ESPAS European Strategy and Policy Analysis System

ESPAS Foresight Papers

Artificial intelligence, quantum and cybersecurity by 2040: Are we ready for the disruption?

AN INTER-INSTITUTIONAL EU PROJECT

AN INTER-INSTITUTIONAL EU PROJECT

European Parliament

Council
of the European Union

European Commission

European Union
EXTERNAL ACTION

European External
Action Service

CURIA RATIONUM

EUROPEAN COURT
OF AUDITORS

European Court
of Auditors

European Economic
and Social Committee

European Economic
and Social Committee

European Committee
of the Regions

European Committee
of the Regions

European
Investment Bank

European Investment
Bank

euiss

European Union
Institute
for Security studies

The 2024 ESPAS Global Trends Report found that artificial intelligence could be the biggest technological disruptor for Europe since the Second World War.

SUMMARY

Leading in the development and application of artificial intelligence (AI), quantum and cybersecurity, harnessing first mover advantage, securing resilience, and setting global standards will all play a key role in the international power game. These three technologies are critical, due to their potential to increase productivity and competitiveness, to drive economic growth, and accelerate research, innovation and technological progress. They will also have a huge impact on the way we live, work and function as a society, and on the future of democracy. They are also of growing importance for security, as those controlling the most advanced technologies and supply chains can concentrate power on an unprecedented scale, which will have an impact on the economic security and freedom to act of others.[1]

In the coming years, the global technological race between the US and China will become even fiercer, with the EU likely **consolidating** its leading position and new players entering the stage. This contest will be underpinned by massive investments in new technologies and their applications. We will see competition between different approaches, combined with efforts to ensure the rolling out of each party's own models and solutions to the entire world. As a result, efforts to effectively address risks related to the advancement and uptake of AI and quantum could become more urgent.

Strong synergies and opportunities, but also new risks, will develop at the intersections of the three domains. Combining quantum technologies and AI will open new opportunities, offering much more powerful AI models able to perform tasks AI and quantum machines alone would not be able to do. But it will also enable the development of highly accurate sensors and sensor systems, or advanced brain-machine interfaces with applications in medicine or learning. Progress in cybersecurity will probably enable the development of safe, AI-powered conversational and multimodal human-machine interfaces. Finally, quantum-assisted security and quantum-safe architecture will help strengthen the cybersecurity of information systems and networks.

The risks include the existential one for humanity, of losing control over technology once the capacities of AI exceed the capacities of the brightest human beings, and the risk that the dominant AI models do not comply with EU values and the interests of our societies. Key challenges relate to ensuring **democratic control** over decisions and policy-making

processes where AI will play an increasing role, **managing the risks** of over-confidence in such tools, as well as developing the necessary **skills and resilience**. The EU will also have to cope with increasing risks related to the use of these technologies for criminal or other malicious purposes such as warfare, cybersecurity risks, and ethical challenges related to certain applications such as human enhancement with AI.

The EU will need to address several **strategic issues**. These range from developing the necessary skills and keeping talent in Europe, to mobilising investment, especially European risk capital, as well as rapid improvement of the 'enabling environment', as recommended in the Draghi[2] and Letta[3] reports. Other issues include how to ensure EU strategic autonomy, maintaining a regulatory framework capable of shaping these rapidly developing technologies, adapting the management and risk assessment frameworks, and ensuring timely transition to post-quantum cybersecurity. Finally, taking a leading role and mobilising international partners, to support the European human-centric and values-based approaches to AI development will also be important.

Introduction

In view of the upcoming changes AI, quantum and cybersecurity will bring, this foresight paper explores existing and potential future trends in the development of these three domains over the coming 15 years, as well as related opportunities, challenges and risks – globally and for the EU. As all three areas are undergoing such rapid development, with a significant dose of unpredictability, the 2040 perspective of this paper is quite distant, and many foresight projections in this paper apply only to the next couple of years. Moreover, several milestones have timelines which are difficult to define. The paper analyses general trends and the likely advances of the global tech leaders, with a focus on AI, quantum and related cybersecurity questions, and the implications for Europe and the world. It focuses on possible future opportunities for Europe, as well as challenges and risks at the intersections of the three areas. The final chapter presents the key strategic choices that EU policy- and decision-makers will face in the coming years.

The preparation of this paper has been mandated by the ESPAS Steering Group, and involved experts from the European Commission (SG, DG JRC, DG CNECT and DG RTD), the European Parliament and the European Court of Auditors as well as external experts. The preparation process included literature analysis, a foresight workshop with ESPAS institutions and external experts, as well as interviews with high-level experts. The team preparing the paper also posed questions to AI models managed by DG JRC in the European Commission.

1. The rise of the new technological order – Key trends to watch

The development of AI, quantum and cybersecurity in the years to come will be driven by a quest for increased efficiency, competitiveness and financial gain, underpinned by other technological advances in both hardware and software. All three domains will play a critical role in security, resilience, and strategic autonomy in the broad sense.

1.1. AI development is accelerating

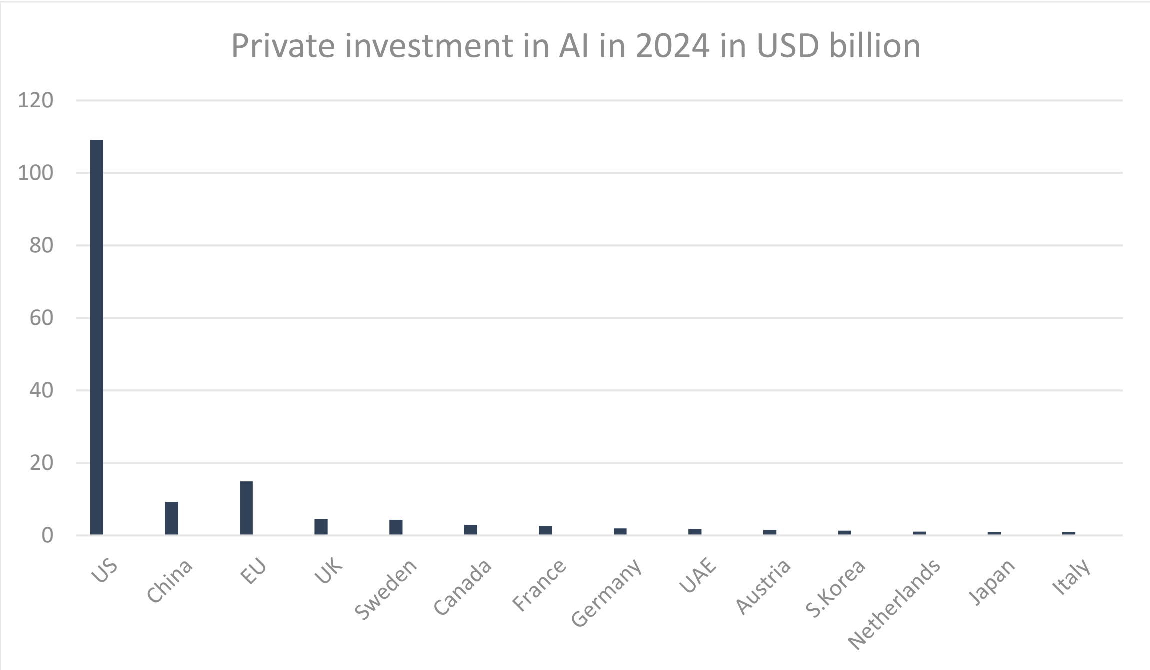
AI is advancing at an unprecedented pace, offering new capabilities that will transform the public sector, how industries work and the ways economic growth is generated, and ultimately how all these things will impact on society as a whole. The rapid **evolution of Generative AI**, with increasingly powerful models demonstrating increasingly strong performance in tasks such as programming, abstract and scientific reasoning[4] is fuelling momentum towards the development of **Artificial General Intelligence (AGI)**. AGI would possess the ability to perform any complex intellectual task a human can do, namely understanding, reflection, independent learning and the application in various contexts of the knowledge it has. Depending on strategic choices made by policy-makers and scientific advances, AGI could then potentially evolve into **Artificial Superintelligence (ASI)**, with capacity exceeding that of the most brilliant minds. Timelines for the arrival of AGI and ASI are uncertain, with **some experts asserting that AGI could be here within 2-3 years,**[5] **while others suggest it will be a decade from now or even later**.

In parallel, **specialised AI** will be further developed and rolled out for specific applications, from systems supporting doctors in the analysis and interpretation of medical data, the discovery of medical treatments, and helping with management and planning, to systems supporting the optimisation of industrial processes, the management of transport and public services in cities, and the detection of crime.

In the coming years, we will see further rapid development of **agentic AI** – that not only generates content, but also executes tasks it has been mandated and trained to do. AI agents will conduct end-to-end processes, replacing the human workforce in many cases, and augmenting their work by performing tasks faster, more efficiently and better. They are already performing many coding tasks, as well as frequently ensuring the first line of customer service and support. As a result, the workforce in businesses and organisations will increasingly become hybrid – human and agentic, with humans performing the oversight roles[6] – and entire organisations' operating models and business management will change profoundly.

Depending on its design and application, **AI can both enhance human performance and efficiency, and act as a substitute for human workers**, starting with less complex jobs. The latter phenomenon is already detectable in the labour market, with fewer offers for several entry-level jobs.[7] **AI can help mitigate demographic challenges for the labour market in Europe** and also enhance the efficiency of human employees. The direction this development takes in Europe will depend on political choices.

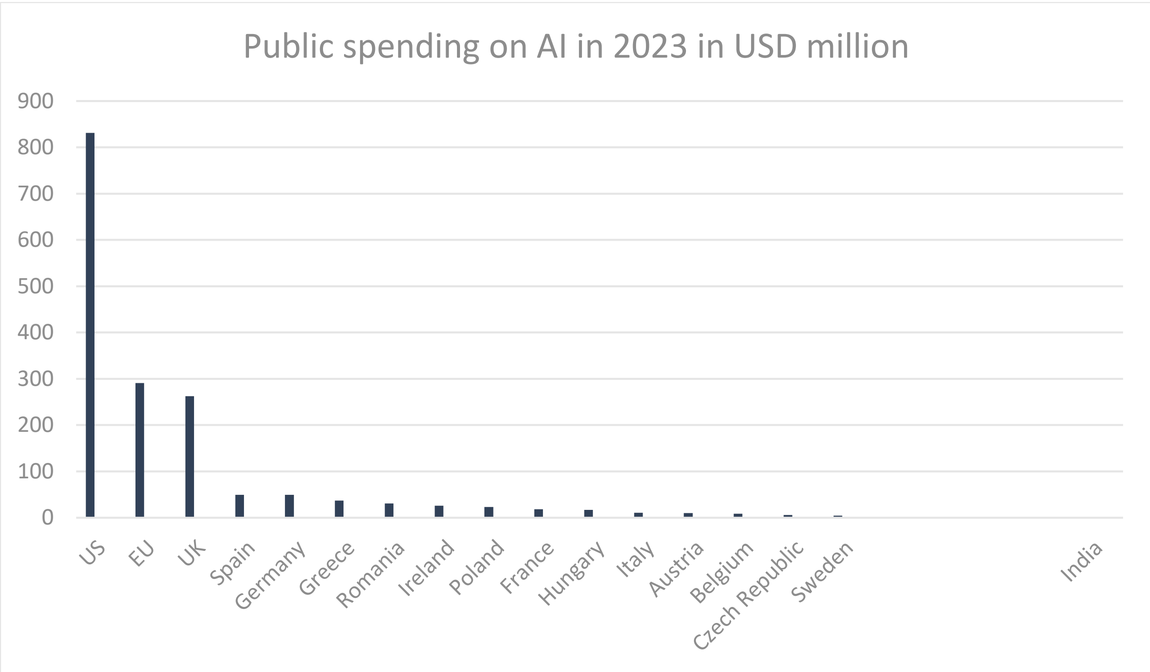
Chart 1. Private investment in AI in 2024 in USD billion



Source: 'Stanford AI Index 2025' report.

The AI race, in particular the progress of Large Language Models (LLMs) will be facilitated by the further rapid development of data centres and clusters of data centres, where hundreds of thousands of chips work in a synchronised way to train and fine-tune AI models, and by **inference** – use of AI models for specific tasks. Global expenditure on data centres, estimated in 2025 at USD 475 billion (up 42 % as compared to the previous year) are expected to grow to reach almost USD 3 trillion by 2029, with more than 50 % coming from investors and developers.[8] Other estimates foresee that, to keep up with global demand for AI, by 2030 investment in data centres of up to USD 5.2 trillion[9] or even USD 6.7 trillion[10] will be required. In 2025, global data centre capacity reached 122 GW, of which almost three-quarters is held by the US (54 GW) and China (32 GW). The EU, with capacity of 12 GW, currently lags behind. Other major players include Japan, South Korea and India.[11] Critics of rapid data centre capacity development in the US driving this race point out the risks of over-capacity if AI does not roll out as quickly as expected, or if Chinese competition offers more cost-efficient access to AI capacity. Higher losses could occur if real costs exceed estimates, and technology ages quicker than expected. The European Central Bank (ECB) and some other central banks warn of the possibility of market correction in AI and other tech companies. There are also growing concerns related to the environmental and social impacts of increased water and energy use to operate the rapidly expanding AI infrastructure.[12]

Chart 2. Public spending on AI in 2023 in USD million (contracts)



Source: 'Stanford AI Index 2025' report.

AI advances will likely **facilitate the further development of brain-computer interfaces**, and extending their application from medical use, where they started, to consumer and military applications. Medical interfaces will benefit many people otherwise unable to move or communicate. Other applications (several already in test phase) aim to augment human mental and physical capabilities or experience, raising many ethical and security concerns, including cybersecurity. The potential uses of such consumer applications range from learning and marketing to immersive gaming experiences or even, in a dystopic scenario, control of employees and their productivity. Military applications could enable the possibility of enhancing training and soldiers' performance, or the remote control of military equipment.[13]

AI will also drive development and deployment of **autonomous robots**, including collaborative and interactive robots. This area is dominated by China, which continues to install more robots than the rest of the world combined.[4]

If current trends continue, **AI will be integrated in all aspects of the economy, society and governance within the next 15 years**. AI technology is expected to become highly autonomous, requiring less and less input and direction from people. Broad use **of AI will likely accelerate research and scientific discovery**,[14, 15] and drive efficiency and growth in many areas of the economy, including manufacturing and services, and public services such as health or administration.

Estimates of the **additional economic growth to be created with generative AI** in the next decade vary substantially depending on the source – from USD 6.1 to 7.9 trillion (5.4-7 % of global GDP) annually (McKinsey) for the global economy,[16] to more moderate estimates of just 1-1.8 % in annual GDP growth over the next 10 years for the US.[17] The moderate estimates are explained by limited productivity growth (0.7 %) linked to higher costs related to applying AI to harder-to-learn tasks, as compared to the economic benefits in the near and medium term. Besides the uncertainty of future economic growth, we can also anticipate risks related to governance and security, including in respect of data and intellectual property loss, or security breaches. Another mechanism leading to the moderate impact of AI on economic growth is its expected effect in exacerbating inequalities.[18]

1.2. Dynamic development of quantum technology

Quantum technology is still at a relatively early stage of development and includes 3 key areas: quantum computing and simulation, quantum communication and quantum sensors. In the years to come it is expected to develop rapidly and become the **key area of the global tech race**, due to its information security implications and expected quantum advantage for those in the lead.

Quantum computing represents a paradigm shift in computer power, enabling faster solutions to certain important computational problems and solutions to some that are currently intractable. Quantum computers are developed using various approaches to create high quality qubits, protected from external noise to reduce error rates and aimed at advances in error correction. Currently, it is impossible to predict which approach may prevail in future. **Scaling up using scalable control stacks** (modular, highly integrated systems including hardware and software to control and read increasing numbers of qubits) **and**

developing quantum computers with an increasing number of logical qubits remains a key challenge. Up to now, even the most capable quantum computers have only 1 200 physical qubits, most of which would be required for error correction (computational operations are done on logical qubits). Leaders are Atom Computing and IBM Heron. It is expected that, by 2030, a 1 000 fully error-corrected logical qubit quantum computer can be built. Due to the limitations of quantum computers' computing capacity in the near future, **hybrid quantum and conventional computers will gain ground, including hybrid supercomputers** where quantum computers are integrated with conventional high-performance computers. Hybrid supercomputers require the resolution of integration and hardware-related challenges but are expected to increase computing capabilities (speed and processing power) substantially compared to classical and quantum computers.

It is likely that, by 2040-2045, we will have a universal quantum computer, and some expect that quantum computers could surpass the capability of conventional computers even five years from now.[19] Still, large scale commercialisation of quantum computing is expected no sooner than a decade from now.[20]

Quantum computing (**general and specialised**) is expected to accelerate the progress of research and scientific discovery and to help with optimisation of different processes, as well as resolving problems in a wide range of areas. However, quantum computers will not ultimately replace conventional computers in all applications.

Quantum (resilient) communications is a critical quantum technology developed to ensure secure information transfer and distributed quantum computing. The latter allows to connect, in a secure way, multiple quantum devices in various locations to work as a single, more powerful computational system. **Secure information transfer** anticipates that quantum computers will allow the breaking of conventional encryption methods, and accessing and exploiting encrypted information collected previously. It focuses on two tracks. First, developing and deploying **post-quantum cryptography (PQC)** is the default path for broad systems that must be deployed with crypto-agility and lifecycle management. Second, **quantum key distribution (QKD), and quantum random number generation (QRNG)**, would be applied for specific, high assurance user cases with distinct trust and infrastructure requirements. PQC is software-based, and cheaper to deploy, using advanced cryptographic algorithms while QKD requires special hardware and is therefore more expensive, but at the same time less vulnerable to purely mathematical methods of decryption and allows for the detection of information leakage. Secure communication is of critical importance in security and defence, public administration and business, and in general, for strategic autonomy and the resilience of states. In the coming years, **development and deployment of quantum-computing resilient information systems will be given high priority**, including by public administrations.

Quantum sensing allows for high-precision measurements of various characteristics, such as temperature, pressure, magnetic fields and electric fields, which would not be possible using conventional methods. Quantum sensors are already used in medicine (in magnetic resonance scanners), and for research science and defence. Atomic clocks are used for navigation, in defence and for financial trading, and as fundamental standards. Further miniaturisation, and addressing challenges related to environmental interference and calibration, will allow quantum and hybrid (quantum-conventional) sensors to be widely deployed in many domains, including navigation, chemical and material analysis, intelligence, defence, and geographical exploration.[21]

Progress in the uptake of quantum will depend on its accessibility, including costs. The global quantum technologies market (infrastructure, hardware, software, services) is at an early stage but is expected to grow strongly in the coming years and reach a value between USD 46 and 97 billion by 2035, and between USD 106 billion[22] and USD 198 billion by 2040. The greatest share is expected to remain with quantum computing – at 66 % of the total, followed by quantum communication at 18 % and quantum sensing with 16 %.[23]

1.3. Cybersecurity even more critically important

With rapid **technological advances, in particular increasingly capable generative AI, the race to develop quantum computing, and increasing technological reliance of our economy, businesses, politics and functioning of democratic institutions, governments and public services, communication as well as individuals, cybersecurity will play an increasingly central role in the years to come**. Mounting international tensions and the intensification of cyber-attacks associated with state actors will make cybersecurity even more important.

According to ENISA's (EU Agency for Cybersecurity) recent Threat Landscape report,[24] state-aligned offensive cyber activity against the EU in 2024/2025 was associated mostly with Russia (32 %), China (24 %) and North Korea (12 %), followed by Iran and India. Third-party targeting covers a wide spectrum – from EU institutions and Member States' public administrations to digital infrastructure, industry, and civil society. It is related to strategic political interests (e.g. related to the Russian war against Ukraine) as well as strategic data collection, financial services, technology and other intellectual property theft. On top of this, there is cybercriminal activity, increasingly leveraging AI (see the chapter on risks and challenges). ENISA anticipates that, looking to the future, cyberthreat activity is likely to intensify further in three dimensions: convergence, automation and industrialisation.[24]

Due to its strategic importance, critical infrastructure will probably face increasing cybersecurity risks in the coming years. These could be exacerbated by the increasing digitalisation and interconnection of infrastructure in energy, healthcare, transport, public services, and payments, with the presence of legacy technologies posing an additional risk. The roll-out of the Internet of Things in the economy will open new vulnerabilities to cyber-attacks, exploiting weaknesses in systems. Cybersecurity will play an increasingly important role in preventing third-party intelligence operations aimed at information interception, interference and disinformation or misinformation from succeeding. Global spending on cybersecurity is expected to increase in 2025 by 15 %,[25] and continue growing to reach USD 377 billion in 2028. The United States and western Europe will continue to account for more than 70 % of global cybersecurity spending in 2025.[26]

2. The key role of AI, quantum and cybersecurity in the global power game. Can the EU remain a frontrunner?

Securing a leading role in the development of AI, quantum and cybersecurity, and their application to strengthen Europe's innovation, competitiveness, security and people's well-being will be among the decisive factors determining the future positioning of the EU on the global scene and in setting the future world order. The importance of the three domains extends, however, far beyond increasing the productivity and competitiveness of economies, accelerating research and scientific discovery, technological and human progress. Those controlling the most advanced technologies and their supply chains (model developers, chip suppliers, data centre owners) can concentrate power on an unprecedented scale. This applies to both states and leading businesses. Contingent on who leads the technological race, this may put at risk the economic security and sovereignty of others.[1] Both AI and quantum are dual use technologies, and their military applications will likely lead to advantages in defence and security capabilities. They can also enhance the capacity of state actors to carry out disinformation and other hybrid and influence operations. Other impacts will probably see the creation of new dependencies in countries using these technologies and a deepening of the digital divide among countries.

All of the above explains the acceleration of investment in these domains by the US, China, and the European Union, and other key players such as Japan and UK.

2.1. Strong on research and specialised AI, catching up on general use AI

In 2025, close to 95 % of commercially available AI capacity is to be found in the US or China, with the US dominating with 85 % of global capacity.[27] The US hosts 75 % of AI supercomputers, with China way behind in second place with 15 %. Traditional supercomputing powers such as the UK, Germany and Japan have a significantly smaller share in AI supercomputing.[28] Planned investments in AI capacity will gradually change this picture – next to the US, the Gulf countries (UAE, Saudi Arabia) plan construction of huge data centres, followed by the EU, South Korea and India. Among the leading global AI tech companies, none are European at this point, and European start-ups currently need to look for US funding or move to the US to scale up.[9] This imbalance has already led to several takeovers by US competitors. The EU is strong in AI research and specialised AI, focusing on specific applications and operating business-2-business models building on a strong industrial base with several global companies such as SAP and Siemens. However, the EU remains dependent on US suppliers of chips, and does not have full autonomy in all elements of the supply chain, lagging behind the US and China as regards data centres and cloud capacity.

The **EU's AI policy and regulatory framework** aims at making the EU a world-class leader and a hub for AI, ensuring it is human-centric and trustworthy, compliant with EU democratic values and in line with OECD guidelines. This includes the EU's AI Act[29] of 2024, the EU's AI Continent Action Plan[30] of April 2025, the Apply AI Strategy,[31] the AI in Science Strategy[32] of October 2025, and the upcoming EU Cloud & AI Development Act. As a result, in 2025-2026, at least 15 AI factories and gigafactories will be operational, prioritising access to AI for European start-ups and SMEs. Private investment is stimulated by the Invest AI facility of the value of EUR 200 billion. Achieving the ambitious goal of ensuring a leading global role for the EU in AI in the long term is dependent on rapid progress on the Competitiveness Compass[33] developed following the recommendations of the

Draghi and Letta reports. In particular, it will require opening access to European risk capital and the ability in the medium term to secure strategic autonomy for the entire supply chain, all in close partnership with European businesses.

The **US government's top priority for the development of AI and related infrastructure is to keep the US ahead of China in the AI race, ensure a competitive advantage for US companies, and support national security**. It is supported by massive public and private investment. In January 2025, the new US administration launched a USD 500 billion 'Stargate' programme for development of AI infrastructure, which was followed by announcements of other investments (including USD 90 billion in AI and related energy infrastructure in Pennsylvania). The US AI Action Plan, unveiled in July 2025 includes a set of initiatives and policy recommendations aimed at safeguarding the US as a global leader[34] and focused on accelerating innovation, developing American AI infrastructure, skills and making US hardware and software the standard for AI developments globally. **Upholding free speech has been set as the condition for frontier models to participate in US government procurement, as well as in the use of AI by private large-scale platforms and gatekeepers.** Other actions include streamlining permitting processes and partnering with AI companies, as well as limiting regulations and removing those considered as excessive. However, repealing earlier laws on AI safety on theat federal level raises concerns that efforts to keep AI safe will be less effective and makes it more difficult to keep tech companies accountable.[35] The US also envisages the creation of AI export packages including AI models (both hardware and software) that will be made available to US partner countries. To limit advances by China, the US applies export controls on the most advanced chips. **The US Silicon Valley-driven AI development model is based on large closed-source language models, trained on huge data sets.**

China's AI Development Plans are given the highest priority in the country's technological development programme. China leverages open-source technologies to push domestic innovation, integrate AI in all areas of the economy and reduce Beijing's dependence on the West. US restrictions on exports of the most advanced AI chips to China accelerated efforts to develop home-grown technology to produce advanced chips. China also aims to become the leading provider of digital infrastructure for the developing world, through initiatives such as the Digital Silk Road Initiative.[36] Shortly after the launch of the US AI Action Plan, China announced its own Action Plan for Global AI Governance, building on the 2023 Global AI Governance Initiative.[37] This underscores China's aim to shape global AI governance, and includes actions such as dialogues to reach international consensus on AI standards and norms in key areas (security, ethics, industrial applications, inclusiveness, interoperability and elimination of algorithmic bias). The plan contains measures to support countries in the 'Global South' through technology transfer, digital infrastructure development (intelligent computing power, data centres, next generation networks, clean electricity) and capacity-building. This would contribute to the promotion of unified computing power standards and standards for energy and water efficiency. The plan prioritises open-source AI development and cross-border collaboration. China also proposed establishing a global AI cooperation organisation based in Shanghai, to ensure international cooperation on AI development and regulation and 'support' the UN.[38]

Unlike the US, **China's AI development strategy relies on developing smaller-scale models fed by more limited data sets ('small data, big task' approach)** and is more flexible. The focus is put on such qualities as resourcefulness in novel situations, social and physical intuition as well as making a link between cause and effect.[39] This approach gives Chinese technology an advantage in developing countries, due to its adaptability to local needs and lower costs.

In the years to come, AI will remain a field of fierce competition for technological primacy between the US and China, with the EU taking steps to remain in the race, while other players enter the arena. It will become an important tool for the projection of soft power across the world and the basis for new dependencies. Open-source models, so far mainly Chinese, even though less powerful, will approach the closed models in their levels of performance, while offering users the possibility to adapt the models to their needs and generally requiring less computing power to train. These features result in lower costs and higher accessibility, giving the open-source models a comparative advantage in the developing world, and could lead to entrenching Chinese technology in global AI stacks, the digital infrastructure underlying AI, including models, chips, and data centres. Chinese AI strategy could also capitalise on a generally more positive attitude in developing countries towards AI and the benefits it can bring. As long as there are no alternatives, Chinese open AI models will likely become the primary choice for countries that want to take advantage of AI technology but do not possess sufficient financial or computational resources to build their own models from scratch. Apparently, closed models as offered by US providers do not give sufficient flexibility to customise them for use for local applications.[36]

The development and uptake of AI and quantum globally, and in Europe, will to a great extent depend on the **existence of an enabling environment**. This includes the availability of skilled employees, investment in research, access to funding including risk capital to enable new start-ups to navigate successfully through the early stages of development, then scale up and grow, and AI infrastructure. Support for launching start-ups, and collaboration between the research community and business, will also matter, especially in Europe where they remain less developed than in the US. Equally important will be access to affordable energy and infrastructure, including data centres and, in Europe, eliminating obstacles related to the incomplete internal market which currently makes cooperation across borders and scaling up more difficult.

2.2. Frontrunner in the quantum race

The EU is one of the global frontrunners in the development of quantum technologies. Up to 2025, total EU public investment in quantum (EU budget and Member States) reached EUR 11 billion[40] while those of China were estimated at around USD 15 billion, Japan USD 7.91 billion and the US USD 7.67 billion.[22] The development of quantum technologies is also financed by private funding, which was particularly significant in the US. The EU, together with the US, leads on the number of quantum patents granted, followed by Japan and China, but China leads on the number of patents applied for. On the other hand, China leads on the number of scientific publications, followed by the US and the EU.[23, 41]

European countries, including the UK and Switzerland, are leaders in quantum research, but for reasons listed in the Draghi report, EU actors often have difficulty transforming the results of research into practical applications and market opportunities, and then scaling up. Altogether, EU public investment in quantum (around USD 12 billion) is close to that of China, but lack of access to private funding, fragmentation and limited cross-border cooperation have hindered progress. The EU has the largest quantum start-up ecosystem (8 of 19 start-ups launched in 2024 were from the EU), and one third of all quantum companies worldwide are based in the EU.[40] However, these companies are generally smaller than their US counterparts, and these start-ups frequently need to look for US capital to mobilise funding to launch, and then scale up, a fact that also makes them prone to takeovers by US competitors. Europe has a strong position in quantum sensing, in particular in metrology, gravimetry, timing and navigation. Next to China, the EU leads in Quantum Key Distribution technology. The Quantum Europe Strategy[40] of July 2025 aims at addressing the weaknesses, and positioning Europe as a global leader in quantum by 2030.

The development of quantum technologies, in particular quantum information

technologies and quantum computing are seen by China as a top priority and a key area of global tech competition. The focus on quantum communication technologies is driven by the goal to secure first mover advantages in cryptology, secure communication and information processing. This strategic goal is underpinned by public investment of over USD 15 billion. China's quantum technology development is state-driven, and government services in security and military domains are the primary beneficiaries, though the technology is being rolled out to other areas, including education and business. China was the first country to deploy a quantum satellite, in 2016, and will launch a third one in 2026 as part of a space-ground quantum communication network project. China has already developed the biggest quantum communication network of more than 12 000 km.[42] China lags behind the US in quantum computing but is advancing quickly, and announced in March 2025 that it had developed a 105 (logical) qubit processor prototype.[43] Following the introduction of export controls by the US in 2024, and subsequently by Europe, on advanced chips, China prioritised the development of its own quantum chips and foundries.[42] By 2030, China aims to build 1000+ qubit quantum computers, achieve quantum advantage in real world applications such as finance, logistics and biomedicine, and become a leading global supplier of quantum technology and systems.[43] The country also has the ambition of setting global standards. Such rapid advances and the stated determination of the Chinese government imply that **China could be on track to deploy quantum communication first**.[42]

The US leads in quantum computing, including quantum computing data centres as well as in sensors. The development of quantum technologies in the US has been predominantly driven by the private sector (IBM, Google, Microsoft, Amazon, and a number of smaller players and start-ups). Private-sector-driven development has given priority to quantum computing and quantum sensing, where there is the most potential for practical applications and revenue, but this approach has under-served quantum communication.[44] US public investment in quantum represents only 50 % of China's (USD 7.67 billion as of 2025). Concerns about China gaining an advantage over the US in quantum technologies led to the initiative of preparing a new quantum strategy underpinned by funding from the federal budget. According to media reports, the White House is preparing a comprehensive quantum strategy underpinned by executive orders on quantum tech and post-quantum cybersecurity, to accelerate federal adoption of quantum technology and post-quantum cryptography, with the latter expected to be the focus. The orders are expected to set migration timelines across federal agencies and contractors.[45] The policy memorandum of 23 September 2025 on research and development priorities for 2027 places quantum next to AI, semiconductors and secure networks at the top, focusing on quantum, both in fundamental research and applied engineering, to secure US leadership, and linking it with national security, energy independence, competitiveness and economic growth. The government will support the creation of consortia to support pre-competitive research, expanding test beds and critical infrastructure, and funding for advanced manufacturing. Priority will also be given to maturing enabling technologies that underpin quantum computing and sensing, developing practical applications, speeding up the transition of quantum from lab-based experiments to the commercial marketplace, and preparing the US for post-quantum cryptography and strengthening cybersecurity.[46]

2.3. International cooperation on AI and quantum

The EU contributes to international cooperation on AI within the UN, OECD, Council of Europe, in the format of AI safety summits as well as in the G7 and G20. The UN Global Digital Compact[47] of September 2024 gave rise to an international scientific panel and a global policy dialogue on AI. The Global Digital Compact commits to developing AI capacity-building partnerships, and considering a Global Fund on AI. In 2022, UNESCO developed recommendations on the ethics of AI[48] and in 2024 the Council of Europe adopted a Framework Convention on AI, Human Rights, Democracy and the Rule of Law.[49] The OECD is leading work on AI Futures, to develop insights on possible future uses of AI and to help governments address potential challenges and seize opportunities, as well as to develop necessary capabilities. The OECD also leads cooperation within the Global Partnership on AI committed to the OECD AI Principles. The cooperation initiated at the 2023 AI Summit resulted in the publication of International AI Safety Reports,[50] and AI follow-up summits in Seoul and in Paris, which adopted several actions and commitments to foster trustworthy AI accessible to all, in the public interest. These include the development of more sustainable AI, trustworthy AI in the world of work, strengthening international AI governance and maintaining human control in AI-enabled weapons systems.

In line with the International Digital Strategy for the EU[51] of June 2025, Council conclusions of 2023 on digital diplomacy,[52] and the new Apply AI Strategy,[31] EU engagement in international cooperation on AI aims at strengthening EU leadership in global digital governance by promoting a rules-based digital global order, respecting fundamental values and ensuring a human-centric approach to the digital transition.

The second key objective is strengthening competitiveness and addressing dependencies on AI and AI-related risks in the context of the European Economic Security Strategy.[53] The EU will set up a new Digital Partnership Network to help strengthen its own tech competitiveness as well as that of its partners, and will develop the EU tech business offer involving public-private investment, including in AI factories, secure connectivity, cybersecurity and digital public infrastructure.

The EU is involved in cooperation on quantum within the G7, NATO (dual use and security context), and bilateral partnerships with like-minded countries such as Japan, Canada, South Korea and Australia, as well as with non-EU countries that take part in 'Horizon Europe'.

2.4. Cybersecurity

The leading providers of cybersecurity solutions come from the US, China, the UK, Japan and Germany.[54]

The increasing importance of cybersecurity is reflected in cybersecurity strategies and actions as well as in international cooperation. Initiatives such as the EU Cyber Resilience[55] and Cyber Solidarity[56] Acts have paved the way for stronger cybersecurity requirements in the EU, and the coordination of cybersecurity responses on a large scale.

To encourage the development and implementation of consistent Member State strategies of transition to quantum-safe digital infrastructure and to promote interoperability across Europe, the European Commission issued in April 2024 a Recommendation on Post-Quantum Cryptography.[57] ENISA, the European Union Agency for Cybersecurity, supports the EU and national authorities as well as the private sector in enhancing cybersecurity, including the transition to post-quantum cryptography. While many Member States have well-developed plans on the transition to post-quantum cryptography in critical sectors, many non-governmental organisations and business are not yet post-quantum ready, nor have they solid transition plans. With the roll-out of AI, businesses are also increasingly susceptible to related cybersecurity risks (see the chapter on risks and challenges). The EU Cyber Resilience Act of October 2024 enhances the cybersecurity standards of products with digital elements, requiring manufacturers and retailers to ensure cybersecurity throughout the lifecycle of their products,[55] which should help address one of the key cybersecurity challenges. The upcoming revision of the Cybersecurity Act[58] is planned to improve the European cybersecurity certification framework to strengthen resilience, and will support the development of a secure and resilient supply chain, and EU cybersecurity industrial base.

The EU is developing its Quantum Communication Infrastructure (EuroQCI), building upon the innovative quantum communication technologies developed within Quantum Flagship projects. EuroQCI includes a set of industrial projects and Member States' national projects supporting their transition to **PQC**, and should be used to validate architectures, interfaces and operational procedures.

International cooperation is becoming crucial, and takes place within the UN, INTERPOL, as well as NATO, and focuses on promoting cyber-resilience programmes, facilitating cross-border investigations, and intelligence-sharing. The level and intensity of this cooperation is determined by the level of trust that exists in different formats, and is closest among allies.

3. Developing strategic opportunities building on synergies between AI, quantum and cybersecurity

The future development of AI, quantum and cybersecurity are closely interconnected, with many potential synergies but tensions are also evident at the intersections.

3.1. Synergies in development of AI, quantum and cybersecurity

Advances in quantum computing will allow for much faster processing of data, performance of complex computational tasks conventional computers are not able to do, accelerating the development of AGI and the creation of more powerful AI systems. The key enablers and strategic opportunities are quantum machine learning (QML) and hybrid quantum-classical machine learning (QCML). Building on quantum operations, they permit improvements in complex machine learning computations in terms of speed, efficiency and accuracy. The integration of QML/QCML and AI offers an opportunity for more efficient AI systems.[59] Quantum computers could in future be used to better train AI on larger data sets, within a shorter timeframe. They might one day be better than conventional AI at performing certain operations, such as identifying correlations in data or developing models.[60] Integrating quantum computers into data centres will enable more efficient execution of large-scale data-processing tasks, which in turn will lead to further development of AI applications. Quantum computing, which consumes less energy than conventional AI machines (but still requires energy to power cryogenic cooling, laser or vacuum depending on the quantum technology used), could have the potential to help reduce the energy consumption of AI once fault-tolerant quantum systems are available, but is not likely to resolve the problem alone.[61]

AI will facilitate the design of more efficient quantum computing chips and algorithms for controlling and optimising quantum machines, as well as for mitigating and correcting incoherences (representing one of the main weaknesses of quantum computing) and analysing outputs.[21] It will enhance data processing in quantum sensing, improving its precision and sensitivity. It will also allow for the creation of user-friendly quantum programming interfaces.

Both **AI and quantum technologies can bring substantial advantages in cybersecurity, employing increased computational capacity to analyse big data sets for fast, automated threat detection and real-time response**. However, the same technologies will pose new threats, as explained in the next chapter. Quantum computing will on the one hand empower AI as regards cybersecurity, and on the other hand increase the risks of successful cyber-attacks.

Quantum computing can break existing cryptographic protocols and will require novel post-quantum cryptographic solutions. With increasingly widespread reliance on AI, including in the optimisation of industrial processes, management of energy grids and health or public services, cyber-attacks against AI-based systems could have a big impact. The application of **new quantum-based cryptographic methods such as QKD will strengthen cybersecurity** by offering increased protection against attacks aimed at intercepting the sharing of encryption keys. The use of QRNGs will enhance multi-factor authentication (MFA) for one-time passwords or challenge response procedures that today rely on pseudo-randomness.

AI-driven algorithms can play a role in QKD systems, helping to detect potential security breaches and to detect and correct errors.[9]

Advances in cybersecurity will facilitate secure quantum and hybrid computing, the creation of software more resistant to interference, and drive demand for quantum-computing-based technologies.

3.2. Possible innovations at the intersection of AI, quantum and cybersecurity

While there is substantial foresight research on possible innovations that could be developed within the three domains individually, insights into innovations that could be developed at the intersection of two or three of these domains are limited. The foresight process that informed the preparation of this paper identified several potential innovations which can be developed at the intersection of two or three of the domains. The following are some examples, although the list is not exhaustive.

3.2.1 AI–quantum

Floquet engineering, using quantum noise as a resource for error correction, and engaging AI, could speed up the uptake and scaling-up of quantum computing. For quantum sensing, it could facilitate the development of faster and lighter sensors that could be used, for example, in space.[62]

Combining quantum sensors with classical or hybrid (quantum-classical) AI will enable higher accuracy sensors. AI will play a key role in processing and analysis of the output of quantum sensors, such as pattern recognition and automatic detection, as well as filtering and reducing the external noise captured, or compensating and suppressing its effects on the useful signal (leading to reduced costs). AI could also be used for the optimisation of quantum sensors' systems, where many sensors work in a synchronised way, and sensor calibration. In the future, AI could enable quantum sensors' systems to detect slight geomagnetic changes across the Earth, and predict earthquakes or volcanic eruptions much earlier than is possible today. AI-assisted imaging could see deeper into body tissues. And in a more distant future (10-20 years) AI-quantum sensors could be used in geoengineering.[63]

AI could enable quantum sensors to detect slight geomagnetic changes, predict earthquakes and volcanic eruptions much earlier.

Femtosecond qubits could allow building of ultra-fast AI models, not limited by traditional chip (CPU/GPU) architecture. This technique would offer the advantage of building on the existing silicon-based technology and the feasibility of large-scale production.[64]

AI-assisted imaging could see deeper into body tissues.

Quantum-supported AI will facilitate approaching AGI and further development of natural human-machine interactions in a wide range of areas.

The introduction of **quantum sensors and computing will bring brain-computer interaction to a new, higher level** allowing for the acceleration of AI training, better simulations of neural networks, rapid modelling of large-scale brain datasets, and encrypted, and possibly secure, brain-to-device and brain-to-brain data transmission. Possible future applications may enable quantum-secure brain-to-brain communication including sharing thoughts, emotions or even intentions. Such solutions may facilitate collaboration in different emergency situations. Other potential applications could include the monitoring and treatment of mental disorders where the brain-computer interface monitors various signals of the mental status of a patient and suggests interventions or adapts the environment to help with regaining emotional balance. Another example could be smart, adaptive education, where a student's attention and comprehension are monitored, and the teaching methods and content offered are adapted accordingly.[65, 66, 67]

> Quantum-secure brain-to-brain communication could include sharing thoughts, emotions or even intentions.

3.2.2 AI–cybersecurity

Defensive autonomous AI agents will be deployed to protect IT systems by continuously monitoring for threats, proactively identifying and patching vulnerabilities, simulating cyber-attack scenarios to detect vulnerabilities, and responding in real time to cyber-attacks. These agents can operate with a level of speed and adaptability exceeding traditional security tools, enabling organisations to move from reactive to proactive, automated security protection.

> Autonomous AI agents will protect IT systems by monitoring for threats, identifying and patching vulnerabilities, simulating and preventing cyber-attacks

Other potential new opportunities are related to the paradigm shift in human-machine interactions enabled by **AI-powered interfaces**. These will allow moving beyond traditional dashboards and command-line tools to **AI-powered conversational and multimodal interfaces that leverage reasoning and intuitive interaction** to help professionals in cybersecurity and virtually any other complex domain, and even everyday users, to navigate and accomplish complex tasks.

AI-powered brain computer interfaces open space for innovation in cybersecurity – our unique brain patterns could be used to protect access to systems, e.g. operating like a biometric proof[68] (like fingerprints) used alone or with other verifiable factors.

> AI-powered conversational and multimodal interfaces leveraging reasoning and intuitive interaction will help professionals navigate and accomplish complex tasks.

3.2.3 Quantum–cybersecurity

Practical innovative applications of quantum computing in cybersecurity could focus on **quantum-assisted security and quantum-safe architecture**. Quantum-assisted security integrates AI methodologies with quantum computing to systematically analyse and strengthen cryptographic security.[69] Quantum-assisted AI can support cryptanalysis by detecting patterns and vulnerabilities in large data sets, and could accelerate the design of quantum-resistant cryptography through simulated quantum attacks and systematic identification of weaknesses. It will help map the boundary between what remains secure under emerging quantum capabilities and what requires new defences.

> Quantum-assisted security integrates AI methodologies with quantum computing to systematically analyse and strengthen cryptographic security.

Increased computational capacities of quantum systems, coupled with AI and machine-learning tools, open the way to **real-time threat detection and response**. This will enable Security Operations Centres (SOCs) to provide quicker and more effective responses to threats, and to avoid propagation to partner infrastructures with which they share cyber-threat intelligence.

> Computational capacities of quantum systems, coupled with AI and machine-learning tools, open the way to real-time threat detection and response.

Quantum-safe-oriented innovation could lead to developing and integrating algorithms resistant to quantum attacks, including practical migration strategies that ensure crypto-agility, and facilitate organisations achieving quantum readiness.

4. Understanding challenges and risks. Are we prepared?

While offering tremendous potential advantages, rapid development of AI and quantum, as well as cybersecurity, will present several significant challenges and risks.

4.1. Strategic autonomy and innovation-related

The country which leads in the technological race and gets first-mover advantage in critical technologies, such as AI and quantum computing and quantum communications, including post-quantum cryptography, will not only harness the economic and societal benefits, but also will be better equipped to safeguard its **security and strategic autonomy. Those lagging behind run the risk of aggravating existing dependencies, limited influence** in shaping the development of these technologies including setting standards, and a **lower share in the future tech market with all its consequences including risks for their security**.

In the coming years, **the digital divide is likely to deepen globally**, and the development of AI, quantum and cybersecurity will play a key role in this.

If the EU does not develop strategic autonomy in all critical elements of the value chain of the three domains, including semiconductors, general purpose AI and data management including data centres, cloud and edge during the coming years, this may **limit the economic and other advantages Europe can expect to gain from these domains as compared to its competitors**. It could also impact on Europe's global role, and open potential security and economic risks.

There is also **a risk that the values that will shape the development of technologies like general purpose AI (where the EU is not in the lead) will not be in line with the EU values** (for example, the US government and industry leaders promote unlimited freedom of speech, while the EU has strong policies to address hate speech and disinformation, which is intended to be further reinforced by the forthcoming 'European Democracy Shield'. Furthermore, solutions such as AI networks provided by other players can be biased, and their use could lead to suboptimal results for the EU users.

In view of US and Chinese policy to make their hardware and software the global standard, underpinned by proactive promotion of their solutions to third countries, **EU digital diplomacy that envisages supporting partner countries in developing AI infrastructure through the Global Gateway will face strong competition**, and may lead ultimately to promoting solutions offered by the lead players in the absence of European ones.

There are also **concerns that these critical technologies in the hands of authoritarian governments could be used for strengthening surveillance of opponents, social control and repression**.[70]

The EU strategies and investments in the three technologies could prove to be beneficial, but **it will be a challenge for the EU to keep pace with the US and China if there is no rapid improvement in the enabling environment** and addressing the obstacles defined in the Draghi[2] and Letta[3] reports. The Draghi report explicitly recognises the importance of increasing computational capacity in the EU as a critical component of a mature data economy.

Without improving the enabling environment, and in particular access to

European private venture capital, there is a **risk that the best European start-ups will continue to be exposed to takeovers by foreign competitors, who are also competing for European talent**. Attracting venture and other private capital is particularly challenging for quantum start-ups, where the timelines for commercialisation and significant revenues are longer than in the case of AI, and prospects of future profitability uncertain. An insufficient number of early adopters of AI and quantum among large European industrial players (unlike in the US) is further depriving European start-ups of sufficient market perspective.[40] Dependence on funding by non-EU actors also runs the risk that these actors will influence or determine the development of European companies in line with their vision and values.

So far, EU-wide cooperation in the development of these new technologies has mainly been supported by EU funding, while national programmes mainly focus on national projects. This is beginning to change (e.g. joint German-Dutch-French projects in quantum), and will need to expand further if the EU is to benefit from better cross-border cooperation and strengthen its competitive advantage vis-à-vis rivals in the US and other countries.

Reliance on data centres and cloud services located outside Europe gives the businesses managing them a competitive advantage over European ones and could be a source of other risks.

Further challenges are related to **limited uptake of these new technologies in the EU, which may put European businesses at a competitive disadvantage**.

In the advance of AI and its applications, several immediate and tangible challenges still remain to be addressed, such as the quest for explainability, robustness, fairness and accountability. These are issues that raise profound theoretical questions and have significant practical implications.

If the current scaling-up trend continues, AI factories and data centres will increase demand for energy and for water used for cooling, at a time when water shortages are on the rise. A hyper data centre is estimated to consume as much energy as 80 000 households. The International Energy Agency (IEA) estimates that, by 2030, energy consumption worldwide will reach more than 945 TWh compared to 425 TWh in 2024, and 1 400 TWh by 2035. In the coming years, this increase will occur mostly as a result of the use of fossil fuels such as gas and coal, which will undermine efforts to reach CO_2 emission targets (by 2030, CO_2 emissions from data centres will more than double, and will start falling slowly only thereafter),[71] and re-opened or new nuclear power plants. The transition to renewables will remain problematic in the near future, considering the unpredictability of supply and the need to satisfy steady demand of data centres for energy, and spikes of energy consumption during the AI training phase. Leading AI companies therefore invest in off-grid power plants. There are estimates that, by 2027, AI globally may use up to 6.6 billion m^3 of water, the equivalent of nearly two-thirds of England's annual consumption.[72] Furthermore, with the current trends in scaling-up of AI data centres (training computations doubling every 5 months for notable AI models, while datasets for training Large Language Models are doubling every 8 months), the power required is growing annually,[4] and there is a **likelihood that supply chains will be strained globally.**[73]

4.2. Security-related

Quantum computers will be able to break the cryptography on which our conventional systems rely. This implies not only a cybersecurity threat at some point in the future, but also a potential cybersecurity threat today due to 'harvest now, decrypt later' actions by third-state actors[17] making **timely migration to post-quantum cryptography urgent and critical.**[18] This applies to all levels of public governance, from the state to local authorities, the security sector as well as businesses and civil society organisations.

Increasingly capable AI will exacerbate cybersecurity challenges and risks.[9] **Conversational interfaces and increasing technology access will significantly expand the opportunities for cyber-attacks and other vulnerabilities.** The challenges can be grouped in two clusters:

- **Attacks on AI and AI vulnerabilities.** AI systems are targets for cyber-attacks, and as they will increasingly be part of governance and decision-making systems in the public and private sector, the implications could be serious. With increasing participation of AI agents in the digital economy, for example by subscribing to paid or free platforms, or conducting financial transactions on behalf of people or organisations, they will introduce a new layer of cyber risks. Furthermore, issues in AI training and use can compromise privacy, introduce biases, and result in degraded performance[1]. These vulnerabilities threaten the integrity of the deployed systems.
- AI-powered insecurity. Attackers – criminals or third-state actors – will have increasingly easy access to generative AI to carry out more sophisticated, faster and large-scale cyber-attacks using personalised phishing, and other social engineering with

the use of deep fake and fake personas, and profiling information collected thanks to AI to install malicious codes. AI can also be used to run attacks aimed at automated detection and exploration of vulnerabilities in IT systems, and to gain a foothold to infect as many systems as possible. The latest ENISA Threat Landscape 2025 reports the emergence of stand-alone malicious AI systems such as Xanthrox AI which indicates the trend of threat groups moving beyond jailbreaks towards customised tools running on local servers to avoid detection. Malicious actors also use fraudulent websites for legitimate AI tools and poisoned hosted machine-learning models to distribute malware.[24] Furthermore, widespread use of AI-assisted programming virtual assistants, without proper human oversight and control, may lead to unintentional acceleration of insecure software development and usage.[74, 75]

The transition to post-quantum cybersecurity will also pose multiple challenges. In the first place, **there is a significant under-estimation of quantum capabilities**, and of the risks related to breaking conventional encryption algorithms and decrypting previously collected, encrypted content once quantum computing reaches a stage to allow it. This **may result in insufficient resolve and sense of urgency to put in place post-quantum cybersecurity solutions which need to be applied to entire ecosystems** where the protected content is used, including by contractors, for example. Moreover, experience in the deployment of other security technologies indicates that, despite providing strong guarantees, deployment can be hampered by usability barriers and the lack of specialised expertise.[76] Unless **human and behavioural factors are anticipated and addressed early, technological progress risks stalling**.

The spread of brain-computer interfaces, powered by AI in consumer and other contexts, will probably **turn the human brain itself into a new battlefield in this fast-changing environment**. This new category of cybersecurity risks – if they materialise – may lead to breaches of individuals' mental privacy or integrity and even attempt to change their mental capabilities or specific character features. Access to and mining of raw neural data would give attackers the possibility to detect and use illegally, and without the individual's agreement, many potentially sensitive attributes. Innovative safeguards will necessarily be required to protect against threats to mental privacy and manipulation.[77]

4.3. EU regulatory framework and governance-related

Widespread use of AI to support the processes and decision-making of democratic institutions and governments at all levels may have **serious implications for policy choices and effectiveness of democratic control** of decisions taken and policies adopted, and ultimately lead to undermining public confidence.[5] One of the key challenges is to be found in **errors and hallucinations** included in the output of generative AI-based tools, which limit their reliability. **The risk is exacerbated when there is no effective human control of AI outputs, or those in authority do not understand the technology and its limitations well enough.**[78]

There are **concerns about the ability of humans to keep control of Artificial General Intelligence, and its Superintelligence version, once it is ultimately developed and becomes highly autonomous and less or even non-dependent on human input.**[79] The warning signals come from experts in AI, including those who led AI development like the Nobel Prize laureate Geoffrey Hinton and experts behind the International AI Safety Report.[50] These concerns led to an appeal initiated in March 2023 to pause development of AI models more powerful than GPT-4 level until there is sufficient confidence that the effects of their development will be positive and the risks manageable.[80]

With increasing availability and capacities of AI and AI-based tools like those used for automated profiling, targeting deep fakes, widespread **disinformation, public opinion manipulation, and other social engineering actions by third-country and internal actors**, seem set to take a further toll on society, democratic systems, and trust in public institutions, if urgent action is not taken to rapidly develop societal resilience and uphold democratic institutions and processes.[81] The objective may be manipulation of public opinion, generating support for specific policy choices, influencing choices of voters in elections, provoking a sense of uncertainty, or destabilising the political situation and markets. This may further increase the vulnerability of already disadvantaged or marginalised groups in society, like the elderly, the disabled or less tech-savvy people, and lead to undermining public confidence in democratic institutions and policies.[5] This category of risks is explored in more depth in the ESPAS foresight paper on democracy.[82]

People in decision-making roles using AI in representative and governmental institutions, businesses and other organisations, may not have the **necessary**

skills to understand the limitations and capabilities of the AI systems they are using to assess the quality of AI outputs, or they may have too much confidence in the AI tools used and their own capabilities. This could lead to an **over-reliance on AI outputs**, with the risk of propagating hallucinations and biases by integrating flawed outputs into critical processes or decisions. The key challenge will be to ensure that humans stay in control and are capable of assessing and mitigating these risks.

The authors of the International AI Safety Report 2025 also point at existing information gap between what AI companies know about their AI systems and what governments and non-industry researchers know. Strong competitive pressure may lead to deprioritising risk management.[50]

The increased complexity of AI systems combined with insufficient skills could lead to a reduction in **the effectiveness of traditional risk assessment and management practices**.

The expected increased use of agentic AI will create new vulnerabilities, such as **responsibility gaps in hybrid human–AI teams**.

Concerns related to transparency and traceability of AI operations will grow. This particularly applies to sectors where AI-supported decisions will have an impact on human life and health or lead to legal or economic implications potentially resulting in litigation.

For **business and financial markets**, the implication of widespread use of AI to support analysis and decision-making could **increase operational risks, may harbour the potential for increased herding behaviour and market correlation**, and pose risks for financial institutions and the wider financial system.[83] Further risks could be related to the increasing advantage of big players over small investors in making optimal investment choices.

Shifting the paradigm of **human–machine interaction through development and application of brain-computer interfaces, AI poses new ethical challenges**, such as questions about the rights to access someone else's thoughts, or human brain enhancement with AI and interpretation of human rights in the new context. Another type of ethical challenges is related to automation of decisions that may have implications for human health, life or other loss, like in autonomous transport, in situations when accidents are inevitable. Further ethical challenges emerge in the interactions between humans and generative AI models, when the latter offer misleading advice driving people to harm themselves, or give an impression of empathy, build relationships and provoke sentimental feelings. Other risks relate to online AI-supported personalised advertising and trading services applying profiling and behavioural insights.

4.4. Skills-related and socio-economic

Skills and knowledge will remain the critical factors in safe and responsible deployment of AI, quantum and post-quantum cybersecurity in the EU, and in ensuring European innovation and research remain on a par with the US and China. This challenge applies from decision-makers to experts in their domains, and across society at large. Rapid advances in AI, quantum and cybersecurity imply that **the skills gaps cannot be addressed only by updating curricula in schools and universities, because such changes will bring results only in the medium and long term**. Moreover, European start-ups and research entities often cannot compete with the key global players when it comes to the attractiveness of employment conditions, posing a challenge to prospects of retaining talent in Europe. There is also a new trend of takeovers of the entire teams of start-ups by their competitors.

The **roll-out of AI will bring fundamental changes to the labour market** – according to the IMF it will affect 40 % of jobs worldwide, starting with 'easy-to-learn tasks', and require skills to manage its use.[84, 85] It is also likely to bring changes to the economic model we know today and, depending on how the use of AI is managed, it may lead to job losses instead of increasing employees' productivity, complementing human capabilities and empowering people. **If this materialises, the job replacement scenario would probably lead to a deepening socioeconomic divide** and a (disproportionate) increase in wealth for those controlling digital technologies.[86, 87] In Europe, the adoption of AI has the potential to change the social contract.[88] Moreover, the **claim that, in future, work will be done by AI-driven agents and robots, while humans, benefiting from universal income, can use their time for more creative activities is misleading** for several reasons. First if these creative activities can be automated, they will sooner or later be taken over by AI. Second, work and other activities creating value for people and society are important to people and contribute to their sense of purpose.[89] As the self-determination theory points out, **satisfying basic psychological needs such as sense of empowerment, individual autonomy, competence and relatedness is essential for people's wellbeing and growth**.[90] There is also a risk of gradual loss of skills and competencies in the long term if they are no longer used and further developed. All in all, **there is a risk that the benefits of AI will not be equally distributed across society**, which will have implications for socioeconomic fairness, civic access and participation, and potentially for the future of democracy itself. Similarly, in line with the already clear trend, **big companies will likely lead in the application of AI, quantum and cutting-edge cybersecurity solutions, gaining competitive advantage over small and medium-sized enterprises**. This may lead to an increasing divide if the smaller companies and other organisations do not get sufficient support to take advantage of these new technologies.

5. Managing the disruption – Strategic choices for EU policy-makers

To take full advantage of the new technologies and manage their risks, the EU should consider a number of strategic choices.

5.1. Strengthening strategic autonomy and innovation

The **EU's strategic autonomy and economic security in all three domains covered in this paper should be developed in partnership with European industry and the research community**. European industries and companies should play a key role in supply chains.

Dependencies in critical supply chains need to be urgently addressed in EU policy-making and, when necessary, through public support encouraging and leveraging private investment. This applies to the development of European data centres and cloud capacity, prioritising highly critical use cases and high security needs in the public and private sectors. Other areas where action is necessary include cybersecurity, semiconductors and critical supply chains for quantum technologies. Hence the importance of a speedy roll-out of initiatives as 'AI Continent', 'Apply AI' or 'AI in Research' as well as the forthcoming 'Cloud & AI Development Act' and 'Cybersecurity Act', regular assessment of progress towards set goals and when necessary, speedy corrective action.

The EU is facing a strategic choice between overcoming differences and inertia, and taking decisive action based on the recommendations of the Draghi and Letta reports, or backsliding in the global tech race with all the consequences for European competitiveness, growth prospects and strategic autonomy. With limited public resources, **public-private partnerships and private investment** will be instrumental in pursuing the EU's long-term goals related to development and adoption of technology in the three **domains**. The key areas where urgent action is needed are the **development of an effective, deep risk-capital market to improve accessibility to risk funding in Europe for European tech start-ups and innovative companies** seeking capital to launch their project and then to scale it up (so that they do not need to turn to the US market and the Nasdaq) and **leveraging public funds to support innovation and attract private funding**. Public procurement, and instruments like Important Projects of Common European Interest (IPCEI) can help de-risk European manufacturing capacity while maintaining open, standards-based interfaces for a competitive marketplace. The EU could also consider a CERN-like EU AI initiative.

In particular, a solution has to be found to **facilitate funding for quantum start-ups which bear higher risks and have long timelines to get to market and become profitable**. The EU could further learn from the US experience and ecosystem that facilitates the launch and development of innovative start-ups.

More funding, both public and from the private sector, will be needed for applied and fundamental research. **Research cooperation involving several Member States should be encouraged.**

Good practices like incubators of innovative start-ups at European universities, providing guidance and support for graduates to start their own business could be more widely known and replicated across Europe. Creating such an enabling environment requires closer cooperation between the public sector, academia and research institutions, and industry.

Different EU policies and initiatives set out in the Competitiveness Compass – some already in place, such as the European Startup and Scaleup Strategy,[91] the Quantum Strategy, the Apply AI[31] initiative as well as the forthcoming European Innovation Act and EU Cloud & AI Innovation Act – will help address these challenges, but will require expedited implementation and sufficient funding, including in the next multiannual financial framework.

The EU needs to **enable development of European champions** in AI and quantum, which are able to compete and operate globally.

To enable European businesses and other organisations to benefit from the high AI and quantum-based computing power that will be made available and from the deployment of autonomous AI-based robots, the EU should work towards the **timely availability of high capacity (5G, 6G) and low latency telecommunications infrastructure across Europe** to ensure real-time device-provider interactions.

The EU has a vested interest to **keep up its leading role in research in all three domains** covered by this paper. In quantum, the EU could prioritise error-correction quantum research as well as the development of compiler/runtime ecosystems that shorten the paths from algorithms to hardware, and co-development of early, domain-specific use cases in key potential application areas such as chemistry, materials, optimisation and secure communications. In AI, both fundamental and applied research are important. It is fundamental research that addresses the key challenges such as explainability, safety, security, bias, robustness, fairness and alignment. Progress in these areas would have a cascade effect across all application domains and would help improve policy and legislative mechanisms of control.

To address the challenge related to high usage of energy and other resources, the **EU should promote sustainability by design in development of AI and quantum infrastructure** including energy and water metering, heat reuse, and responsible management of helium for quantum and end-of-life plans. European quantum initiatives need also to address critical supply chains including cryogenics, lasers, vacuum systems, control electronics and other specialised materials.

Due to practical challenges in hybridisation, co-location of hybrid quantum computers at the European HPC sites and common interface profiles (job scheduling, timing, telemetry, safety) should be the default choice, enabling industry-relevant pilots and reproducible benchmarks.

In the area of **quantum sensing**, Europe's strengths can be leveraged through **coordinated validation and conformity assessment programmes**, which could include reference datasets and test sites. The priority areas for quantum sensing could include subsurface exploration and infrastructure monitoring, precision navigation in GNSS (Global Navigation Satellite System)-denied settings and biomedical diagnostics.

Accelerating the building of the necessary infrastructure for AI and quantum, including establishing European AI factories and gigafactories, and ensuring access for EU companies and scientific institutions needs to remain the top priority. It is important that new EU AI labs and gigafactories are in place quickly, as they will be **vital for rolling out the application of AI across Europe as well as for strengthening its strategic autonomy**.

The EU should not give up on catching up on general-purpose AI, potentially being able to choose more efficient and sustainable ways than the current global leaders, and maintaining compliance with EU values. This would imply smaller models, based on open sources, trained properly with limited sets of quality data. This would require greater discussion and, if confirmed, setting a clear vision and realistic expectations.

5.2. Security aspects

Even though it will take some years before full-size quantum computers materialise, the capabilities of advancing quantum technology may remain under-estimated. For reasons presented in the risks and challenges chapter, the **development and**

roll-out, as well as regular updating of post-quantum cryptography solutions is already an urgent priority for the EU. This requires **developing awareness and skills, and making necessary investments**, accepting the risks that some solutions may in the end not work, or become obsolete in a short period of time.

Setting timelines could help. The transition strategies need to apply to the entire ecosystems, including businesses and contractors that have access to protected content. In view of EU competitiveness and the protection of intellectual property rights, the successful transition of businesses and research organisations to post-quantum cybersecurity is also important.

In migration to post-quantum cryptography, **lessons from previous experiences with classic cryptography, including behavioral insights, should be applied**. Availability of usable libraries, development environments and configuration tools will be essential for a secure and rapid transition to a European digital infrastructure that is resilient to quantum-enabled threats, to avoid developers introducing security issues in applications.[92]

Furthermore, **it will be necessary to address cybersecurity-related vulnerabilities of AI systems and prevent new types of cybercrime that may compromise AI systems**. The EU should make effective use of the Cyber Resilience Act to ensure the suppliers of IT solutions, both hardware and software, apply due diligence, and detect and eliminate vulnerabilities in their products offered in the EU.

While basing the advance of AI on open-source technologies, the EU needs to anticipate related risks of use of AI by malicious actors or for criminal purposes, and put in place appropriate safeguards.

An increasing role of AI agents acting as autonomous 'users' and providers of digital services will require a change in the digital services infrastructure and its security. This will likely require to be accompanied by adaptation of the regulatory frameworks. Technological innovation will be needed to prevent misuse and guarantee safe interaction, with agent-specific identity frameworks being key.

5.3. The EU regulatory framework

The EU regulatory framework will clearly need to keep pace with innovation and technological progress, and the evolution of risks and opportunities, to frame the development of the new technologies. As many experts have warned, development of general-purpose AI in particular, without the necessary safeguards, may lead to unwanted and irreversible results, and regulations put in place post factum may not be able to address the problems. **Creating an adaptive policy and regulatory**

framework will require agility from the EU and further streamlining of the decision-making processes which are long in view of the pace of advances in AI development.

In order to address the build-up of problems with misinformation, social engineering and criminal or other illicit activities using deep fakes and other AI-supported techniques, and to protect citizens, **enacting legislation protecting people's image, voice and other characteristics used for such practices should be urgently considered**, drawing on the experience of Member States like Denmark and Italy.

Facing two very different visions of the future of AI, driven by the US and China, the EU chose to pursue its own path of responsible and human-centric AI and tech development, and as already committed to in its policy documents, **needs to take decisive action to lead, mobilise the support of international partners and influence the development of global governance frameworks**. The EU needs to **work with international partners to identify risks and promote approaches addressing these risks and challenges related to the development and application of AI**.

Development of Artificial Superintelligence is not inevitable and depends on the strategic choices of the key players – international cooperation is necessary to better explore potential risks and advantages.

The EU will also need **to work closely together with like-minded partners to assess and address the risks of development and use of AI and quantum technologies by its adversaries, in the military and hybrid warfare context**.

With massive roll-out of AI in the years ahead and increasing reliance on AI solutions to inform and support decision-making, as well as the evolution of a hybrid human and agentic workforce, **there is an urgent need to adapt decision-making and management as well as risk assessment and management methodologies, and policies to address the emerging risks**.

In view of the **ethical concerns about the development and deployment of certain AI applications** like brain-computer interfaces for human enhancement, **there is an urgent need to identify related risks in an anticipatory way**. This should be accompanied by reflection involving experts about how these concerns can be addressed, and expediting the necessary policy and regulatory action to protect rights, in particular privacy, autonomy and integrity of human beings and their rights as consumers and in other roles, to effectively prevent malicious actors from using these technologies for criminal and other illicit or unethical purposes.

It is also necessary **to consider putting in place requirements that machine-human interfaces be designed in a way to facilitate critical thinking, counter cognitive biases,**

and guide informed decision-making with a human in the driving seat, performing tasks for which the machines have been developed, from security configuration or misinformation handling to medical diagnostics and design of treatment therapies, or in managing industrial processes. This approach will be of strategic importance both to reinforce organisational and societal resilience against digital threats, ensure human control over technology and prevent a decline in skills.

5.4. Skills, education and socio-economic

The global battle for talent to keep up the pace of innovation will become even more critical in the years ahead. **To keep and attract talents, the attractiveness of working in research and innovation in Europe could be further improved.**

It will be necessary to rapidly upgrade the skills of different professions to enable the optimisation and management of the use of the new technologies in a way that increases their productivity and efficiency and output quality, while still complying with the human-centric approach. University curricula in all the relevant domains will require to be regularly updated and better linked to the anticipated needs of the labour market, to equip graduates entering employment with the necessary skills. They should also include the ethics of application of the new technologies and the legal framework. **Priority should be given to modernisation and regular updating of curricula in technical and scientific domains.** It is also urgently necessary to **address the shortages of AI, quantum and post-quantum security-competent IT professionals**, to ensure an efficient and secure uptake of AI and quantum across Europe and transition to post-quantum cybersecurity. Finally, **general skills such as critical thinking and anticipation as well as awareness of the opportunities and risks related to use of the three technologies will become indispensable to strengthen societal resilience** in the face of risks related to advances in the new technologies.

The skills challenges and the pace of the AI and quantum-induced change **calls for urgent action, also beyond the conventional education cycles** as the latter will produce results only in the medium and long term. **In particular, training and integrating highly skilled technical experts across academia, industry and governance, to keep pace with innovation and enable evidence-based decision-making could be prioritised.**

The European Union, with its objective of human-centred technological development, should seek to **frame the future deployment of AI across all areas in a way that would empower humans and enhance human effectiveness and capacity. The way AI deployment is framed and carried out** will have **far-reaching implications for the**

social contract, social and political cohesion across the EU and within Member States, for economic growth, the condition of society and individuals and – ultimately – the future of European democracy. It will require further anticipation/foresight to inform strategic policy decisions, and a strong political steer, with incentives and effective checks and feedback mechanisms.

There is a need for more in-depth analysis and understanding of the potential impact of new technologies, in particular AI and its possible future applications, as well as the way they will change the environment in which we live, on human beings and society as a whole, drawing on psychology, medical and sociological research.

ENDNOTES

1 Özcan, B., Juijin, D., Graabak, J., Bogerd, S., 'Advanced AI: Possible Futures. Five scenarios for how the AI-transition could unfold', Centre for Future Generations, 10 July 2025.

2 Draghi, M., 'The future of European competitiveness', September 2024

3 Letta, E., 'Much more than a market. Speed, security, solidarity. Empowering the Single Market to deliver a sustainable future and prosperity for all EU Citizens', April 2024

4 ''Artificial Intelligence Index Report 2025', Stanford University, Human-Centered Artificial Intelligence, 2025.

5 Sucha, V., 'Before AGI arrives: why 2025-2030 determines the future of democratic AI governance', European University Institute, July 2025.

6 Rahilly, L., Amar, J., 'The Future of Work is Agentic', McKinsey podcast, 3 June 2025.

7 Milmo, D., Almeida, L., 'Workforce crisis: key takeaways for graduates battling AI in the jobs market', The Guardian, 13 July 2025.

8 Kinder, T., 'Absolutely immense: the companies on the hook for the $3tn AI building boom. Private capital joins Big Tech in seeking to capture rewards from historic expansion of data centres', Financial Times, 14 August 2025.

9 Stylianou, N., Learner, S., Bradshaw, T., Uddin, R., Bott, I. et al, 'Inside the relentless race for AI capacity. The quest for superintelligence in spurring a data centre boom – but critics question the cost, environmental impact and whether it is all needed', Financial Times, 31 July 2025.

10 Noffsinger, J., Patel, M., Sachdeva, P., Bhan, A., Chang, H. et al, 'The costs of compute: A 7$ trillion race to scale data centers', McKinsey Quarterly, 28 April 2025.

11 'U.S. and China Carry the Weight of Global Data Centre Growth', digitalinformationworld.com, 8 March 2025.

12 Bangalore, S., Srivathsan, B., Bhan, A., Del Miglio, A., Sadcheva, P., 'Why invest in the data center economy', Mc Kinsey, 17 January 2023.

13 'The Next Frontier of Human-Machine Interaction', IE University, Brief No 14, 28 August 2025.

14 Murgia, M., 'Microsoft's Christopher Bishop: Scientific Discovery is AI's Killer Application', Financial Times, 3 April 2025.

15 Malervy, J. 'Google's AI Co-Scientist is outsmarting human scientists', AI GPT Journal, 19 February 2025.

16 Chui, M., Roberts, R., Yee, L., Hazan, E., Singla, A. et al, 'The economic potential of generative AI: The next productivity frontier', McKinsey & Company report, 14 June 2023.

17 Acemoglu, D., 'The Simple Macroeconimics of AI', April 2024, MIT Economics Stone Centre, April 2024.

18 ibidem

19 'From High-Performance Computing to High-Performance Problem Solving', World Economic Forum, 23 January 2025.

20 Shivakumar, S., Wessner, Ch., Schumacher, A., 'Quick take: Quantum Technology Global Competition', CSIS - Center for Strategic International Studies, 3 February 2025.

21 Tomoshige, H., Singerman, P., 'Progress Towards Practical Areas of Quantum Technology', 15 July 2025, CSIS – Center for Strategic & International Studies, 15 July 2025.

22 'Quantum Initiatives Worldwide 2025', QURECA.com, 2 October 2025.

23 Soller, H., Gschwendter, M., Shabani, S., Svejstrup, W., 'Quantum Technology Monitor 2025. The Year of Quantum: From concept to reality in 2025', McKinsey Digital, 23 June 2025.

24 'ENISA Threat Landscape 2025', European Union Agency for Cybersecurity, October 2025.

25 'Gartner Forecasts Worldwide End-User Spending on Information Security to Total $213 Billion in 2025', Gartner, 29 July 2025.

26 'Worldwide Security Spending to Increase by 12.2% in 2025 as Global Cyberthreats Rise, Says IDC', IDC – International DataCorporation, 21 March 2025.

[27] Hawkins, Z., Lehdonvirta, V., Wu, B., 'AI Compute Sovereignty: Infrastructure Control Across Territories, Cloud Providers and Accellerators', Oxford University, 20 June 2025.

[28] Pilz, K.P., Rahman, R., Sanders, J., Heim, L., 'Trends in AI Supercomputers | Epoch AI', www.epoch.ai/blog, 23 April 2025.

[29] 'Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)', OJ L 2024/1689, 12 July 2024.

[30] 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: AI Continent Action Plan' of 9 April 2025, COM (2025) 165, 9 April 2025.

[31] 'Communication from the Commission to the European Parliament and to the Council: Apply AI Strategy', COM (2025) 723 final, 7 October 2025.

[32] 'Communication from the Commission to the European Parliament and the Council: A European Strategy for Artificial Intelligence in Science. Paving the way for the Resource for AI Science in Europe (RAISE)', COM (2025) 724 final, 8 October 2025.

[33] 'Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: A Competitiveness Compass for the EU', COM (2025) 30 final, 29 January 2025.[34] 'Winning the Race. America's AI Action Plan', White House, July 2025. [35] Eadicicco, L, Duffy, C., 'Trump's AI plan: Pull back restraints on tech', CNN, 24 July 2025.

[36] Daniels, O.J., Dohmen, H., 'China's Overlooked AI Strategy. Beijing is Using Soft Power to Gain Global Dominance', Foreign Affairs, 25 July 2025.

[37] Cong, W., Yeping, Y., 'China launches Global AI Governance Initiative, offering an open approach in contrast to US blockade', Global Times, 18 October 2023.

[38] 'China announces Action Plan for Global AI governance', ANSI (American National Standards Institute), 1 August 2025.

[39] Che, Ch., 'I have to do it: why one of the world's most brilliant AI scientists left the US for China', The Guardian, 16 September 2025.

[40] 'Communication from the Commission to the European Parliament and the Council. Quantum Europe Strategy: Quantum Europe in a Changing World', COM (2025) 363 final, 2 July 2025.

[41] Lewis, A., Scudo, P., Cerutti, I., Travagnin, M., Marcantonini, C. et al, 'Future Directions of Quantum Technology in Europe, October 2025', European Commission-JRC, Publications Office of the European Union, Luxembourg, 2025, European Commission-JRC 141050.

[42] Hmaidi, A., Goenwegen-Lau, J., 'China's long term view on quantum tech has the US and EU playing catch up', MERICS (Mercator Institute for China Studies), China Tech Observatory, 12 December 2024.

[43] 'Quantum Computing in China – Innovation, Industry, Leaders and Future Prospects', SPINQ, 18 August 2025.

[44] Marci, T., 'Renewing America's Quantum Strategy for the Next Computing Era', QuEra.com, 20 August 2025.

[45] Swayne, M., 'Reports: White House Prepares Executive Actions On Quantum Tech And Post-Quantum Cybersecurity', Quantum Insider – thequantuminsider.com, 20 September 2025.[46] 'Memorandum for the Heads of Executive Departments and Agencies on Fiscal Year 2027 Administration Research and Development Budget Priorities and Cross Cutting Actions', White House, 23 September 2025.

[47] 'Global Digital Compact', UN Office for Digital and Emerging Technologies, 22 September 2024.

[48] 'Recommendations on the Ethics of Artificial Intelligence', UNESCO, 23 November 2021.

[49] 'Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law', Council of Europe, September 2024.

[50] Bengio, Y., Minderman, S., Privitera, D., Besiroglu, R., Casper, S. et al, 'International AI Safety Report 2025', DSIT 2025/01, 15 February 2025,

[51] 'Joint Communication (of the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy) to the European Parliament and the Council: An International Digital Strategy for the European Union', JOIN (2025) 140 final, 5 June 2025.

[52] 'Council conclusions on EU Digital Diplomacy', Council of the European Union 10526/23, 26 June 2023.

[53] 'Joint Communication to the European Parliament, the European Council and the Council on "European Economic Security Strategy"', JOIN/2023/20 final, 20 June 2023.

[54] 'Cybersecurity – Worldwide', Statista, 2025.

[55] 'Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2023 on horizontal cybersecurity requirements with digital elements and amending Regulation (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)', OJ L, 2024/2847, 20 November 2024.

[56] 'Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act)', OJ L,2025/38, 15 January 2025.

[57] 'Commission Recommendation of 11.04.2024 on a Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography', C(2024) 2392 final, 11 April 2024.

[58] 'Consolidated text: Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)', Eur-Lex, 4 February 2025.

[59] Slapczynski, T., Stradomska, M., 'Opportunities and Challenges in Integrating AI with Quantum Computing', ASEJ Volume 29, No 2, pp 56-64, July 2025.

[60] 'From High-Performance Computing to High-Performance Problem Solving', World Economic Forum, 23 January 2025.

[61] Pashaei, P., 'Can Quantum Computers Address the AI Energy Problem?', Quantum Computing Report by CQI, 28 March 2025.

[62] Baker, B., Hastings, M., Haah, J., 'Azure Quantum Innovation: Efficient error correction on topological qbits with Floquet codes', Microsoft Research Blog, 5 May 2022.

[63] Ivezic, M., 'AI and quantum sensing. A perfect synergy', Postquantum, 28 February 2025.

[64] Cole Johnson S., Jhuria, K., 'Femtosecond laser creates 'programmable' optical qbits in sillicon', Laser Focus World, 18 June 2024.

[65] 'The Future of Brain-Computer Interfaces: AI and Quantum Tech Leading the Way', Neuroba, 21 June 2025.

[66] Gielas, A.M., 'Warfare at the speed of thought: can brain-computer interfaces comply with IHL (International Humanitarian Law)?', ICRC blog – Humanitarian Law & Policy, August 2025.

[67] Maiseli, B., Abdalla, A.T., Massawe, L.V., Mbise, M., Mkocha, K. et al,'Brain-computer interface: trend, challenges and threats', Brain Informatics, Volume 10, 20 (2023), August 2023.

[68] Arias-Cabarcos, P., Habrich, T., Becker, K., Becker, C., Strufe, T. 'Inexpensive brainwave authentication: new techniques and insights on user acceptance', Proceedings of the 30th USENIX security symposium 11-13 August 2021 pp. 55-72, 2021.

[69] Radanliev, P., 'Artificial intelligence and quantum cryptography', Journal of Analytical Science and Technology, 15, 4, 2024.

[70] Weber, V., 'Data-Centric Authoritarianism: How China's Development of Frontier Technologies Could Globalize Represssion', National Endowment for Democracy & FORUM – International Forum for Democratic Studies, 11 February 2025.

[71] Bryan, K., Tauschinski, J., Stylianou, N., Xiao, E., Webber, J., 'Inside the AI race: can data centres ever truly be green?', Financial Times, 7 August 2025.

[72] Li, P., Yang, J., Islam, M.A., Ren, S., 'Making AI Less "Thirsty": Uncovering and Addressing the Secret Water Footprint of AI Models', Cornell University, 6 March 2025.

[73] 'Sixth Annual Global Technology Report', Bain & Company, 23 September 2025.

[74] Pearce, H., Ahmad, B., Tan, B., Dolan-Gavitt, B. and Karri, R., 'Asleep at the Keyboard? Assessing the Security of GitHub Copilot's Code Contributions'. *2022 IEEE Symposium on Security and Privacy (SP)* (pp. 754-768), IEEE Computer Society, May 2022.

[75] Perry, N., Srivastava, M., Kumar, D. and Boneh, D., 'Do users write more insecure code with ai assistants?', Proceedings of the 2023 ACM SIGSAC conference on computer and communications security (pp. 2785-2799), 23 November 2023.[76] Halevi, S., 'Advanced Cryptography: Promise and Challenges', Keynote address, ACM CCS 2018, Toronto, 2018.

[77] 'The risks and challenges of neurotechnologies for human rights', UNESCO and University of Milan-Bicocca – Department of Business and Law, and State University of New York (SUNY) Downstate, UNESCO 2023.

[78] Hoos, H. (interview), 'A Great Opportunity or a Great Risk – How Exactly Should We View AI?', RWTH Aachen University, 4 July 2025.

[79] Brown, S., 'Why neural net pioneer Geoffrey Hinton is sounding the alarm on AI', MIT Management Sloan School, 23 May 2023.

[80] 'Pause Giant AI Experiments: An Open Letter. We call on all labs to immediately pause for at least 6 months the training of AI systems more powerful than GPT-4', Future of Life Institute, 22 March 2023.

[81] Sucha, V., 'Preserving human agency in the age of AI', EUI, STG, Policy Brief, 2025/12

[82] Finamore, S., ' What future for democracy in Europe?', ESPAS foresight paper, November 2025.

[83] Leitner, G., Singh, J., van der Kraaij, A., Zsamboki, B., 'The rise of artificial intelligence: benefits and risks for financial stability', Financial Stability Review, European Central Bank, May 2024.

[84] Georgieva, K., 'AI Will Transform the Global Economy. Let's Make Sure It Benefits Humanity', IMF Blog, 14 January 2024.

[85] Cazzaniga, M., Jaumotte, F., Li, L., Melina, G., Augustus J.Panton, A.J. et al, 'Gen-AI: Artificial Intelligence and the Future of Work', IMF, January 2024.

[86] Acemoglu, D., Johnson, S., 'Power & Progress. Our 1000-Year Struggle Over Technology & Prosperity' p. 297-338, Public Affairs, New York, 2023.

[87] Aziz, M.H., 'The overlooked global risk of the AI precariat', World Economic Forum, 20 August 2025,

[88] Jaokar, A., 'The Digital World Towards 2040. The Rise of AI & Intelligent Autonomy. What does it mean for Europe?', European Internet Forum, 2024.

[89] Hoos, H. (interview), 'AI Replacing Humans? The Truth About GPT-5, Jobs & Creativity', Youtube, Ones Changing the World, 31 August 2025.

[90] Ryan, R.M., Deci, E.L., 'Self-Determination Theory', Encyclopedia of quality of life and well-being research, 2022.

[91] 'Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, The European Startup and Scaleup Strategy: Choose Europe to start and scale', COM (2025) 270 final, 28 May 2025.

[92] Green., M, Smith. M., 'Developers are Not the Enemy!: The Need for Usable Security APIs', IEEE Security & Privacy, vol.14, no. 5, pp. 40-46, September – October 2016.

AN INTER-INSTITUTIONAL EU PROJECT

Acknowledgements: The preparation of this paper was a collaborative exercise drawing on the knowledge and expertise of colleagues across the EU institutions and bodies, contributing to the interinstitutional ESPAS project. Sincere thanks to the ESPAS Steering Group for their guidance and direction. The authors of this paper are: Beata Kolecka, Igor Nai Fovino, Patricia Arias Cabarcos, Gary Steri, Ignacio Sanchez and Adam Lewis. They were supported by the interinstitutional project group led by Beata Kolecka including G. Carter, O. C. Dumitrescu, R. Kuenzel, R. Ugolotti, W. Vandevelde as well as L. Bontoux, O. Nagy, P. Goran, S. d'Ambrosio and T. Tamer. The paper was developed through a series of brainstorming sessions, a foresight workshop involving experts from the ESPAS institutions and bodies as well as external ones, and insights obtained in interviews and consultations. The latter involved: V. Šucha, S. Kadhi, O. Diez, C. Huet, J. Heikkila, F. P. Carli as well as A. E. Jauregui and C. Monti.
Published November 2025.