DIGITALEUROPE

BRUSSELS, 7 NOVEMBER 2022

Critical digital technologies for European digital resilience

Introduction

On 6 October, a high-level roundtable on developing critical digital technologies for European digital resilience brought together key stakeholders from the **EU institutions, Member States, NATO allies as well as the digital industry**. The discussion looked at the collaboration on new technologies between the public and private sectors, at how to empower SMEs and how to advance the cooperation between civil and military.

A first observation is that there **is a lack of structured dialogue between the private and the public sectors – both NATO and the EU**. Since the war in Ukraine, we have seen a paradigm shift as countries reconsider their approach to defence. The invasion has focused minds and budgets, but the Ukrainians themselves have also showcased a new model for public-private cooperation which we can learn from.

Events in Ukraine and elsewhere in the world also show a widening split between democratic and authoritarian societies. Cooperation between NATO and the EU becomes more and more important. At the same time, **democratic countries must work harder to retain their technological edge** and stay ahead of the competition.

Another trend to note is that **most of the innovation now comes from the private sector and is picked up by the military**. Historically, it has been the other way round.

Europe has been depleted of scale-up tech companies. We need to find solutions to help European SMEs making dual use goods grow. Overall, we need to incentivise a healthy competition.

To attract non-traditional players and support smaller companies, there is also general agreement that **we also need to become more agile in terms of procurement and investments, including more pan-European investments** across all regions. The defence industry as a whole is going through a digital transformation, requiring a highly skilled workforce. The future of warfare is collaborative, which makes interoperability a vital element.

1. NATO - EU collaboration

Collaboration between NATO and the European Union is vital, the more so **as 23 NATO allies are also members of the European Union**. Although there is a good dialogue between the two at the moment, it can still improve. In addition, there is also a need for the legislative tools on both sides to be aligned to deliver on common aims.

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

However, **NATO - EU collaboration alone is not sufficient. There is also a need for collaboration within each Member State, between the EU ministries and Defence ministries**. This collaboration needs to be pushed by political awareness and willingness to shape a new structured formal governance.

Defence is becoming more and more a priority for the European Commission. **While the EU has a limited mandate in this area, there is an increased understanding of the need to build concrete common defence capabilities**. With President Ursula von Der Leyen, a former Defence Minister, at the helm, this has accelerated. For the first time, the EU has recently proposed a €500 million framework for common defence procurement for Member States. In addition, the latest budget puts €8 billion towards the European Defence Fund, under which there is a specific research area for disruptive technologies.

The **EU Treaties have proven to be a constraint** to these ambitions. The current legal structure does not allow for budget and action on civilian and defence. One approach would be to work around the treaty and foster more research and more initiatives on defence and innovation for dual use.

The EU is well-placed to play a role in this field due to its experience in funding and the well-established private sector defence industries. Yet if we want to create a common market for defence, there are still major hurdles. For example, many Members States still prefer to buy from their own national companies**. Without the scale of the European market, companies will never be able the maintain their innovative edge and make the investments needed.** This poses a fundamental risk to the resilience of our continent.

There has also been a shift on the side of NATO, as **total defence[1] moves towards general defence planning and societal robustness**, albeit allies have different views on this approach given the conflict between open and more authoritarian societies, which can also be observed in Europe.

Although it is difficult to imagine now shared responsibilities between the EU and NATO, having common standards e.g., on cybersecurity, could help avoid difficulties in procurement and bureaucracy. **NATO has a big role to play as a standard-adopter**, not necessarily as another developer of standards. Nevertheless, the EU holds the policy toolbox, something NATO lacks, therefore further coordination between the EU and NATO is highly needed.

On cybersecurity, Member States have traditionally distrusted formal collaboration with NATO and the EU, arguing it must remain a national competence. Nevertheless, NATO and the EU have been collaborating on cybersecurity since 2010. The collaboration has been improving over the years. However, on an operational level both parties still struggle to achieve smooth information sharing. But as we are in time of war, NATO leadership must ensure operational excellence to further advance this collaboration.

With the war in Ukraine, we saw a paradigm shift. We should capitalise on this opportunity. An important step forward would be the more systematic sharing of threat intelligence with the private sector as it is currently the case with the military side.

2. Investments

[1] Total defence represents all activities preparing the society for war.

Europe cannot afford to fall behind when it comes to investment in defence and security. European funds for defence and security are available through various tools.

We can invest in civil innovations through Horizon Europe. The EU can push for innovation from non-traditional players, while at the same time learning from them.

We can invest in infrastructure and capabilities as well as cutting-edge technologies through the European Defence Fund (EDF) (€8 billion). For example, the EDF dedicates a significant amount to innovation, with 60 projects focused on cybersecurity, AI, cloud or 5G. There are also other ways to boost innovation through programmes such as the EU defence innovation scheme or the innovation hub in the EU Defence Agency. This fund works as an incentive for Member States to work together because we need to avoid fragmentation. Also, smaller Member States need purchasing power. **The European Commission aims to instil a culture of cooperation. We are not the only ones procuring various defence products, and common purchasing power would be an advantage in the market.**

The **European Commission plans to invest more tangibly in the defence and security sector to boost innovation**, particularly in start-ups. We need to deliver capabilities. A way would be to blend the EDF with the European Investment Fund (EIF) to invest in equity in start-ups and SMEs.

However, innovation is easier than procurement and speed is of essence. **Today, it takes ten years between prototypes and phases of approval, which is too long in cyber or AI**. We need to find a way to move faster and become more agile in terms of investments and procurement. Hackathons or challenges are a way to do so. For example, a challenge on sensors for drones was organised in France, with solutions and products being found in only a few months. Member States or Allies need, however, to take the lead.

We also need a framework at European level to ensure that non-European allied countries are allowed to participate in procurement in parts of the supply chains. Otherwise, the risk is that a domestic approach will prevail instead of a collaborative one.

Unfortunately, **the budget in the European Union is still small** compared to the US. Dual use technologies, new actors coming on the scene, non-defence specialists and SMEs have real potential.

3. Interoperability and standards

Interoperability should be an absolute priority. The future of warfare is collaborative, with data playing a massive role. We will have a connected battlefield in the next ten years. The aim is to reach a level of hyperconnectivity never seen before. It is paramount that we can operate together – public and private in an interoperable manner (e.g., data exchange, communication systems). The EU and NATO could collaborate in the future on a shared data space.

Our governments need to look closely at industry-based standards and become an adopter of standards, notably of private sector standards in terms of innovation and defence. With key technologies becoming off the shelf and accessible, interconnection and cooperation between countries and with industry is key.

4. SMEs

SMEs are confronted with difficulties throughout procurement calls. The first is that they simply don't have the time to look for all the different calls. They are also faced with many bureaucratic obstacles as **authorities keep setting up different funding mechanisms** requiring them to start from scratch each time. A simplified and streamlined funding application system would help them.

European funding unfortunately does not make a big difference for SMEs because **the EU prefers big consortia of companies and academia, which are very challenging for smaller companies to bring together**. For example, the EDF is complex and difficult to participate in for SMEs. In addition, it is rather difficult for SMEs to find resources for research and development. **A solution would be to build an agile SME regulation test and centres of excellence to enable SME innovation**.

Several Member States have found an efficient way to distribute Recovery and Resilience Facility funding to SMEs – for example, Spain through its Digital Toolkit package. The **European Commission and the European Council should have a close dialogue on how to earmark funding for SMEs and the most efficient ways to drive SME funding on EU and pan/European level**.

Furthermore, the **EU should learn from NATO and the new SME accelerator programme DIANA**, that supports SME innovation and cross border contracting amongst NATO allies.

5. Skills

Skills are of paramount importance to improve the resilience of our societies. **Companies large and small report difficulties in finding people with the right skill set.** Europe lacks between 350,000 and one million cyber specialists.[2] This is a major risk for our democracies in the digital era. The lack of focus on critical security skills in western democracies stands in sharp contrast to countries like China and India who have had a focus on STEM and tech skills for the past 20 years. **2023 is the European Year of Skills** and the public and private sectors have the chance to use this momentum to collaborate further.

However, the angle to look at skills is not only though the need for cyber experts, but a broader one – for example, cloud skills. **A variety of skills can be used in defence, not only those traditionally associated with defence domains per se e.g., quantum. All citizens need to have digital skills, not only as users** but also as creators, and be able to prevent and address vulnerabilities. Digital education should be more coordinated at the EU level to include subject matters e.g., coding in the curricula of all Member States. Europe should not only seek to develop digital skills, but also attract talent and companies from outside. EU immigration rules should be amended accordingly.

Finally, institutions should learn from and work together with the industry. **There is no time for the artificial boundaries between private and public sectors – let us act as one team for the benefit of European citizens and like-minded nations.**

[2] DIGITALEUROPE (2019), *A Stronger Digital Europe – our call to action towards 2025*, <https://www.digitaleurope.org/policies/strongerdigitaleurope/>.