Digitalisation and the EU's role in the World

By Margrethe Vestager | 1 June 2021

Key Issues

- Digitisation is changing the way that countries cooperate, compete and develop.

- The more we depend on technology, the more that creates vulnerabilities that can be used to attack us.

- Sovereignty does not mean autarky. It does not mean disengaging from the world around us. Europe is a trade and investment superpower – the world's largest trading bloc, comfortably ahead of both the US and China.

- We are moving in a direction of transatlantic convergence. Because we share the most fundamental values. We agree on the importance of fair and open markets, and the need to protect human rights and democracy in the digital age.

Digitalisation has transformed the way we shop, the way we talk to friends, and even how we get dressed for work. It has changed the meaning of industrial leadership. Digitalisation is now much about using data well. And like a fractal, the changes that we experience in our daily lives are repeated at bigger and bigger scales – all the way up to the canvas of global affairs.

Digitalisation is changing the way that countries cooperate, compete, and develop. And while it is as important as ever that Europe's foreign policy can offer security, prosperity, and freedom, digitalisation means that our ability to reach those goals depends on how we reach our partners across the world.

The deep integration in global supply chains provides the European industry with crucial markets and essential supplies.

But it also means our prosperity depends more than ever on our links to the world – on access to markets and suppliers, not least for vital technologies such as computer chips and artificial intelligence (AI) – and on the ability of European companies to compete on fair terms with their global rivals.

The more we depend on technology, the more we create vulnerabilities that can be used to attack us. As the coronavirus has threatened lives and livelihoods in Europe, those who wish us harm have seen new opportunities to undermine our security. They have mounted cyberattacks on our hospitals and spread disinformation that threatens our ability to fight the virus.

Even our ability to protect our rights and freedoms is linked to the actions of others beyond our shores.

Not long ago, I visited a research lab in Denmark where they are using AI to analyse the results of blood tests that can spot a whole range of different cancer types at an early stage so that people can get treatment quickly and lives can be saved. And the lab has done that in a way that fully protects sensitive data about people's health.

That is what we mean when we talk about human-centred technology. It's an attractive vision of the digital future – but it's a vision that's not available to everyone. In other parts of the world, authoritarian governments are building much less appealing models – models of surveillance and social control, where platforms manipulate people's choices and governments use technology to oppress minorities and limit free expression.

The more those models expand across the world, the harder it will be to build a successful human-centred digital ecosystem in Europe.

The importance of openness

In this digital world, our security, our prosperity, and even our freedom are deeply dependent on others around us. This is why it is so important for Europe to assert our digital sovereignty. This is our ability to ensure that the key decisions that will shape our digital economies and societies are taken within our European democracies.

But sovereignty does not mean autarky. It does not mean disengaging from the world around us. Europe is a trade and investment superpower – the world's largest trading bloc, comfortably ahead of both the US and China. Trade accounts for more than a third of our GDP, and it supports 35 million European jobs. So I find it unthinkable – as well as impossible – that Europe would turn its back on the openness that serves us so well.

But alongside that openness, we need a clear understanding of how our dependence on others creates risks – and an effective strategy to deal with those risks.

Europe's capacity to act

There are two parts to that strategy. In Europe, we need the right powers and the right rules to protect Europeans from the harm that the actions of foreign countries can create. And beyond our shores, we need to work with like-minded countries to create a safe and fair global digital environment.

This strategy can only succeed if Europe has the capacity to act. We need the weight and the influence to make our own decisions here at home, and promote our vision overseas.

We start from a strong position. Our economy accounts for a sixth of the world's GDP. But that doesn't truly reflect the weight that we have in the digital world. In Europe you find some of the most digitalised countries in the world. And we've successfully converted that leadership into influence – our rules on privacy, for instance, have become an effective global standard.

To maintain this sort of influence, we need to stay at the forefront of digitisation, as the digital world does not stand still.

Therefore, we proposed a Digital Compass last March, which sets out specific goals for transforming our economies and societies by 2030. This Compass marks out the path to a Digital Decade, where Europe can take the lead in advanced technologies like quantum computing and cutting-edge computer chips. It sets milestones for digitising businesses and public authorities, and for building the advanced digital skills that will offer good jobs for Europeans – and help industry compete.

All these goals are backed up by the investment necessary to realise them. At least 20 percent of the more than 670 billion euros from our Recovery and Resilience Fund will support the digital transition. Therefore, we have the means to shape the digital future in a way that benefits the interests of Europeans.

Managing dependencies – the internal aspect

Europe has to take energetic actions at home to be able to resist cyberattacks. We have supported EU countries to develop a toolbox to keep 5G networks secure all over Europe. We need to protect ourselves from the risk that some untrustworthy

suppliers could offer ways in for attacks on this vital infrastructure. We are reforming the Networks and Information Systems Directive to ensure a high level of protection for all important and essential economic actors in our Union. There is not only talk but also action: last summer we put sanctions in place, for the first time, against persons and organisations from Russia, China, and North Korea that were involved in recent cyberattacks.

We are also making sure that we have the right rules in place to protect fundamental rights in the digital future. Our proposal for a Digital Services Act aims to give Europeans the same protection against dangerous goods and harmful content online as offline, while also protecting their freedom

share – shaping global standards on things like AI or cybersecurity; promoting fair and open digital markets; and sharing our human-centred model of digitalisation.

There is no doubt in my mind that this cooperation has to start with a close partnership with the United States. Of course, we do not always see things the same way. We can, and we do, have different interests and opinions. We need to have dependencies to manage, as each side reassesses its vulnerabilities.

But my sense is that we are moving in a direction of convergence, because we share the most fundamental values. We agree on the importance

I find it unthinkable – as well as impossible – that Europe would turn its back on the openness that serves us so well.

of expression. In April we put forward a new legal framework that will use a risk-based approach to ensure that when artificial intelligence is used in sensitive areas – like deciding who gets a job or a loan – decisions are made transparently and without bias.

We are also taking action to make sure our economy is fair, as well as open. Our proposal for a Digital Markets Act will make sure digital gatekeepers use their power fairly, so the millions of businesses that rely on them have a fair chance to innovate and compete. And just last month, we proposed legislation to deal with foreign subsidies that would harm fair competition in Europe.

International cooperation

But this can not be done purely from within. We don't want Europe to be an island in a hostile sea, relying on these rules to hold back the tide of a global digital environment that's fundamentally opposed to our values and interests. Instead, we want to work with like-minded countries to advance the ideals that we

of fair and open markets, and the need to protect human rights and democracy in the digital age. We have important shared interests in cybersecurity. We even now have a shared understanding that the global tax system needs to be overhauled, so that large businesses, including digital ones, pay their fair share of tax in the countries where they do business.

For these reasons we have proposed to set up a Transatlantic Trade and Technology Council as a forum to convert those shared values into effective partnerships on practical issues.

And this transatlantic cooperation can also be the core of something even bigger – of a coalition of like-minded countries that share our digital vision.

It is easy to forget, among all the noise about how the US and China are going their separate ways, that other countries, too, have their own views about the digital future they want for their people. At the end of April 2021, I was at the meeting of G7 Digital Ministers, which included guests from Australia,

India, Korea, and South Africa. I was struck by how much we all had in common – same analysis, same assessment of the challenges that we face.

And I am convinced that this shared understanding can give us a firm platform for shaping the future together. We can work together to promote global standards that will keep the digital world open and fair. We can give substance to our belief in human-centred technology, by working on shared approaches to regulation. And we can work together to tackle the risks that come along with global supply chains, by reaching agreements to secure supplies, underwriting trust and resilience with mutual dependence.

At the same time, we also need to make sure that our vision of a human-centred digital future is reflected in the way we cooperate with our partners in the Global South.

Between 2005 and 2019, the proportion of Africans with Internet access went from 2% to 40%. This has helped improve the lives of millions of people. And yet, that still leaves more than half the continent disconnected – and even behind those figures hide big divides, not just from one country to another, but between city and countryside, or between women and men. For instance, Africa's gender gap in Internet access is more than 30% – and in recent years, that gap has actually been growing, not shrinking as it ought to.

Closing these divides can help some of the world's poorest countries make huge strides towards reaching the Sustainable Development Goals – not just the goal of universal, affordable Internet access by 2030, but also other goals like better health, better education, and gender equality. That's partly a matter of building infrastructure – but infrastructure alone cannot guarantee that digitalisation is fair and inclusive. We have seen how certain investments can have downsides too, when it comes to exposing citizens to surveillance, repression, or insecurity. Human rights and digitalisation are two sides of the same coin. They must come together.

This is why our new cooperation programmes will not just provide the money to build new digital connectivity, but also help to develop strong standards for a safe, trustworthy digital world, in areas like privacy and cybersecurity. So that, alongside physical infrastructure, citizens in developing countries can benefit from the same sort of human-centred model of digitalisation that we expect for ourselves here in Europe.

Conclusion

Decades of continuous digital innovation have taught us to look forward. We may not know exactly what the future will look like. But we have a shared understanding that if we want to guide technology, so it works in a way that fits with our interests and our values, we have to act early.

It is clear that our success in doing that will be deeply affected, not just by our own actions, but also by the choices of our partners throughout the world. So this is a moment when our digital policies and our external policies need to come together. Because our ability to promise Europeans a positive digital future doesn't just depend on what happens in Europe – but on how we manage to shape the world around us.

ABOUT THE AUTHOR
Margrethe Vestager

Margrethe Vestager is Executive Vice-President at the European Commission, responsible for 'A Europe Fit for a Digital Age'. This brief draws on the Executive Vice-President's keynote address at the 7th edition of the European Union in International Affairs conference held in Brussels between 26-28 May 2021.

@vestager

The **Centre for Security, Diplomacy and Strategy (CSDS)** seeks to contribute to a better understanding of the key contemporary security and diplomatic challenges of the 21st century – and their impact on Europe – while reaching out to the policy community that will ultimately need to handle such challenges. Our expertise in security studies will seek to establish comprehensive theoretical and policy coverage of strategic competition and its impact on Europe, whilst paying particular attention to the Transatlantic relationship and the wider Indo-Pacific region. Diplomacy as a field of study will be treated broadly and comparatively to encompass traditional statecraft and foreign policy analysis, as well as public, economic and cultural diplomacy.

The **CSDS Policy Brief** offers a peer-reviewed, interdisciplinary platform for critical analysis, information and interaction. In providing concise and to the point information, it serves as a reference point for policy makers in discussing geo-political, geo-economic and security issues of relevance for Europe. Subscribe here. The CSDS Policy Brief is a discussion forum; authors express their own views. If you consider contributing, contact the editor Prof. Michael Reiterer: michael.reiterer@vub.be.

Follow us at:
Twitter @CSDS_Brussels   LinkedIn CSDS Brussels   Youtube CSDS
http://csds.brussels-school.be

The Brussels School of Governance is an alliance between the Institute for European Studies (Vrije Universiteit Brussel) and Vesalius College.

Visitor's address:
Pleinlaan 5, 1050 Brussels, Belgium
Mailing address:
Pleinlaan 2, 1050 Brussels, Belgium

info_bsog@vub.be

www.brussels-school.be