DIGITALEUROPE

BRUSSELS, 25 JANUARY 2023

EVENT REPORT

DIGITALEUROPE RESILIENCE COUNCIL: Public, Civil and Private Cooperation for an ambitious EU Cyber Defence

Introduction

The Ukraine conflict has brought to light that warfare has reached a new level in the digital age. Transport, energy, to healthcare have fallen to attacks from foreign state actors using ransomware and other malware to paralyse critical infrastructure.

To address this, DIGITALEUROPE's Resilience Executive Council convened a high-level roundtable with leaders from public and private institutions in Cyber Defence Policy to find solutions for improved governance, threat assessment and mitigation and acceleration of EU's ability to counter threats through procurement, standards, and skills.

Three conclusions emerged prominently throughout the event:

- **Private sector is critical for the success of key EU initiatives:** For example, the newly launched Security Operations Centres (SOCs) to address fragmentation amongst Member States can benefit from cyber expertise in the private sector, SME ecosystems and resources to enhance operational cooperation.

- **Earmarking funds for cyber, a simpler procurement process.** Common standards amongst allies could contribute to making sure Europe is ready for emerging digital threats by ensuring Europe has the best technology, infrastructure and skills. Formal information sharing is crucial to protect Europe's critical infrastructure. With various ongoing initiatives existing at the EU level, the private and public sectors need to increase operational agility.

DIGITALEUROPE
Rue de la Science, 14A, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

- **Cooperating globally**: we need to use all fora to collaborate globally. Our aim should be to avoid duplication. EU-NATO collaboration is essential. Joint exercises between the EU – NATO – private sector could be a step forward.

Participants agreed on a set of KPIs to be reviewed and discussed in the group again in six months' time to engage actively and drive the success of the following activities:

1. A formal information-sharing forum between EU, Member States, and private sector.
2. A map of key cyber governance initiatives relevant to Europe.
3. 20 Member States on board for a more formal structure.
4. An EU list of trusted cyber vendors/reserves.
5. 200 cyber-SMEs with pan-European procurement contracts.
6. Regional cyber campuses built across the EU and 20 public-private cyber trainings taking place within the next 12 months.
7. EDT standardisation work consolidated between like-minded partners.

The event was joined by the following:

Chair

- **Cecilia BONEFELD-DAHL**, Director General, DIGITALEUROPE

Officials

- **Lorena BOIX ALONSO**, Director for Digital Society, Trust and Cybersecurity, DG CNECT, European Commission
- **Dan CÎMPEAN**, General Director, Romanian National Cyber Security Directorate
- **Richard KADLČÁK**, Special Envoy for Cyber Space, MFA Czech Republic
- **Marina KALJURAND**, Member, European Parliament
- **Mart NOORMA**, Director, CCDCOE

- **Wiktor STANIECKI**, Deputy Head of Security and Defence Policy Division, European External Action Service

Industry

- **Izabela ALBRYCHT**, Director of the Cybersecurity Center at AGH University of Science and Technology
- **Hazel DIEZ**, CISO Global Services and Global Head of Governance, Risk and Compliance, Group Santander
- **Vincent DEFRENNE,** Director, Cyber Strategy & Architecture, Nviso
- **Gavin HENDERSON,** Vice-President and CSO for Mastercard International Markets, Mastercard
- **Andrew LEE,** Vice-President of Government Affairs, ESET
- **Nanna-Louise LINDE**, Vice President, EU Government Affairs, Microsoft
- **Mikael RYLANDER**, Vice President, Technology Leadership, Nokia
- **Eva TELECKA**, Executive Director, Regional CISO, MSD

More insights into the main conclusions of discussions are below.

The Joint Communication on an EU Cyber Defence Policy,[1] published on 10 November 2022, is aimed at enhancing Europe's cyber defence capabilities. To achieve this goal, the collaboration between the private and public sectors is key. We need to work together to create a resilient infrastructure, have an incentive-based system, and cooperate globally.

1. **Private sector is critical for the success of key EU initiatives. We need to ensure agile and more operational cooperation between public and private sectors: formal information sharing is crucial when it comes to critical infrastructure.**

European institutions agree that cooperation with the private sector is important. As a matter of fact, the lesson learned in Ukraine is that we need more operational cooperation between the two sectors. For example, in case of an incident, institutions will rely on the private sector to provide assistance.

[1] European Commission (2022), *Joint Communication to the European Parliament and the Council: EU Policy on Cyber Defence*, <https://www.eeas.europa.eu/sites/default/files/documents/Comm_cyber%20defence.pdf>.

However, institutions envisage the role of the private sector rather outside of the legislative processes i.e., information exchange, operational cooperation, and skills.

- **Various ongoing initiatives at the EU level**

Currently, there are several ongoing initiatives which involve the private sector. Mirroring the EU-US cyber dialogue discussions, ENISA and the European Cyber Security Organisation (ECSO) are working on developing similar communities. At the same time, there is also an initiative to create a cross-border network of Security Operations Centres (SOCs). Member States participate in these SOCs, but information-sharing remains voluntary. On its side, the EU Cyber Solidarity initiative also aims to include some aspects pertaining to SOCs to ensure that the SOC infrastructure is permanent. However, the question of how to cooperate to make an EU cyber reserve permanent remains.

Both institutions and the public sector agreed that it is important to have a reserve that has the capacity to respond even on occasions when the private sector cannot. The European Commission is still assessing whether a certification scheme for trusted providers at the EU level is necessary. The private sector pointed up that working together fast and as a team is much needed, more so as while the industry can wait for the public sector to lead, cybercriminals are not.

- **Need for increased operational agility**

Panellists agreed that we need increased operational agility, calling for combined public-private cyber exercises, a common penalty system to fight cybercrime, a two-way information sharing and a concrete plan on how this information is used. Sharing threat intelligence is crucial to combat cybercrime. Therefore, the private sector needs to assess the threat actors and cooperate with the public sector in pursuing them, potentially creating a common penalty system. Also, information sharing should not be private sector sharing information. We need a concrete plan about what happens and how to best use that information. Trust and transparency are needed in building the sharing of information. Equally important, the private sector runs a lot of cybersecurity exercises, however, they need to combine them with the ones happening in the public sector.

2. **Earmarking funds for cyber, a simpler procurement process. Incentives such as clear roles and responsibilities together with less fragmentation would enhance collaboration. SMEs need access and long-term financing.**

- **Private sector as a long-term partner**

European institutions understand that there is a business angle. Therefore, it is important to create a system of incentives to ensure that the private sector can react quickly. A way to incentivise the industry is to give it a place at the table and work with it as a long-term partner. Understanding the convergence of civilian and military, especially on skills and operational capacity and defining clear roles can lead to a more efficient collaboration between public bodies, but also public bodies and private entities. For this, we would need a clear legal framework at the national level that clarifies how relevant agencies and bodies work together, which would also ensure less fragmentation.

- **Access and long-term financing for SMEs**

We also need to ensure an incentivising approach for SMEs. For example, NATO has been discussing how to give access to SMEs. Open architecture and interoperability are ways to include them, instead of focusing on one industry partner only. Long-term financing is also key for SMEs. We already have assets in Europe as well as a communications system which we need to further build on. When it comes to certification, it is necessary to think bigger than Europe and avoid building expensive testing for certification that smaller players cannot afford.

3. Cooperating globally: we need to use all fora to collaborate globally. Our aim should be to avoid duplication. EU-NATO collaboration is essential.

Global cooperation even in the least expected fora is key. These include e.g., the UN, with its Economic and Social Council (ECOSOC). At the same time, we need to be aware as there are many initiatives globally about multilateral issues such as cybersecurity. The International Telecommunication Union (ITU) is a typical example, as no one paid attention until China came with their initiatives. It is equally necessary to involve NGOs in these processes.

At the same time, we need to ensure that we avoid duplications given the limited resources. A few examples of public-private cooperation already exist at NATO and UN levels. The private sector strongly agrees that the discussion on cyber defence need not happen in isolation in Europe, but it needs to be done with NATO.

And whereas European institutions are perceived more and more as security providers in the EU, there are growing expectations externally. However, there are not many reaction teams at this stage e.g., in the European External Action Service that could provide security to like-minded smaller partners.

DIGITALEUROPE's recommendations are as follows:

Governance

1. **Create a Joint Public-Private Advisory Council on Cyber Resilience ("the Advisory Council").** It supports and facilitates strategic cooperation and preparedness for a high level of security of network and information systems in the EU. The Advisory Council could be set up by the European Defence Agency. We need to streamline the number of organisations and clarify roles and responsibilities when implementing the EU Cyber Defence Policy.
2. **The Advisory Council plays a crucial role in defining the EU Cyber Solidarity initiative and cyber reserve.** It suggests criteria for cybersecurity certification schemes for trusted private providers and develops them. It supports the framework to set up the EU-level cyber reserve of private vendors and civil specialists.

Procurement

3. **European Defence Investment Programme (EDIP) to include relevant provisions for the joint procurement of digital and cybersecurity technologies**. Upcoming regulation prioritises digital and cybersecurity as core components of our efforts to increase the security of EU citizens. It should be a pan-European while earmarking dedicated funds for SMEs.
4. **NATO's DIANA model to be duplicated at the EU level to drive SME innovation**. A similar bureaucratically agile and streamlined model replicated at the EU level could spur more SME innovation.

Standards

5. **The Advisory Council can work with the High-Level Forum on European Standardisation to promote and develop hybrid civil/defence standards.** It can contribute industry expertise to establish a strong common ground in standardisation (e.g., on Common-and-control, Emergency Management, Cyber Threat Intelligence, data & information risk levels).
6. **The Advisory Council will strive for greater cooperation between NATO and the EU on setting standards for key dual-use data sets and technologies**. DIGITALEUROPE is participating in NATO conferences and play a central role in the EU Commission's High-Level Group for Standardisation, namely in the groups dedicated to digital and resilience.

Skills

7. **The Advisory Council is an integral part of the initiative on a Cyber Skills Academy.** The Advisory Council can contribute to outlining the framework for the

Cyber Skills Academy. We encourage both the EU and NATO to pool resources, investments, and capabilities in developing this initiative.

8. DIGITALEUROPE is already coordinating similar programmes e.g., **Women4IT**. In addition, we are currently working together with relevant institutional stakeholders to set up a **network of cybersecurity skills campuses** across Member States to facilitate and support local training initiatives. This network of campuses would allow cybersecurity solution vendors and other enterprises to step up their trainings in the interest of Europe's security. With a shortage of almost 300,000 cybersecurity specialists in Europe, we need a more operational public-private cooperation. Therefore, we also need to use the platform provided by SOCs as well as the upcoming cyber reserve to promote relevant skilling programmes at national and multi-national level. We need to streamline all initiatives to ensure the necessary level of skills and competences in Europe.

***