TECH SUMMIT – 3rd edition

The rising technological influence in the next multipolar world

Turin, 10-11 April 2024

Report of the event

Dinner discussion: AI and Ethics

Artificial intelligence has clearly become a geopolitical battleground, as testified by recent developments in the US and the new European laws – the latter highlight how even the EU has realized the critical importance of this technology. While its very definition is still highly debated, in order to meet the current and coming challenges, Europe would need to invest in the development of a variety of capabilities in both the civilian and military domain. The war in Ukraine has made evident how the distinction between the two is often blurred and AI applications are countless.

The regulation of AI stems also from a fear that technology can take over from us. While this might seem a sci-fi scenario, in reality it tells a lot more about us than about AI itself. The combination of Artificial Intelligence and human recklessness could be utterly dangerous: what really matters in the end is the bad use of AI. In this regard, the war in Ukraine represents a watershed moment, as the first digital war: digital technologies are being used in the entirety of the war effort, from the collection and analysis of data to the improvement of combat capabilities. AI is indeed supporting kinetic warfare. This use brings us to a debate that has been ongoing for years among the military about the use of AI as of now, we were not highly aware of it uses and applications. Another clear example is the use of AI in the conflict between Israel and Hamas. For the first time in the last few years, the international community has found itself facing the crucial relationship between technological advancements and ethical repercussions. While there is a general understanding of AI being very reliable and relatively low-cost, at the same time it has questions the actual limitations in establishing targets. Thus, AI appears to have its vulnerabilities. Another major issue is the lack of accountability: since there are no general standards that could be applied universally, there is no chance to develop proper margins of cooperation.

A major issue about regulating AI is that it is essentially a technology that we do not control: we only see the outcomes, but the process remains largely non-transparent and obscure. This, in turn, makes AI quite unpredictable, making it difficult to fix when the outcomes of its processes are wrong. High vulnerability and the difficulty in controlling it make AI particularly dangerous. Also, the actual responsibilities of its misuse are hard to assess: non-intentional results cannot be easily attributed to either the machine or the users. Therefore, regulation is essential to prevent the worst outcomes; at the same time, international standards to allow for cooperation are complex. A major risk we are facing is that this regulatory gap would be filled by the military using it, as it is happening with the war. This would be highly problematic as the military domain does not respond to democratic principles and rules.

AI is also bringing about a revolution in human and social sciences, a revolution that would be uncontrolled without regulation. As some innovations like Neuralink show, our way of thinking would be more and more integrated with the machine, without the mediation that has existed before. With machines learning directly

With thanks to and for kindly supporting this initiative

how we think, the domain of education is also going to be affected, eliminating some of the previous boundaries. To tackle AI issues from schools to the military domain regulation is key. However, besides regulation, a better understanding of AI processes is needed, as we would be facing a hybrid system where machines coexist with humans. In this new world, machines would be progressively more capable and able to perform many human jobs, that is why we would need to adopt a more human approach, investing on the skills and capabilities that machines would not be able to replicate.

A key feature of AI developments is that they mostly depend on research and developments from private companies. This is a stark difference from the past, where most innovations entered the civilian and commercial domain after having been developed by the military. Some private companies are opting for more transparent open-source models, while others are more secretive, making effective regulation harder. In essence, AI is a statistical model working on very large databases: it is hard to see the need for regulation about the technology itself, what has to be tackled is the use. Countering the development of technologies is hardly a winning strategy, the more so with highly disruptive techs like AI; on the other hand, regulations have to set up the necessary adjustments, from boundaries to course corrections. Here, transparency from the companies involved in researching and developing AI models is necessary, as the public authorities cannot replicate the level of investments of big techs: thus, they need to be made aware of what is going on to address specific uses and potentially dangerous applications of AI. Regulating the use of technology should be interpreted as a crucial point even for industries themselves and not something counterproductive or limitative for the business. In this sense, the role of policy makers is essential: communicating properly the importance behind cooperation and even giving incentives becomes fundamental. Reaching the sensitivity of citizens is equally important too.

The inability of governments to compete with big tech firms is also behind the regulatory spree ongoing in Europe: as the EU lags behind investments in technologies, it is trying to develop a role as an international regulator. However, a purely legislative role on AI would hardly equip the EU with the capabilities needed to face the changing world: efforts should also go in the direction of investments. On par with this, the EU has to step up the game in terms of international cooperation, making sure that a high degree of interoperability can be maintained with like-minded partners. Here, the G7 and the OECD remain the best frameworks to develop joint standards, as values are shared.

Kick-off speech

Today, Europe is witnessing two conflicts on its doorstep – Ukraine and Gaza – that represent two peaks of conventional warfare, but its connectivity and supply chains are threatened by many other conflicts. In both those two wars, technology is proving a game changer on the battlefield: between Russia and Ukraine, war is being waged in the kinetic domain and in the cyber and space ones at the same time; in the Middle East instead, Israel relies heavily on satellite acquisition and surveillance, but the low threshold for dual-use tech has also helped Hamas improve its capabilities.

Technology is creating a new, more disruptive paradigm of warfare, transforming and expanding the traditional military domain thanks to the massive dissemination of digital technologies among the civilian population. This acts as an amplifier, exponentially magnifying the impact of malicious actions. Parallel to this, developments in AI are changing the structure of human control over machines, requiring new regulations that go beyond the possible use of the technology. This requires a systemic and cooperative approach at EU level, with the ability to share information and capabilities across borders. Europe should also maintain a competitive edge in the long term, replicating what has been done in the space domain. On new technologies,

With thanks to and for kindly supporting this initiative

no effective strategic autonomy is possible without close cooperation with allies, working together to tackle vulnerabilities and secure technological corridors – which are strategic tools and not just economic endeavors.

Technology is highly strategic; however, it shows patterns of fragility. The reasons behind it are various. First of all, the fight to obtain critical materials for their production. Secondly, the access of statistical data to improve and set AI applications. Thirdly, it can be easily subjected to attacks for espionage and industrial competition.

Panel I – Time is Ticking: The EU as a Multilateral Tech Actor

The current tech revolution resembles other times when new discoveries changed the world. In the late Middle Ages, it was Europe that emerged and gained an edge that later allowed it to impose a Western hegemony over the world. Now times are changing, and such a western technological edge cannot be taken for granted anymore. The same happens with the concept of peace: is not a given anymore. The continent is facing two intertwined challenges at the same time: one technological and one political. The need to reinforce European security and defense capabilities requires a strong focus on technological developments, integrating innovative solutions into the security domain. Here, AI and other innovations related to the broader security framework rather than just to defense, as most of them are dual-use. Therefore, we need to shift the thinking away from the current framework, expanding the set of expertise working on those topics.

There is indeed a risk of duplication if the EU and NATO proceed on different tracks, and they are already covering all aspects, ranging from the military sphere to civilian and economic security. This double dimension helps cooperation with the UK after Brexit, and in fact it is not by chance that the British are very active on DIANA. However, the limited resources available require merging all this into a single framework, one that can deal with the epochal challenge Europe faces. Here, a dedicated Defense Commissioner is necessary, but effective only if provided with adequate resources and planning capabilities. Cautiousness and audacity should go hand in hand, requiring a prudent but innovative leadership.

Since 2021, the EU is showing an understanding of the challenges in the technological domain: the EEAS has established a dedicated team and an office in San Francisco, close to US tech giants. At the same time, the EU appointed a tech envoy and set up a network for digital diplomacy. However, foreign ministries are ill-equipped to deal with the digital domain, while telecoms one lacks the foreign policy component. Thus, for Europe is essential to have digital diplomats to conduct digital diplomacy. EU delegations in Member States can help federating the work in the different countries, while also drawing from specific strengths that can be leveraged at the transatlantic level. The partnership with the US, through the TTC and other fora, is essential to European technology developments, but Europe has to reach out to other allies and regions. Japan is a key partner in the Indo-Pacific, while India is a more difficult actor to engage with, but Europe has to show the seriousness of the approach and accept that things move slowly. The digital component is also a growing element in the EU's engagement with Latin American countries and a pillar of the Global Gateway towards Africa. In the continent, the Commission is working on the regulatory field and on data centers, helping African countries build a digital single market and retain their data instead of having them stored in the US or China. The digital dimension is essential for the resilience of small states. Among the countries with whom the EU has managed to establish strong outer cooperation there are Kenya, Tanzania, Colombia, Nigeria and Brazil.

On the broader AI framework, Europe needs to maintain the engagement with the US and to prevent them from forging their own set of regulations: transatlantic convergence is essential here. China remains the elephant in the room, but polarization is weakening the regulatory process at the international level. For the

With thanks to and for kindly supporting this initiative

time being, it remains easier to work with like-minded partners rather than pursuing an UN-level agreement.

Despite the difficulties of multilateral approaches, the EU has to explore partnership opportunities beyond its traditional set of alliances, building coalitions with countries that share European concerns in the digital and technological spheres. ECFR's Multilateral Matchmaker is a useful tool that has been developed to analyse the landscape of middle and rising powers with whom the EU can forge ties. Technological developments and the ability to govern digital change feature high in the list of those countries' priorities and the EU has to stand out in a crowded field to be chosen. In this regard, the ability to create value for both sides is essential: Europe's engagement should enhance also the strategic autonomy of those partners rather than just the Union's one. At the same time, the EU has to remember that middle powers often wish to diversify their suppliers and to keep relations open with a diverse set of partners. On this, Europe is called to deliver and to develop strong bilateral ties instead of focusing only on the multilateral dimension. On the one side, the EU has to remain attractive with concrete initiatives and go for easy wins when they are possible. On the other hand, Europe has to be present to avoid those countries looking the other, rival powers like China. The first group of partners are those that share the European desire for a free, open, and accessible internet, preventing AI from restraining the freedom and spreading disinformation. The regulatory zeal of EU institutions, paired with its slow decision-making process, might annoy middle partners that push for their own regulatory approaches, not necessarily in line with European views.

Europe faces several challenges in promoting its open internet vision: this multi-stakeholder approach is often disliked by many actors in the global south, which perceive it as a based, western-led system. Also, the EU and other Western players need to overcome a lack of credibility in developing countries that is allowing other models to emerge.

PANEL 2: Surrounded by conflicts: EU-NATO defense and technology cooperation

It is no secret that the ideas behind security and defense, and how we perceive them, have been changing very quickly. A great role in shaping the current geopolitical context was the conflict in Ukraine. Among the most crucial aspects the international community had to face was the emergence and the wide use of disruptive technologies. As a matter of fact, these have been developing in an unprecedented way, and this contributes to how we perceive nowadays human security paradigms. For all these reasons, there is a strong need to continue preserving technological predominance. Europeans have seen how the Russian war against Ukraine has turbo-charged the adoption of technology into military operations. Whether the discourse lays around malicious attacks or not, international events cannot continue to be addressed as usual. A cultural change is needed.

For the first time, cutting-edged technology has been developing outside the governments. While tools such as internet and GPS devices were historically born within the military world, nowadays there is a huge number of private enterprises generating and working on technological research and elaboration of sensitive data.

Among NATO initiatives to tackle this situation, there is DIANA: it has been conceived as a unified approach for working on emerging disruptive technologies, from quantum to hypersonic. The three main steps are: acting on the strategies by a full technical understanding of devices; adopting new technologies and protecting discoveries. This programme funds early-medium staged developers coming from private businesses to present their ideas, to test their solutions at military facilities and to make them ready to enter the market. This initiative took its first steps in 2023.

Another crucial issue is the technological cooperation between the EU and the US in relationship to Russia and

With thanks to and for kindly supporting this initiative

Cina as global actors. This could be a source of alliance. Trump would be a huge challenge to transatlantic cooperation. With Biden's administration, there have been some commonalities in the general approach but still there are many regulatory issues to be solved. Collaboration between the EU and US will depend on the strategic cooperation between EU member states themselves. The Trade and Technology Council (TTC) will continue to be essential, especially for semiconductors.

Ukraine remains a critical junction for the EU. This, for certainly, can allow possibilities of change, however, there are defense dilemmas that need to be considered. First and foremost, NATO and EU cooperation. It would be necessary to avoid duplications. Security is an always changing need: it goes from crisis management to actual border defense. In the EU, the market logic has always been more important than the security one. In this sense, there are two main obstacles: the diverse threat perceptions between different areas of Europe and the actual differences in regulatory approaches. These two elements make it difficult to intervene in joint programmes and still leave most issues to be tackled at national levels.

A second feature within the development of a NATO-European defense doctrine is the political strategic dimension. Here, there are two main blocks: economic constraints and public opinion. While the former reflect extreme challenges, especially for countries that do not have big margins for changing their economic structures or to redirect resources towards defense, the latter is a double-sided medal: the more the threat is clear, the more the public opinion is ready to face and react on a certain situation by enhancing military expenditures, however, the more the most of the possible military interventions, the more people will feel detached from the cause.

A third aspect is the shift between foreign policy and national security paradigms. Crisis management and direct experiences have taught the system how to react in certain situations. Within Europe itself, there have been different trajectories. In Italy, for example, there has been a clear consolidation of power for crisis management. In terms of armaments, artillery and ammunitions were not so considered in the past and now we have seen the consequences. This was particularly given by economic constraints.

Finally, what has emerged in recent years is also a general dimishing in the role of national Parliaments for security-related decisions. Rather than addressing public opinion, everything has been working within closed-doors meetings.

PANEL 3: Connectivity wars: challenges and opportunities of new technological corridors

In an increasingly fragmented world, connectivity infrastructures, intended as physical and geopolitical spheres, play a key role. The EU is emerging as an ambitious and strong actor in fostering connectivity, pushing for a bigger engagement toward economic corridors in a technological sense. When people think about corridors, sometimes they connect them to transportation and infrastructural systems only. However, connectivity infrastructures are now, more than ever, security issues, where the technological dimension is paramount.

Talking about connectivity today means looking at the reconfiguration of the world order in concrete terms. China has understood the potentials and the needs of modern infrastructures – also in developing countries – before anybody else, observing how connectivity creates long-term dependencies. For this reason, this element is not neutral, but it comes with rules, regulations, and a crucial governance component. So far, the EU has focused a lot on protection towards the issue, assuming a defensive and compromise approach with the implementation of a market logic and investment regulatory instruments. However, small things have been done on proactiveness and agency. In the US-China geopolitical competition, EU's posture should be more ambitious. The EU has incredible financial and technical capabilities, but it still cannot use them in a

With thanks to and for kindly supporting this initiative

decisive and strategic way. For this, the new EU Commission should call for a more competitive Europe, implementing a proper division of connectivity-related tasks between DGs to better understand and address the next challenges in this field.

Improving in connectivity could be achieved by the EU considering two main aspects: first, a more strategic approach to bigger scales, going beyond the small dimensions, and putting EU private sector at the centre. Second, working on speed, stepping into the logic that, unless we can deliver quickly, we can forget results. With a competitive China, the India-Middle East-Europe Corridor (IMEC) emerges as a good example of these two pillars. It is therefore necessary to mobilise the private sector in both aspects, in line with EU's ambitions and needs. A quick and stronger involvement of private capital would be functional to complement public budgets and investments, creating a blended finance mechanism approach that could reduce financial risks and, at the same, envisage fiscal-economic incentives to tech investments. Worrying figures, such as climate-related ones, should be considered too, to adopt mitigation solutions in time. To stimulate a stable and business-friendly development environment, legal and regulatory barriers that hinder the mobilisation of private investments should also be overcome.

Strategic infrastructure and investment initiatives are also among the core pillars of the G7 policy agenda, of which Italy holds the presidency this year. The Partnership for Global Infrastructures and Investments (PGII) the G7 countries are working on, mobilising 600 billion dollars by 2027, needs to move forward and speed up within a strongly competitive arena. The Italian G7 presidency agreed that the banks can establish an expert group on PGII and development finance institutions, involving all G7 countries and the EU investment bank. This can be a good starting point, together with the strategy, proposed by Cassa Depositi e Prestiti, to set a more permanent mechanism for PGII. More in general, it should be observed whether different strategic interests between the US and EU can be reassessed in the PGII – so far, mainly US-led processes – asking ourselves if the PGII provides a viable framework for embracing the EU strategic initiatives (GG and Mattei plan) or it is something more related to the US.

The Global Gateway for Africa has been another key topic during the discussion. At political level, there is an understanding of what needs to be done with partner countries. African countries have long called for a focus on investments rather than development, and the Global Gateway definitely meets this demand. However, this should not be translated into applying developing policies towards these countries. To be effective in the Global South, a shift from development thinking to industrial dialogue is necessary. As these countries are interested in moving up their value chains and building resilience, this mutual approach could be useful for their strategic economy.

There is a huge infrastructure gap in connectivity in Africa, with low tech rates and unequal coverage at the geographical level. However, China seems to have filled this gap, increasing the sense for Europeans to play a counteracting role rather than a proactive one. A new era for the EU in terms of international cooperation is therefore needed, using the "learning by doing" logic more proactively. At a policy level, the Global Gateway should be embedded into a wider political dialogue with developing partners by identifying key countries and ensuring good coordination among the Commission DGs which have dedicated budgets for the project implementation. Looking at infrastructural development, the emphasis must be placed on mapping and studying in-depth local ecosystems, so as not to build infrastructures destined to become white elephants. On implementation, the EU still rely on a stakeholder-based approach not properly involving the private sector. This logic should be reformed and supported by more flexible instruments and private capital.

In this context of connectivity, some considerations should be made about submarine cables, part of the physical infrastructure compartment that is often discussed, but without having a real idea of how it works. In a context where the longest undersea cable has reached 20000 km, connecting Asia to the Mediterranean, the

With thanks to and for kindly supporting this initiative

market has changed considerably with technology, implementing fibre optics to date. At the same time, the cable industry has moved towards a more limited number of entrepreneurs working on the same cable system, in a more competitive logic.

Despite this, Europe remains at the centre of the world for what concerns digital infrastructure. Seven out of the ten of the largest companies in the world are located in Europe. Traffic flows from east to west and vice versa pass through Europe, putting the continent at the core of the digital ecosystem. The market is changing, and the wars in Ukraine and Gaza made clear about the importance of digital infrastructure, resilience, and robustness of systems. For this reason, building a more interconnected and resilient digital ecosystem is now the main goal, moving from a global network seeking answers to digital demands to a more resilient one. The key challenge is shifting from the demand to a broader diversification with the final aim of reaching resiliency. This needs a strategy to be defined in industrial, legal, and diplomatic ways. Europeans, and Italians in particular, could take advantage of their diplomatic abilities, leveraging on the Global Gateway and the Mattei Plan. Both projects are about connectivity and Italy should capitalise on its political and geographical position to emerge as a leading EU country, in the logic – and opportunity – of bringing the Mediterranean at the geopolitical centre of Europe and further beyond.

Conclusions

The third edition of the Tech Summit highlighted the importance of technology and the need to preserve its multiple facets: from boosting commercial and cyber networks to investing on research and development; from strengthening defense-related tech with a European perspective to regulating private companies' actions. At the root of the debates there was a raising awareness on the existence of profound questions related to ethical aspects, particularly concerning Artificial Intelligence but not only. Europe has found itself metabolizing the emergence of new security paradigms in which, for the first time, it may not be playing the lead role. There are still many points to work on but two aspects, in particular, brought together participants' consensus: the emergence of new players in the international landscape and the need to establish dialogue between the public and private sectors to eventually achieve, with combined forces, stronger confidence in foreign policy and more secured economic competitiveness in the international markets.

With thanks to and for kindly supporting this initiative