European Commission

SPEECH | 24 September 2019

Commissioner King’s remarks at the 2019 Digital Resilience Summit of the Lisbon Council

Good morning.

I am very happy to be here today at the Lisbon Council’s ‘Digital Resilience Summit’. This is something the Commission has, and the Member States, worked particularly hard to improve over the past two years.

As many of you probably know, the President elect Ursula von der Leyen has announced that she intends to make the next Commission a geopolitical one and that she wants to see Europe retain a greater technological sovereignty.

You’ve chosen a challenging title for this plenary today. It is very timely. I shall try to offer some context from a security perspective.

A geotech world

Technology has become geopolitics.

Digital technologies have radically transformed the world’s economic landscape. In 2001, only one of the top five largest companies in the world by market capitalisation was a digital company. Today, the top five are all from the digital sector, and none is European.

Similarly, there is no EU company in the world’s top digital 15. As a result, the contribution of European businesses to the global digital supply chain has gradually diminished, despite the fact that the region remains one of the world’s largest markets for digital products and services.

Meanwhile, we are entering a new era of great power competition where Europe must defend its interests and the multilateral institutions that underpin them.

The reality is that European countries are increasingly vulnerable to external pressure that prevents them from exercising their sovereignty – especially in the technological domain.

So to prosper and maintain our independence in a world of geopolitical competition, we need to address the interlinked security and economic challenges that other actors present to us – without withdrawing our support for a rules-based order.

Most fundamentally, the EU needs to learn to think like a geopolitical power – and understand what that means in the digital era, if we want to secure and bolster our democracies for the future.

Because we are on the threshold of a geotech world.

Recent Chinese acquisitions in the EU are twice as large as EU acquisitions in China. This offers growth promoting FDI in the EU. But it also raises a question mark about the control over strategic technologies. In some sectors, EU firms cannot easily carry out traditional mergers and acquisitions in China. Instead, they have to engage in joint ventures with Chinese firms, transferring technology and intellectual property.

In addition, foreign companies face challenging conditions for doing business in China. For instance, China imposes limitations to market access and the intellectual property right protection can leave something to be desired.

At the same time, the US benefits more from the rise of Chinese science than the EU. In 2017 the US hosted almost double the number of overseas Chinese researchers, and it issued more than three times as many international co-publications with China, compared with the EU.

This puts the EU, its companies and citizens at a disadvantage not just vis-à-vis China but also globally – as we work to grow our companies, sell our products at home and abroad, and invest in our security.

5G security

To be fair, the EU has recognised this challenge.

That is why in March already we committed ourselves to fostering industrial cross border cooperation with strong European players, around strategic value chains, both in the context of the EU-China Strategy as well as the Recommendation on Cybersecurity of 5G Networks.

To remain resilient in a changing global geopolitical climate, we need to act together to identify and mitigate potential weaknesses and vulnerabilities which might undermine our collective security.

That was the thinking behind our Recommendation of March, which set out a European approach to protecting the security of our 5G networks and the massive amounts of critical European data that will travel across them. And whereas in earlier generations - 2 & 3G - cost was a key criterion, with 5G security must be at the heart of the decision making.

With 5G, we are talking about critical European infrastructure. The Recommendation sets out a three-stage process to get all Member States to identify the risks, to formulate mitigation strategies and to share these, to arrive at an EU-wide risk assessment and toolbox of responses.

Member States have conducted their national risk assessments in the first stage, and we are very close to finishing our analysis and will soon present an EU-wide risk assessment prioritising the most sensitive and vulnerable aspects of 5G networks.

To support this work, we have a number of processes in place.

First, the Cybersecurity Act, which was approved by the European Parliament and Council in December, reinforces the mandate of the EU Cybersecurity Agency to better support Member States in tackling cybersecurity threats and attacks. The Act also establishes an EU framework for cybersecurity certification, boosting the cybersecurity of online services and consumer devices. I think we can expect 5G infrastructure to be an important part of the Agency’s work.

Second, under the Directive on Security of Network and Information Systems, the NIS Directive, all Member States have to adopt a national strategy in this area, defining the objectives and appropriate policy and regulatory measures. This includes designating at least one competent authority to monitor the application of the NIS Directive at national level and to nominate a single point of contact to liaise and ensure cross–border cooperation with other Member States.

Third, the Foreign Direct Investment Screening Regulation, once in force, will allow the Commission and Member States to cooperate in their assessment of security risks and raise specific concerns posed by foreign investments, including in digital infrastructure.

Fourth, we provided a set of guidelines in July on the EU’s rules on public procurement including how Member States and public authorities can prioritise measures such as security, data protection, environment, and labour standards.

Fifth, the Body of European Regulators for Electronic Communications (BEREC) is moving forward with an ad-hoc working group, which will ensure involvement of national telecommunications regulators, and BEREC will soon provide the Commission with their assessment on 5G networks and security measures taken across Member States.

All of which will feed into the work we are doing to develop a toolbox of mitigating measures to be finished by the end of the year.

I expect that, by the end of the year, we shall be able to set out clearly both the steps we are taking and recommending Member States take, with clear arguments and justifications, to better secure our 5G networks across Europe.

This will be an important step, but not by any means the end of the story.

5G is a start

Because as we face a geotech world, the work we are doing on 5G is only a first step.

There are a wide range of other technologies and issues that we need to address, to define which of them we consider critical for our future welfare and security, and to position Europe to take action.

In particular, in my view, we need urgently to address a number of interlinked issues:

First, to have a proper innovation base we will need a world-class education and research base to be able not only to compete but also to understand key technological developments.

Second, to build robust digital supply chains we will also need to have enough self-standing technology companies that can ensure secure supply of critical pieces if needed.

Third, to ensure our European firms have the capacity to compete in the face of state subsidies, weaker merger control, lack of market access and forced technology transfers. We need to face up to the fact that our liberal and social market economy is in direct competition with very different political-economic models, with a less clear separation between the state and business. And we need to work out what we're going to do about that.

Fourth, to address the 'winner-takes-all' aspects of the tech industry. US firms have secured dominant positions; Chinese rivals are catching up fast. US and Chinese firms have advantages in network industries that could result in entrenched monopolies, with long-lasting consequences for Europe's ability to compete in cutting-edge technologies. And we need to work out what we're going to do about that too.

And, fifth, to secure our critical digital infrastructure we are going to need to continue to mitigate the vulnerabilities and risks to our digital networks including the security implications of potential control of key components by foreign powers and non-state actors.

Europe has heft

There is of course no such thing as complete technological independence in an open, interconnected economy.

But an economy of 500 million inhabitants with a GDP of about €14,000 billion should certainly be able to master key technologies and secure critical infrastructures.

Europe has heft, we shouldn't be shy about making that count.

Making our voice count on these vital issues will not only help us bolster the resilience of our security and economic system but also help shape the future geopolitical context around us.

The current Commission has proposed under the next multiannual financial framework (MFF) to invest 15 billion EUR in ‘Digital and Industry’ for Artificial Intelligence, Cybersecurity, Quantum Computing, and much more through the Horizon Europe programme.

Under the Digital Europe programme, we have proposed for EUR 2.5 billion to be dedicated to AI to fund testing facilities as well as software and data platforms, and an additional EUR 2 billion to support other activities connected to AI.

But it is not just about funding – important as this is – it is also about policies. And I welcome the debate that is kicking off now in earnest.

In years gone by there were heated debates about sovereignty of key resources – energy – and pieces of infrastructure - transport, pipelines. The concept of sovereignty applies equally to today’s new infrastructures – digital networks and cloud computing – and new fields such as genomics and artificial intelligence.

In other words, we need to continue the discussion on our technological sovereignty in the new geotech world.

I welcome the fact the incoming European Commission President, Ursula von der Leyen, has underlined the importance of these issues.

She has tasked my colleague and Executive Vice-President-designate Margrethe Vestager to work on our European technological sovereignty, together with Commissioner-designate Sylvie Goulard.

She has also pledged to put forward legislation for a coordinated European approach on the human and ethical implications of AI within her first 100 days in office.

And she has proposed a new Digital Services Act, which will upgrade our liability and safety rules for digital platforms, services and products.

Certainly, these efforts – and more - will be vital if we are to ensure a prosperous, safe and democratic digital future for Europe.

Thank you.