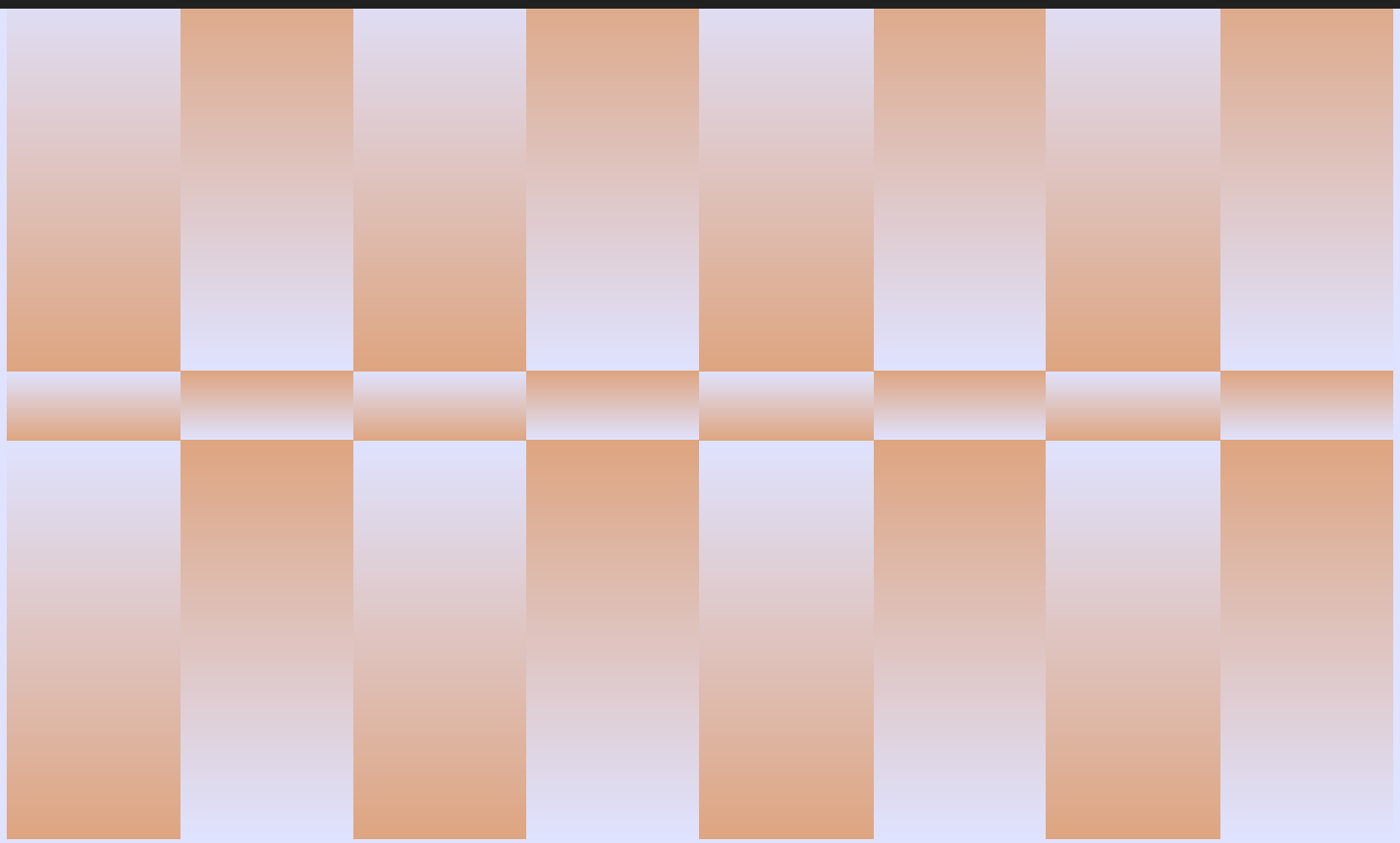

ARTICLE

interface's Tech Observatory

Our top pick of trends to keep an eye on at the start of this new EU Mandate (2024-2029)

Ernesto Oyarbide-Magaña

December 05, 2024

Stiftung Neue Verantwortung is now interface

Since 2014, our team has worked on building an independent think tank and publishing well-researched analysis for everyone who wants to understand or shape technology policy in Germany. If we have learned something over the last ten years, it is that the challenges posed by technology cannot be tackled by any country alone, especially when it comes to Europe. This is why our experts have not only focused on Germany during the past years, but also started working across Europe to provide expertise and policy ideas on AI, platform regulation, cyber security, government surveillance or semiconductor strategies.

For 2024 and beyond, we have set ourselves ambitious goals. We will further expand our research beyond Germany and develop SNV into a fully-fledged European Think Tank. We will also be tapping into new research areas and offering policy insights to a wider audience in Europe, recruiting new talent as well as building expert communities and networks in the process. Still, one of the most visible steps for this year is our new name that can be more easily pronounced by our growing international community.

Rest assured, our experts will still continue to engage with Germany's policy debates in a profound manner. Most importantly, we will remain independent, critical and focused on producing cutting-edge policy research and proposals in the public interest. With this new strategy, we just want to build a bigger house for a wider community.

Please reach out to us with questions and ideas at this stage.

Table of Contents

On 1 December the new European Commission finally took office. Now that all EU institutions are up and running, a multitude of challenges will have to be addressed during this new EU Mandate 2024-2029: from strengthening the Single Market and fostering competition, to enhancing our security and preparedness to future crises while upholding the rule of law and democracy all around the continent. Consequently, the new European Commission has already signalled to pursuing more than 160 upcoming policy initiatives in different sectors and diverse policy areas. And yet, most of these diverse initiatives have an important thing in common: the growing need to better understand tech issues.

Tech is the new horizontal: it permeates a myriad of issues related to Europe's economy, industry, security, innovation, healthcare, social rights, etc. Tech is also an ever-expanding field in continuous evolution, traits that lead to complexity. At *interface*, we are fully aware of how high the stakes are to get tech policy right, and we aim to bring clarity to this complexity. With over ten years of experience in offering tech analysis and insights, we are well-known by policymakers and legislators working on tech issues within the EU institutions and some national governments, such as Germany.

We know that time is precious, and that it is often difficult to keep up to date with tech policy. **That is why today we introduce *interface*'s tech observatory**: this brief resource summarises months –sometimes years– of the research we have carried out in highly complex tech areas, and offers you our top pick of trends in tech that will undoubtedly be making waves during this new EU Mandate. With these trends also come some action points for those wanting to keep tabs in this ever-evolving field. Our tech observatory also offers links to our experts' profiles and their more in-depth studies, so that the reader can move from the accessible summary into more granular detail at will.

As our research evolves, and Europe's policy priorities change, we also aim to update our tech observatory to reflect those changes accordingly. We hope that this type of resource proves useful to you. And we invite you to sign up to our newsletter to keep informed about our research and events. You can also contact us by email here.

> *interface* specialises in five important tech areas: global chip dynamics, platform oversight, artificial intelligence (AI), digital rights & government surveillance and cybersecurity.

Global Chip Dynamics

A short story of chips and PPE

In a recent study from *interface*, we look at the historical development of the EU's Chip Act and offer our perspective on Europe's chip strategy.

In many ways, Europe's current plans to bolster semiconductor production were greatly influenced by the years of the COVID-19 pandemic. During those times of crisis, an overreliance on global private-sector supply chains led to tense moments of significant shortage in essential products, such as personal protective equipment (PPE) at the beginning of the pandemic, but also to other important items during the months that followed, such as chips. Out of the feeling of "powerlessness" came the desire to become more strategically autonomous in key sectors. The EU Chips act became a policy response to this feeling; and it helped enshrine in the minds of many policymakers that we need to reach the goal of 20% of the global chip production by 2030.

The EU Chips Act came into force in September 2023. It has introduced many noteworthy ideas and initiatives, such as looking at ways to subsidise manufacturing and strengthen chip design, or increase resources for research and development (R&D) and allow for easier access to finance. However, to this date, it still fails to meaningfully articulate "why" we should be doing all these things.

The EU Chips Act: A strong ambition that is still in search for a robust strategy

For instance, semiconductors are not like PPE for many reasons. Chiefly among these reasons is that modern products are made of a sheer diversity of chips that are all essential for the assembly of a piece of electronics. Specializing in the production of all of these is nearly impossible.

In addition, even if Europe were to reach its 20% global production goal, we would still not be able to produce "in house" all the types of chips that are required for a smartphone, an ATM or a car. In the years to come, interdependencies will continue to exist, as many non-European countries will keep holding indispensable roles in the transnational value chain. For example, we will stay dependent from equipment suppliers from Japan, or from assembly, test and packaging facilities in Southeast Asia.

This structure of the global value chain puts Europe right in the middle of intensifying geopolitical tensions. All the talk about a strategic autonomy in the news mirrors the important realisation that chips are a strategic asset. But in its current form the EU Chips act is not a completely well thought long-term initiative with a clear vision. It fails to offer meaningful longstanding policy objectives that go beyond the goal to reach 20% of global production. It also doesn't offer us too many any instruments by which to assess whether European efforts toward chip development are going in the right direction. Ultimately, we need to think about who we want to be dependent on (democratic allies, partnerships, etc.), and for which applications.

At *interface*, we have been monitoring some important chip agreements around the world. In the United States, for example, the CHIPS for America Act was in good part made to 'counter China'. In Japan, a semiconductor strategy was developed to ensure the 'strategic indispensability' of the country's companies around the globe. But Europe still needs to decide, in a clear and detailed manner, on a geopolitical strategy to better know where it wants to go with its current chip production plans.

The chip industry is currently set to become a massive polluter

Another important challenge that is not well addressed by the EU Chips Act has to do with the growing ecological footprint of this industry. This will become a pressing issue in the years to come – both on the European and international levels– due to the significant increase in chip demand, which is also leading to massive plans for expansion of chip production globally.

For instance, a large semiconductor factory is already using up to 38 million litres of water per day for its operations, which is the equivalent consumption of around 300 thousand people in Germany. Chip production also relies on chemicals like fluorinated gases with a high global warming potential and forever chemicals.

Perhaps more importantly, if the EU Chips Act's goal of 20% production share by 2030 is met, emissions are projected to at least quadruple by 2030, catching up and even surpassing high-emission industries such as chemicals today, even if renewable energy usage rises significantly.

Action Points

During this new EU mandate, policymakers at each member state will have to properly coordinate and work hard towards the correct implementation of the EU Chips Act and come up with follow-up actions.

They will need to get a robust understanding and a value chain mapping of their

domestic chip ecosystem to understand its strengths and weaknesses. Additionally, member states will also have to start applying a geopolitical lens and see how the EU Chips Act interplays with different policy issues at the European and national levels, such as the block's goals in competition and trade. Mid- to long-term, these actions on both the national and European levels need to be translated in a long-term chip strategy that gives a clear vision, milestones and goals.

Most notably, there will be a great need to harmonise chip production and sustainability goals; and integrate these actions into industrial policies. Right now, a lack of transparency not only hinders a clear assessment of the ecological footprint of chip production, but is also probably limiting the effectiveness of Europe's ambitions towards becoming a circular economy. It is crucial that new upcoming directives such as the Corporate Sustainability Reporting Directive (CSRD) or the Digital Product Passport (DPP) effectively and pragmatically increase transparency instead of only adding bureaucratic burden.

Then, one must take into account important issues related to technological competitiveness and industrial policy. Semiconductors are bound to play an essential part towards attaining a green transition. In turn, the Green Deal's drive to create a more self-sufficient Europe could lead industries towards benefiting eventually from more cost-effective and climate friendly energy sources that are more independent from geopolitical shocks, enhancing competition in the long-term. But only if we invest now, from the onset, to build more sustainable fabs, and establish more circular supply chains.

**Have more questions about upcoming policy issues in global chip dynamics? You can contact our expert, Julia Christina Hess.*

Platform Oversight

Implementing the Digital Services Act: An orchestrated effort

The Digital Services Act (DSA) is Europe's attempt to regulate online platforms operating in the bloc. Having recently enacted this ambitious law, the 2024-2029 Commission mandate will be about ensuring it does not become a paper tiger, but rather gives people a better understanding of how platforms work and makes it easier for anyone to report content and challenge the decisions taken by tech companies.

As previously highlighted by *interface*, while the Commission plays a big role in enforcing the DSA, the national level cannot be overlooked for this crucial task. The bloc's 27 Digital Services Coordinators (DSCs) will check whether smaller platforms in their respective member states follow the new rules. They are the first point of contact not only for these businesses but also for citizens with their complaints and

researchers from academia and civil society with their data access requests. That is why it will be important to monitor how the DSCs manage to develop a fair and transparent system for the enquiries and possible complaints of citizens, researchers, industry representatives and civil society organisations.

It will be essential as well to see how these DSCs coordinate among each other and with the European Commission to prevent the perception among the public of bureaucratic opaqueness or –worse– regulatory capture, as previously experienced with the GDPR in the case of Ireland. Sure enough, over the past years the Irish data authority has sometimes been accused by some civil society organisations of perhaps being too lenient with big tech, leading to some erosion of trust among the public, and eventually some reproving court rulings. DSA enforcers would do well in learning from these events, and embrace transparency from the onset.

Preventing the abuse of power

One of the key goals of the DSA is to address more effectively the problems of disinformation and illegal content in Europe. Still, an important point of contention for the coming years will have to do with the fact that the DSA is actually agnostic when it comes to offering definitions to key terms. Throughout the law, there is no definition of disinformation.

While there are many possible long-term scenarios where this indeterminacy does not become a real problem, this circumstance still offers considerable space for the politicisation of key terms in national debates, or the risk of regulatory capture carried out by companies.

So far, these risks have not come to pass in a serious way, but there have been signs of companies ignoring the DSA and politicians pushing their own agenda with platform regulation. After all, this new EU mandate started on a year with active infringement procedures on the rule of law in some member states (e.g. Poland and Hungary). Similarly, the past years have been marked by many complaints about the curtailing of media freedoms in different European countries (Italy, Greece, Hungary, Slovakia, etc). All in all, it will be a delicate task for the EU to land in the middle of two extremes: between DSA politicization and noncompliance.

Action Points

Over this EU Mandate, it will be crucial to avoid abuse of power related to the DSA in two ways: Companies cannot be allowed to exploit their powerful positions to flout the new rules. Similarly, regulators and national governments cannot be allowed to take advantage of their powers to advance politically partisan interests over public consumer interests.

To that end, a meaningful and structured mechanism for communication between regulators and non-regulatory experts needs to be established. This could happen, for instance, at the European Board for Digital Services, which brings together the Commission and the DSCs.

Communicating clearly and openly about enforcement, yet without even the appearance of political meddling (as was the case for some of former Commissioner Breton's public letters to tech CEOs), will be important to earn and maintain consumers' trust in the DSA.

**Have more questions about upcoming policy issues in platform oversight? You can contact our expert, Julian Jaursch.*

Artificial Intelligence

Implementing the AI Act: The open question on how to best evaluate General Purpose AI

Over the past months, any discussion about Artificial Intelligence in Europe has been greatly influenced by the development of the AI Act. This new regulation is presented as a way to cast more clarity into a highly opaque sector of tech. But its implementation will require a lot of legwork. In this respect, the European Commission and its newly established AI Office now face the enormous responsibility of ensuring that General Purpose AI (GPAI) systems—such as the large language models powering ChatGPT— are effectively supervised and regulated.

However, a recent analysis of AI policy documents around the world has come to show that there are currently many important gaps between the governance aspirations outlined in the AI Act and the technical tools and expertise required for their realisation. A primary challenge lies in evaluating and mitigating risks from GPAI systems to ensure that there is compliance with the law and that European citizens are protected from potential harm.

For instance, how can we assess whether a GPAI model presents "systemic risk" to democratic processes, such as influencing electoral outcomes? Similarly, how can we trace the origin and authenticity of AI-generated models and content? And what measures can GPAI providers take to mitigate all these potential risks? To this date, these issues remain as open questions with no absolute answer.

In many ways, the field of GPAI still needs to further develop the science for its own

supervision and governance. Nevertheless, this open challenge should not deter the European Commission from doing its best to properly implement this regulation. Rather, the Commission should approach enforcement with the same ambition and creativity as when drafting the regulation; and by bringing as much feedback as possible into the process from AI researchers, civil society and the industry. By doing so, we can prevent the AI Act from becoming a law that is strong in principle but weak in enforcement, and instead ensure that AI technologies are developed and used in ways that are truly accountable to people's needs and societal values.

Fostering an AI talent pool in Europe: Towards innovation & inclusion

Over the coming years, it will be a global task to develop and align a series of international standards and norms for robust cooperation in AI development that is not only safe, but also open to healthy commercial competition between countries around the world.

Lately, there has been a lot of criticism over Europe's usually steadfast approach towards regulation. In this respect, many doomsayers predict that the AI Act's strong approach towards safety could kill innovation, and that if we want to survive in the global AI race we will need to liberalise further and invest on larger infrastructures and bigger resources.

However, in business imitation can only take you so far. In Europe, we might do well to think about smart, responsible and cost-effective ways towards innovation. Rather than compete with the United States and China by "burning" money to create large language models, we should find niches of specialisation where Europe has an advantage.

A key factor in achieving this goal lies in our approach to AI talent. Over the past months, *interface* has been looking at the origins of the AI workforce in Europe. Currently, the European Union heavily relies on international expertise, with an average of 30% of its AI professionals being foreign nationals. This dependence on third-country talent highlights both the global nature of AI development and the urgent need for Europe to nurture and retain its own AI workforce.

Every year, European universities witness the graduation of highly specialised people in the field of AI. These people come to study to Europe from different parts of the world. But then we lose this talent to the United States. This brain drain represents a serious challenge to everyone involved in enhancing AI research and boosting industry on the continent.

Moreover, as shown by a recent study, we're not fully tapping into the potential of

our own population. Globally, women comprise only 22% of AI talent, with even lower representation at senior levels – occupying less than 15% of senior executive roles in AI. This means that we're neglecting nearly half of the world's population when it comes to nurturing AI talent, a situation that urgently needs addressing.

Action Points

Just like with the Digital Services Act (DSA), implementing the AI Act will require the feedback of researchers, policymakers, civil society organisations and industry representatives. An important challenge for this regulation will be to develop and coherently adopt appropriate and widely shared methods of assessment for General Purpose AI. During this EU mandate, hiring for socio-technical expertise and building out governance capacity will be key missions for all the stakeholders involved in this task.

In this respect, focusing on AI talent development and retention is a strategic opportunity for both safety and innovation; and this aspect could be easily strengthened by policymakers in Europe by designing policies that make it easier for AI professionals to immigrate, creating programs that focus on retaining talent after university, and implementing initiatives to encourage women to enter and advance in AI careers are areas where governments traditionally have considerable influence.

By championing talent-focused policies, Europe can amplify its AI capabilities, turning brain drain into brain gain and unlocking a diverse pool of innovators poised to shape the future of AI.

**Have more questions about upcoming policy issues in Artificial Intelligence? You can contact our experts Siddhi Pal and Lisa Soder.*

Digital Rights, Surveillance and Democracy

Data brokers: A massive privacy challenge

Data brokers are companies or entities that collect, aggregate, and sell information obtained from various sources, such as social media, mobile apps, public records, and browsing behaviour. They often acquire this data without an individual's knowledge or explicit consent, compiling detailed profiles that can include sensitive and personally identifiable information, such as location history, purchasing habits, sexual orientation, health information, and even political or religious affiliations.

Data brokering is an important trend that merits far more scrutiny. It has become a multi-billion Euro industry with individual companies holding data on millions of individuals across Europe. Parts of the industry are responsible for some of the

worst privacy infringements in recent years. In Germany, for example, it is possible to access a live data set containing updated geolocation data of millions of users for the monthly fee of EUR 13.000. Worse still, and very much under the radar of current national and European policymakers in this space, European law enforcement bodies and intelligence agencies are also purchasing licenses from data brokers to access their data sets to enhance their own intelligence collection. They currently do so without a sufficient legal basis, let alone effective oversight.

The expansion of military surveillance in European NATO Member States

Another rising trend that policymakers should pay far more attention to is the expansion of military intelligence across Europe. The military forces of European NATO Member States are increasingly enhancing their digital surveillance capabilities to monitor online activities of soldiers and combatants, mobile phone networks, and other forms of digital communication deemed necessary for military preparedness and resilience.

There are two main drivers behind the push for more effective data collection in this sector. First, armed forces in Europe see the automation of warfare as a development in which they need to keep up to date to counter possible threats. This requires enormous amounts of high-quality data. Second, armed forces in Europe increasingly see the need to respond more effectively to asymmetric threats, such as disinformation campaigns. In this respect, they need to collect far more data as well, so as to better counter such threats.

As defence agencies are being further empowered and military intelligence is being prioritised at great speed, democracies must provide solid legal bases for these activities, and do far more to protect fundamental rights and basic freedoms in the process. Any state surveillance conduct must be paired with independent and effective oversight to ensure legitimacy and deter potential violations of basic rights and other forms of government malfeasance.

In this respect, a recent study from *interface* examined the surveillance activities of the German military (*Bundeswehr*). It concluded that the current German legal framework for military intelligence is woefully insufficient, for it fails to meet basic constitutional and European norms and standards for rights-based surveillance. Moreover, current oversight and accountability mechanisms for intelligence collection by the German military are also entirely inadequate. In its current state, the *Bundeswehr* has far less limitations for data collection than the German foreign intelligence agency, the BND. In addition, the military's unconstrained automatic data transfers to the BND are also a major concern, as they may lead to scenarios of

accountability evasion by means of collaboration.

More scrutiny on the build-up of European intelligence co-operation

It is often said that the EU does not really engage in intelligence collection of its own, as this remains a prerogative of Member States. But this is only partially true, given that some EU bodies, such as Europol and INTCEN, are increasingly engaged in their own use of publicly available data which may also include sensitive data purchased from data brokers. Just as in the case with national governments, this type of surveillance interferes with basic rights and is often done without enough legal protection and oversight. This should be remedied with the help of comprehensive reforms.

As it stands, Europe's future path in the realm of defence and security is in major flux. Current geopolitical tensions and the ensuing possibility of imminent threats are gradually leading policymakers around the bloc to substantially increase spending and adopt consequential new policies towards security. Over the coming years, this situation will probably translate into much closer coordination of intelligence sharing among European countries, between the EU and NATO, and possibly even towards the creation of a fully-fledged European Union agency for intelligence coordination.

This scenario has already been suggested in the report prepared for the European Commission by the former Finish President Sauli Niinistö. However, moving towards this path of heightened security and intelligence sharing will have enormous ramifications for EU Member States' obligations under domestic and international law. Should the EU move toward engaging in additional intelligence activities, it must also ensure to fully protect fundamental rights and honour democratic principles. It is therefore paramount that decisionmakers pay close attention to the democratic governance of any incoming measures aimed to boost intelligence sharing and cooperation among states in Europe.

Action Points

As the EU and its Member states are likely to significantly build up their current intelligence coordination capacities, policymakers would do well in observing how exactly the mandates of EU bodies evolve, and whether enough legal protections and oversight mechanisms are developed to counter potential executive overreach or the abuse of powers.

During this new EU Mandate, Member States also need to rapidly invest additional resources and, more importantly, supervisory technology to strengthen their oversight and accountability mechanisms in order to effectively control their civil and military intelligence services. This will increase the public trust and the legitimacy of any

government action towards increasing security and defence in Europe.

In addition, policymakers ought to keep a close eye on key legal developments currently taking place at a non-EU institution: the Council of Europe in Strasbourg. With the development of its Convention 108+, the Council of Europe offers the only international treaty to date that enshrines key guardrails and protections to the automatic processing of data by government entities without exempting the domains of national security and defence from this process.

It is high time for Convention 108+, signed by most EU Member States in recent years, to become fully ratified and transposed into national law. At present, and quite remarkably so, Denmark is the only EU Member State that has still neither signed nor ratified this important convention. The EU Commission should sign this landmark convention, too.

**Have more questions about upcoming policy issues in Digital Rights and Surveillance? You can contact our experts Thorsten Wetzling and Corbinian Ruckerbauer.*

Cybersecurity

The road to implementation: Finding your way through a complex framework

Over the past decade, the EU has become one of the main cybersecurity legislators in the world: From regulating cybersecurity aspects of *in vitro* diagnostic medical devices to creating dedicated cybersecurity-specific horizontal and sectoral Directives and Regulations. As a result, Member States now have to enforce the most comprehensive regulatory cybersecurity framework in the world. Without implementation, there will be no advancement in actual cybersecurity. With the added complexity, however, it is easy to lose track and difficult to maintain a comprehensive overview of efforts already taking place, and those underway.

Over the past months, *interface* has been mapping out the different stakeholders, policies and regulations. We have made this information available for everyone through a compendium that aims to help in navigating the EU Cybersecurity Policy Ecosystem. For governments, the private sector and other organizations alike, understanding the policy landscape will be the first step towards implementation which is the next crucial agenda item in the EU's approach towards a more cybersecure Union.

The Progress of Machine Learning: Making emerging technologies more secure

We live in a moment where the subject of Artificial Intelligence is continuously brought in the news cycle and policy debates, often as a bringer of much needed innovation to Europe. While the EU definitely needs a good AI policy to drive innovation, it also has a role to play to make sure that newly introduced technologies are safe and secure for use.

As far as emerging technologies go, the adoption of machine-learning enabled software applications is vastly increasing across European societies. It is therefore vital that governments and industry understand the attack surface and security implications of such emerging technologies and improve their security. While regulation does play a role in this endeavour it will be mainly the job of European companies and organizations developing and deploying such applications as well as governmental cybersecurity agencies to work towards secure and resilient use of emerging technologies. For that endeavour to work, governments have to shape an enable a good policy ecosystem.

The need to keep analysing ongoing foreign threats

At the start of this new EU mandate, Russia-enabled cyber campaigns continue to be a prevalent threat for European societies. However, a too singular focus on one threat actor tends to lead to costly blind spots. It is therefore of eminent importance for decisionmakers to better understand the threat landscape more broadly, so that they can design more effective European security systems and improve response mechanisms.

Within this perspective, any type of assessment about foreign threats should include a more comprehensive and diverse analysis of threat actors, including those from Iran, North Korea or the People's Republic of China (PRC), among others. In the past, *interface* provided a threat analysis for Germany with regard to PRC threat actors. One of the conclusions was that policy makers will require more research and analysis to make well informed decisions. This is not an isolated challenge for Germany but for the entire European Union. Therefore, the EU and its members states need to support and streamline relevant efforts across sectors.

Action Points

During this mandate, the EU and its Member States would do well in focusing on policy implementation before developing additional policies and regulations.

The EU should foster a policy ecosystem for secure development and deployment of machine-learning applications and its underlying hardware.

The EU's Member States should analyse a wider variety of threats and more actively share information and cooperate with other Member states.

**Have more questions about upcoming policy issues in cybersecurity? You can contact our experts Sven Herpig, Christina Rupp and Helene Pleil.*

About us

interface is a European think tank specialising in information technology and public policy. Our goal is to ensure that political decision-makers and the public have the expertise and ideas necessary to create policies and make decisions that put the public interest first. We are non-partisan and we are fully transparent about our funding and aims (EU Transparency Register No. 142903829084-58).

Author

Ernesto Oyarbide-Magaña
Lead PR & Outreach
eoyarbide@interface-eu.org
+49 308145037880

Imprint

interface – Tech analysis and policy ideas for Europe
(formerly Stiftung Neue Verantwortung)

W www.interface-eu.org
E info@interface-eu.org
T +49 (0) 30 81 45 03 78 80
F +49 (0) 30 81 45 03 78 97

interface – Tech analysis and policy ideas for Europe e.V.
Ebertstraße 2
D-10117 Berlin

Design by Make Studio
www.make.studio
Code by Convoy
www.convoyinteractive.com