Hungary)
- **KIGEIT** (Poland)
- **NLdigital** (Netherlands)
- **Numeum** (France)
- **PIIT** (Poland)
- **SEPE** (Greece)
- **Technology Ireland** (Ireland)
- **TechSverige** (Sweden)
- **techUK** (United Kingdom)
- **Teknikföretagen** (Sweden)
- **TIF** (Finland)
- **ZIPSEE** (Poland)
- **ZVEI** (Germany)