FINDING DIGITAL FREEDOM IN A CROWDED WORLD

SPECIAL REPORT | SEPTEMBER 2019
https://eurac.tv/9QI4
As the EU enters new and uncharted waters in the digital world, a number of pressing questions emerge as to how the bloc can distinguish itself in a highly competitive marketplace.

With input from high-level political officials, industry leaders and key stakeholders, this special report examines the ways in which Europe is working towards establishing a leading role in the technologies of tomorrow, including 5G and cloud infrastructure.

Nevertheless, on the crest of good intentions, Europe also faces a myriad of challenges. Such include ensuring that cybersecurity standards meet trust expectations and that the bloc’s highly-regarded data protection principles are duly abided by. Amid an unstable and volatile global political context, such challenges only become more explicit. How Europe responds to these hurdles will define its future clout and influence in the digital arena.
The EU’s search for tough cybersecurity standards

By Samuel Stolton | EURACTIV.com

Appearing before MEPs in the European Parliament’s Industry Committee last week, the new head of the EU’s cybersecurity agency ENISA, Juhan Lepassaar, said he hopes the EU’s recently adopted cybersecurity framework will become the “the new global standard for trust.”

Lepassaar has jumped into one of Brussels’ cybersecurity driving seats at a time when the EU is seeking to distinguish its clout in the field worldwide. Along with a new Commission bent on ensuring the strategic autonomy of the EU while new technologies are developing faster than they can be regulated, Lepassaar is in a position to hold substantial sway over the EU’s direction in cybersecurity.

The new ENISA chief is cut from the same cloth as many EU officials working in the cybersecurity field, regarding ‘trust’ as an essential facet in consumer protection, and hoping that the EU’s recently adopted cybersecurity act can, just like the bloc’s data protection standards, distinguish the European Union as a guardian of civil liberties.

Having previously been the head of cabinet of Andrus Ansip, the Commission’s digital vice president, Continued on Page 5
Continued from Page 4

Lepassaar has no doubt taken influence from his erstwhile superior. Ansip told EURACTIV earlier this year that ‘trust is a must’ in the development of next generation technologies, and that consumer protection in cybersecurity should rank highly in the EU’s priorities for the coming years.

**EUROPE’S IMMEDIATE CONCERNS**

The incoming Commission President, Ursula von der Leyen, will have a series of politically delicate hurdles to contend with in the field of cybersecurity. Not least in the domain of 5G, where the EU has come under increased pressure from American counterparts set to adopt a hostile position against next-generation technologies emanating from the far east.

Last week, Washington signed a joint declaration with Poland to collaborate on 5G security in what US Vice President Mike Pence said would “set a vital example for the rest of Europe”.

Moreover, last week, the French telecom company Iliad announced that it has selected the Finnish network vendor Nokia as a partner in expanding its 5G network, which some regard as an indication that Europe’s strategic autonomy in the development of next-generation technologies will emerge as an industry priority.

The news came not long after France made further cybersecurity commitments on the sidelines of the G7 meeting, as part of the Indo-French Roadmap on Cybersecurity and Digital Technology, in which the countries rally for “responsible state behaviour in cyberspace as well as confidence and capacity-building measures developed within the framework of the United Nations.”

Europe-wide, following a Commission recommendation for a common EU approach to the security of 5G networks, member states have recently submitted national risk assessments – providing an overview of their most pressing concerns in the future development of 5G infrastructure. These assessments will feed into the next phase, a EU-wide risk assessment to be completed by 1 October.

Von der Leyen is well-placed to lead the EU’s direction in this field, having been Germany’s defence minister between 2013 and 2019, when she established the country’s first military cyber command. She also stood out in the international defence arena, with the UK’s former Defence Minister Michael Fallon referring to her as a “star presence in the NATO community.”

Following previous legislative devices such as the 2016 NIS Directive and the Cybersecurity Act, which was adopted earlier this year, there is a broader background to how trust may be safeguarded for the future, and there is no shortage of those who believe the EU’s cybersecurity approach could well be ramped up as part of the Commission’s forthcoming mandate.

**CERTIFICATION**

As part of the EU’s cybersecurity act, cybersecurity certification schemes may become commonplace for a breath of goods and services – the scope of which is still to be hashed out by the Commission working alongside ENISA.

EURACTIV understands that the priority for the EU is to ensure that hackable goods connected to a wider network of devices are likely to be included in the scope of the certification framework – including equipment used for 5G infrastructure, as well as Internet of Things devices and cloud services.

Nonetheless, at the time of the adoption of the cybersecurity act, some in Brussels were pushing for a mandatory certification instrument in the EU, citing, in fact, similar reasons to ENISA’s new chief, Lepassaar, on how such approach could assist the EU in the long term.

An official from the German telecommunications giant Deutsche Telekom (DT) informed EURACTIV that an obligatory approach would assist the market in helping to converge standards.

“For us, a mandatory certification framework would have been preferable,” the DT official stated. “This is the best way we can showcase to the world our commitment to high-class cybersecurity standards, without compromise.”

Nonetheless, a mandatory arrangement may not be long in the offing. Following the rollout of the voluntary framework, the hope is that the market will have its say on the value of the certification before a Commission assessment, the first of which is due to take place before the end of 2023, will evaluate whether mandatory certification is necessary.

EURACTIV caught up with an insider working in the cybersecurity industry, who said industry should prepare for itself for a tougher EU approach in the coming years.

“On product certification, mandatory schemes are likely to be considered in the years to come,” the source said, adding that the possible fragmentation of the market in the field of cybersecurity is a risk that the bloc should take account of.

“In order not to deviate from the objectives of the EU Cybersecurity Act, mandatory certification should be considered at EU rather than at national level, it should be market-relevant and accompanied by appropriate transitional or implementation phases,” the source said.

Continued on Page 6
QUANTUM TECHNOLOGIES

Indeed, it’s not only in the private sector that the EU will look to impose itself in terms of cybersecurity. There are plans to modernise the 2008 European Critical Infrastructure Protection Directive and build a European Cybersecurity Shield. More recently, the EU has also made a series of significant steps in attempting to bolster the security of its critical infrastructures.

Following talks in June at Bucharest’s Digital Assembly, a grouping of seven EU member states agreed to take the first steps in developing and deploying a quantum communication infrastructure (QCI) across the EU over the next decade.

The EU hopes that the measures will enable data to be transmitted and stored ultra-securely, and communication assets to be linked all over the bloc, bolstering the security of critical infrastructure against cyber threats and protecting smart energy grids, air traffic control, banks, healthcare facilities and others from hacking.

The measures will help “keep the transmission, protection and long-term storage of sensitive data safe, and ensure the sovereignty of sensitive governmental information,” outgoing Digital Commissioner Ansip said earlier this year.

Pilot projects for Europe’s Quantum Internet plans commenced just last week, with tests due to take place in Austria, Spain, Poland, Germany, Netherlands, Switzerland, France, Italy, UK, Greece and the Czech Republic, over the next three years.

Helmut Leopold, the head of the Centre for Digital Safety and Security at the Austrian Institute of Technology, which is coordinating the project, was unambiguous in the importance of quantum technologies in helping to safeguard Europe’s cyberspace and effectively, ensure that Lepassaar’s commitment to a trustworthy cyberspace comes to fruition.

“This will enable an innovative eco-system for creating a new perspective for our secure digital Europe and building the foundation for next-generation communication technologies,” he said.
Europe needs ‘digital border controls,’ industry chief says

By Samuel Stolton | EURACTIV.com

Europe should consider establishing a ‘digital border control,’ as a means of obstructing internet access to hostile actors in the event of a serious cyberattack, the head of Deutsche Telekom’s cybersecurity division has told EURACTIV.

“In Europe, there’s no way of to shield ourselves in the case of an attack emanating from Asia or the Americas on our infrastructure here,” Thomas Tschersich, Head of Group Security at Deutsche Telekom said. “Sitting in the middle, we’re connected to all entities around us. We don’t have a clue how to disconnect without switching off the whole infrastructure in Europe as well.”

Tschersich added that the state of play across the Atlantic offers US citizens an equal balance of freedom and security, when faced with a potentially debilitating cyberattack.

“In the US, for example, you have just 11 connection points to the global Internet. If you cut that off, the inner US network will function well. The main infrastructure would be up and running fine.”

PROTECTING THE INTERNAL MARKET

Tschersich added that a political debate needs to happen in Europe, to discuss how the continent would confront a potential cyberattack and that it is vital to “protect the functionality of the internal market” in the event of a hostile infiltration of Europe’s network infrastructure.

As part of the European Commission’s newly distributed portfolios, French nominee Sylvie Goulard, will acquire control of “building a real single market for cybersecurity,” and be responsible for “implementing rules on security of network and information systems [and] rapid emergency response strategies.”

Cybersecurity is an area where France have long sought to impose their influence – most recently signalling their commitment to the Indo-French Roadmap on Cybersecurity and Digital Technology, on the sidelines of the G7 talks in Biarritz.

Moreover, the country has been forthcoming in their reading of international law on cyberspace norms, having produced a government

Continued on Page 8
report in which they reserve the right
to respond to cyberattacks, in addition
to attribution, according to researcher
Łukasz Olejnik.

INTERNET SHUTDOWNS?

Tschersich’s notion that Europe
should consider closing-off access to
certain parts of the internet has drawn
criticism. EURACTIV caught up with
Guillermo Beltrà, policy director at
the digital rights group Access Now,
to hear his thoughts on the proposals.
“Shutting off the internet, even if
only parts of it, should never be the
default policy tool at hand,” he said.
“Establishing policies that include
internet shutdowns and network
separation is not the best approach to
create effective, resilient cybersecurity
models that put users’ interest at the
forefront.”

Moreover, EURACTIV also heard
from MEP Patrick Breyer, who sits
with the Greens in the European
Parliament. He had some even tougher
words to say. “Kill-switch capacities
could be abused by hackers and make
the Internet less safe. Scare stories
about terrorists wanting to shut the
Internet down are mostly fairy tales.
We shouldn’t use the same means that
we deplore,” he said.

Nevertheless, Tschersich was
adamant that he would never advocate
the obstruction of internet services.
“I’m not talking about blocking
access to services,” he said. “I’m
talking about blocking massive attacks
coming from the outside Europe,
trying to harm us. The question is how
we are prepared.”

Tschersich went further in
referencing the 2017 cyberattacks
on Ukraine – which saw several
ministries, banks, metro systems
and state-owned enterprises hit by a
series of cyberattacks. The offensive,
Tschersich says, “more or less,
switched off the Ukraine economy for
two days...and there was no protection
at all.”

In this scenario, a ‘digital border
control,’ could be switched on, hostile
foreign access to the affected areas
blocked, with the inner network
still functioning, Tschersich says,
adding that there would inevitably
be a restriction of access to external
services, but that would be a price
worth paying.

Access Now’s Beltrà thinks that
the EU should instead push for
better coordination among national
information security and incident
response agencies, and use legislative
instruments currently at its disposal,
including the Network Information

An industry insider told
EURACTIV, that the notion of a digital
border control sounds rather “drastic,”
as dealing with the more sophisticated
cyber attacks of the future will require
“more targeted, concerted efforts.”

WANNACRY

One of the most severe attacks to
hit critical infrastructures in Europe
occurred as part of the 2017 WannaCry
ransom-wear attacks.

The attack is said to have been one
of the principal determinants in cyber
threats being identified as the most
pressing risks for the bloc in the World
Economic Forum’s Regional Risks
to Doing Business report that was
published last year.

The study asked more than 12,500
executives around the world to select
the global risks that pose the most
significant concerns to doing business
within the next 10 years.

“2017 was a tipping point in the
prevalence of cyberattacks in the EU,”
the lead author of the report, Aengus
Collins, recently told EURACTIV. “The
most significant of which was, of
course, the WannaCry ransomware
attack.” Europol described the
WannaCry attack as “unprecedented”
in scale, after it had struck 200,000
computers across 150 countries.
The hit infected systems with a
ransomware which targeted Microsoft
Windows operating systems, with
targets including the UK’s National
Health Service and German rail
infrastructure.

For Tschersich, attacks on the scale
of WannaCry or Petya are indications
that Europe finds itself helplessly
exposed in cyberspace – reliant on
access to external services while also
attempting to present itself as serious
on cybersecurity.

And regardless of well-intentioned
efforts in the field by a handful of
individual member states, he is clear
that this is a question for Europe as
a whole. “It can’t be done by nation
states alone, it needs to be done on a
European level,” he said.
Europe’s global standing in the cloud infrastructure market has long come under scrutiny for a lack of investment and presence compared with global players. EURACTIV has caught up with DG Connect’s Roberto Viola to analyse the importance of the EU’s data economy and examine how Europe can achieve a greater level of independence in its cloud services.

Roberto Viola is the director-general at the European Commission’s Directorate-General for Communications Networks, Content and Technology (DG CONNECT). He responded to questions from EURACTIV’s Digital Editor Samuel Stolton.

It has recently been claimed that data is now widely considered a more valuable

Continued on Page 10
In terms of Europe's data-driven economy, what can be done to ensure that the EU makes the most of this landscape, while also bearing in mind the importance of data protection standards?

The EU boasts a large market for online content and database services. Cloud can deliver an almost unlimited and scalable capacity of computing and storage that underpins all digital activity of large and small businesses as well as public administrations.

It is essential to implement the existing European consumer and data protection rules in order to ensure that developments in the digital age are compatible with European values and strategic interest. These rules and standards must be applicable and enforceable across the Union’s territory and on all actors accessing our market in order to ensure a level playing field and free and fair competition and to see the emergence of a strong European GDPR compliant industry.

In addition, we are discussing with member states, industry and other stakeholders the creation of common European data spaces in a number of sectors. If we can scale up the existing data sets in member states to the European level, we can compete on a global scale. Our proposal for a Digital Europe Programme will help finance these activities.

Can you give some concrete examples of how Europe’s cloud initiative is helping research and development across numerous sectors?

The European Open Science Cloud enables researchers to combine multiple datasets and services, developed by different organisations in Europe, to predict the spread of dangerous and invasive species in the Mediterranean Sea and to highlight the high-risk zones for fisheries and health security in the area.

Another example is the use of Cloud's resources, together with high-performance computing and Artificial Intelligence methodologies, to foresee and manage natural hazards and extreme events that have led to over one million fatalities and three trillion euro of economic loss over the last 20 years. There are similar stories in other sectors such as the observation of the carbon cycle, molecular imaging with photos and neutrons, or digital cultural heritage.

In addition, the EU has invested no less than €200 million in research and innovation in cloud computing technologies since 2014. Some interesting research such as the ‘SUNFISH project’ led to the development of federations of public sector clouds using blockchain for sharing sensitive data such as criminal records, taxpayer details and data on healthcare among European public administrations.

There are many risks associated with the concentration of Big Data. In terms of cybersecurity, what measures are being taken to ensure that Europe’s cloud initiative has the appropriate safeguards in place to stop data from being used for malicious means?

Secure cloud infrastructures and services are indispensable to the provision of any big data analytics, artificial intelligence, blockchain services. Since December 2017, the Commission has been facilitating the self-regulatory work of the European Cloud Service Provider Working Group, that is composed of various stakeholders such as national cybersecurity authorities, cloud service providers, private certification bodies, universities and end- users.

In June 2019, the group achieved its objective to present its final recommendations for a European cloud certification scheme. On 27 June 2019, the Cybersecurity Act entered into force, on which basis the European Commission, supported by European agency for cybersecurity (ENISA), can establish a European cybersecurity certification scheme for cloud.

A specific example of a potential risk came up recently when it transpired that German data protection officials consider Amazon’s cloud hosting services to be unsafe for the storing of German police data because they could be subject to US spying. How much does the US’s cloud act, which compels US tech firms to hand over data to the government - regardless of where it is located – compromise the EU’s high standards of data protection?

We understand the concerns among European citizens, businesses and authorities around the handing over of their data to foreign authorities. To address these concerns in the context of criminal investigations, the Commission is going to engage in negotiations with the US on the EU-US agreement on the exchange...
of electronic evidence in criminal matters. The Commission already obtained a mandate from the Council in June this year.

This agreement will clarify the conditions under which law enforcement authorities from both sides of the Atlantic may require access to the data of individuals or businesses stored by cloud service providers in each other's jurisdiction, while ensuring appropriate safeguards for the protection of fundamental rights and freedoms, including data protection.

The European Data Protection Board published an impact assessment in mid-July, in which they stated that the Cloud Act conflicts with GDPR. Do you agree with this assessment?

It is worth noting that this document only contains an initial assessment and recognises that further analysis is required. According to this document, transfers in response to a Cloud Act request may be validly based on the GDPR in certain circumstances.

More importantly, while we may not necessarily agree on every detail of this analysis, we certainly agree with the conclusion of this document that an EU-US agreement on access to electronic evidence is the best instrument to ensure both a high level of data protection for Europeans and legal certainty for businesses.

Currently, the UK has many more data centres than anywhere else in Europe. How will Brexit impact Europe's data economy?

Continental Europe hosts all the necessary data infrastructure including data centres for a healthy data economy. For instance, all large (cloud) service providers have a local presence in continental Europe with multiple data centres.

In general, it is our intention to build a framework for international data flows with third countries that safeguards the protection of EU citizens' data and ensures data security.

While the Commission does not speculate on the possible economic implications of different scenarios, it is clear that a withdrawal of the United Kingdom without an agreement would have a serious negative economic impact, and that this impact might be proportionally much greater in the United Kingdom than in the EU27 Member States. While we clearly prefer a withdrawal of the UK with an agreement, we are prepared for all other outcomes as well.

According to recent estimates from the International Data Corporation (IDC), Europe's public cloud market is expected to grow at a 22% rate for the next three years, with US companies taking full advantage of the lack of EU mega cloud providers. Is this an issue for the bloc?

Yes, that is why we are monitoring closely the global cloud market developments. We consider cloud to be an essential and strategic enabling technology that Europe needs to master to ensure digital leadership. By 2022, IDC also estimates that storage deployment modes to manage cognitive and AI workloads will grow at a yearly rate of 36% and it will be based on public, private and hybrid cloud infrastructures.

For Europe to lead the next technological race we need to prioritise investment towards strengthening the existing European cloud infrastructure and service industrial basis. That is why we have proposed more EU funds for cloud under the next multi-financial framework 2021-2027. We invite all to participate in the open public consultations on the new programmes.

What is the future for Europe’s cloud infrastructure and what practical improvements will people see in their everyday lives as a result of the EU’s developments in the field?

While energy-efficient interconnections of existing cloud infrastructures across the EU territory together with cross-border cloud service offerings are surely important, it is too early to say what the future Commission priorities in this area will be.

The federations of cloud infrastructures and services will enhance Europe’s competitiveness and security, with clear advantages for SMEs and citizens.
In October, German Economy Minister Peter Altmaier is set to reveal more detailed plans for the establishment of a landmark European Cloud initiative known as ‘Gaia-X.’

Up until now, the European cloud marketplace has been dominated by US firms and many in Brussels are concerned that American involvement in the industry is compromising EU data protection standards and by extension, the concept of Europe’s ‘digital sovereignty.’

Earlier this year, Altmaier said “Germany has a claim to digital sovereignty. That’s why it’s important to us that cloud solutions are not just created in the U.S.” Following these remarks, delivered in July, the Frankfurter Allgemeine Zeitung leaked an internal government paper in August that revealed Altmaier’s plans, with the German economy minister conceding that “cloud industry is currently largely dominated by US corporations such as Amazon.”

This is a line echoed by the Former

Continued on Page 13
German Foreign Minister Joschka Fischer, who said in a recent op-ed that in order to safeguard it digital sovereignty, “Europe will need to make massive investments in cloud-computing capacity.”

Speaking to EURACTIV recently, a spokesperson from the German Federal Ministry for Economic Affairs said that “data sovereignty and broad data availability can only be really achieved with a data infrastructure that complies with ‘made in Europe’ security standards.”

The official also confirmed that the Federal Ministry intends to “push ahead with the construction of such a data infrastructure” in order to pursue this objective of achieving sovereignty in the field.

The concept of digital sovereignty on the bloc is founded on the principle that the EU should be afforded due autonomy in building up its tech industry, and therefore the ability to effectively implement regulatory frameworks that foster its digital development, rather than hinder it.

**DIGITAL SOVEREIGNTY**

EURACTIV caught up with an expert in the field, Chief Technology and Digital Innovation Officer for the City of Barcelona, Francesca Bria, in order to get to the bottom of what digital sovereignty means in practice.

“Digital sovereignty means that digital technologies can facilitate the transition from today’s digital economy of surveillance capitalism and data extractivism – whereby a handful of US and China-based corporations battle for global digital supremacy - to a people-centric digital future promoted by Europe based on better workers, environmental, and citizens’ rights, to bring long-term social innovation,” she said.

Bria added that the areas in which the EU currently falls short include dependencies on companies managing large data flows. “Europe should tackle the dependence on external technologies: most hardware and software EU critical national infrastructure are built outside of the EU, including companies managing large data flows,” she said.

“Since data is the raw material of the digital economy and fuels AI, we need to take back control of data, and recognise data as a public good, as a public infrastructure, where the terms of data control need to be defined by citizens themselves. If you see who owns the software, the hardware, the chips, the 5G network in Europe and the data which is consumed on top of it, it’s mainly foreign multinationals. So we need to tackle dependence on external technology.”

Bria concluded by saying that unless Europe does not pursue a proactive approach towards obtaining its own digital sovereignty, “we could lose our competitiveness in key industries of the future and become a sort of a digital colony”.

She added that data sovereignty should be a starting point, “to take back the control of data and use city data to tackle our big urban and social challenges: climate, sustainable mobility, healthcare, education.”

And US investment into the EU’s cloud infrastructure is a case in point with respect to the EU’s reliance on foreign services.

The apprehension in this respect in the cloud market is understandable. According to recent estimates from the International Data Corporation (IDC), Europe’s public cloud market is understandable. According to recent estimates from the International Data Corporation (IDC), Europe’s public cloud market is expected to grow at a 22% rate for the next three years, with US companies taking full advantage of the lack of EU megacloud providers.

December 2018 saw Amazon’s AWS opening new data centres in Sweden, while Microsoft announced plans last year to build data centres in Norway, Germany and Switzerland.

**US CLOUD ACT VS GDPR**

But of course, the question is not only an economic one. There are potential legal conflicts in the offing, too. An industry source has informed EURACTIV that due to American investments into the EU’s cloud marketplace, the EU’s high-quality data protection standards are in danger of being compromised.

Earlier this year, following a question from the European Parliament’s Committee on Civil liberties, the European data protection board released an analysis of the potential impacts of the US Cloud Act on GDPR, in which they highlighted potential points of conflict between the two legislations.

Controversy with regards to the American framework revolves around the fact that the Cloud Act gives US law enforcement agencies the legal right to force the release of customer data outside the US, resulting in an “extraterritorial reach of powers”, according to the European Data Protection Board.

“Service providers controlling personal data whose processing is subject to the GDPR or other EU or member states’ law will be susceptible to facing a conflict of laws between US law and the GDPR and other applicable EU or national law of the member states,” the EDPB opinion stated.

Effectively, the EDPB opinion is that the Cloud Act is not legally watertight in bypassing GDPR to justify personal data transfers to the US.

EURACTIV recently took this issue up with the Director General of the European Commission’s DG Connect, Roberto Viola, who said that according to the opinion of the EDPB, “transfers in response to a Cloud Act request may be validly based on the GDPR,” but only “in certain circumstances.”

Continued on Page 14
INDUSTRY LEAD

Any potential legal conundrum that could impact the integrity of the bloc's high data protection standards, is likely to be received with frustration in the EU. And the Germans believe that industry should lead the way in pursuing an independent cloud infrastructure.

The German Minister of Education and Research, Anja Karliczek, recently said that in order for Gaia-X to be a success, a commitment from industry players is required.

EURACTIV spoke to Frank Leibiger, Spokesperson for Cloud Computing at Deutsche Telekom, in order to get a sense of the response in the industry for the plans coming out of the German government.

Unsurprisingly, Leibiger said that DT is fully behind the plans and that “it's about enabling secure data flow between different cloud platforms based on well-structured, close cooperation between government and industry to support the globally connected economy and enable new, innovative business models.”

Leibiger added that the real driving force behind any future cloud infrastructure development in the EU will be a “strong public demand.”

France also backs the plans for a European-wide cloud infrastructure service, with Finance Minister Bruno Le Maire publicly confirming it.

In addition, the French Ministry of Interior is now preparing a roll-out of an internal cloud service known as Nextcloud, a move also made by the Swedish government, who have highlighted the concerns of the “ability of other countries to access, manipulate or deny access to information handled by a service provider.”

Europe's bid for digital sovereignty is likely to commence with a concerted effort to build its own cloud infrastructure service. The task at hand however, is by no means easy.

A senior EU Commission official told EURACTIV recently that Altmaier's Gaia-X plans “are good in theory, but in practice much more challenging to implement.”

Nevertheless, despite the pushback from certain US firms on Europe's cloud initiative, the Gaia-X plans are regarded as central to fulfilling incoming Commission President Ursula von der Leyen's objective of achieving strategic autonomy and digital sovereignty.

The plans are very much being billed as a civil liberties issue, something that former German minister Joschka Fischer regards as to be decided by European citizens, by putting “data at the service of the people,” in the words of Francesca Bria.
A clear trend can be seen for our digital future: What can be connected will be connected. But companies and societies do not network within traditional, analogous borders.

Dr. Thomas Kremer is a board member of Deutsche Telekom Group.

Machines are also increasingly being connected to one another. The Internet of Things is growing faster and faster. These developments give us a unique opportunity to bring the citizens of Europe closer together. And we must not let this opportunity pass us by. At the same time, the digital networks are and will become an increasingly attractive target for criminal or state-controlled cyber-attacks. Deutsche Telekom’s systems have reported up to 70 million different attacks on a single day this year. A new, sad record! And a leap compared to the figures of 2018! Thanks to our efforts, these attacks are not getting through, but the number is vertiginous.

For a company like Deutsche Telekom, but also for all other pan-European or globally active companies, it means being vigilant. Companies develop security strategies across borders, in Europe and worldwide. Cyber security may have been the nerds’ paradise discipline in the past. Today, cyber security belongs at board level, as it does here at Deutsche Telekom. To protect the EU’s digital internal market and the digital sovereignty of European companies and citizens, cyber security must therefore also become a top priority in Europe. With her new team the new President of the European Commission Ursula von der Leyen is responding to this challenge and giving top level attention to Cyber Security. I welcome it.

We talk a lot about the consequences of digitization these days. However, I very much miss a discussion: The European Union must develop into a digital security union.

For this necessary further development, I see us all as having a duty. This is a common task for the EU, its Member States, its citizens and its businesses. Only together we will achieve a better level of security, keep Europe competitive as a strong business location and finally assume a stronger role as a technology leader again.

Networks were and are the locomotive of the European internal market. Network operators are expanding this infrastructure more and more – more bandwidth, more speed. They thus promote growth in Europe and bring people closer together. This requires both strong political backing and forward-looking regulatory guidelines. Then this approach can succeed.

Continued on Page 16
COUNTERING COMPLEXITY

Cyber security is a highly complex issue in Europe. We are looking at a colourful patchwork of European and national regulations. In Europe, for example, we have the Directive on High Network and Information Security, the NIS Directive, the EU Cybersecurity Act and the currently discussed E-Evidence Regulation. A similar picture emerges in Germany. There are the IT Security Act 1.0 and 2.0 and additionally the security requirements for telecommunications network operators of the Federal Network Agency, the Federal Office for Information Security and the Federal Commissioner for Data Protection and Freedom of Information. A comparable patchwork with partly very different security requirements exists in the European finance or energy industry. The situation is similar for security-relevant certifications and the evaluation of products and services. That cannot remain so. This complexity costs us too much strength and speed.

The initiative of the new Commission-President to establish a Single Market for Cyber Security with a Joint Cyber Unit, is a step in the right direction. And it is positive news that a strong Vice-President will be in charge of the Commission’s Digital Agenda. Responsibility, resources and budget need to be concentrated in one hand. The incoming EU Commission attributes highest priority to our Digital Security. The European Parliament should support this policy. We need clear rules for cyberspace that are uniformly applied in Europe. This also requires more efficient EU structures.

EXCHANGE OF IDEAS ALONE IS NOT ENOUGH

On the question of “who should know that…”, we are fortunately one step further. The exchange between the central players in cyber security at state and private level has been intensified and improved in recent years. This applies especially to us in Germany. Nevertheless, significant improvements are still possible and necessary. The dialogue between industry, national supervisory authorities and national legislators is still too national today. This, too, is a direct result of the complicated legislative system. In the process, we need cross-border exchange more than ever on the way to a digital security union. This must be promoted. An agile body of experts consisting of state and business representatives from the EU member states is the logical consequence: network operators in dialogue with national and European institutions, with the task of drawing up concrete proposals. A pure exchange of ideas is not enough! And to avoid misunderstandings: Even in the area of cyber security, sovereign tasks cannot be taken over by private companies.

LOOKING FOR EUROPEAN STANDARDS

From a technical point of view, Europe’s level of security can be further improved, for example by trustworthy digital identities. Making people and machines unique on the Internet of Things is a prerequisite for secure digital legal and government transactions in the domestic market. And last but not least, this is the basis for citizens’ trust in e-government and digital services. You will already suspect it – here, too, every Member State is pursuing its own approach to solving the problem. That is not enough! Today, European citizens need a European digital identity, and not just ten years from now!

Instead of making cooperation more difficult, European network operators must be made easier to cooperate on security issues in particular. Secure networks are a prerequisite for the digital world, for a secure, digital Europe and for satisfied citizens.

And in general. For the digital space, analogue national borders are almost meaningless. The difference between digital and analogue is too often exploited by organised crime. For example, attacks via the Internet are deliberately launched from abroad in order to disguise the authors and elude access. How do we deal with this? Similar to the Schengen area in the real world, digital border controls can enable unhindered and secure data traffic to and from the EU to the whole world. In the event of a massive attack from outside the EU against the functioning of the internal market infrastructure, digital border controllers can be used to selectively prevent external attacks by means of technical filter lists.

There are still many unanswered questions. But one thing is perfectly clear: digital security is a top priority on the European agenda. Europe needs a shoulder-to-shoulder approach between European institutions and network operators to protect the digital world.

Europe needs a digital security union.