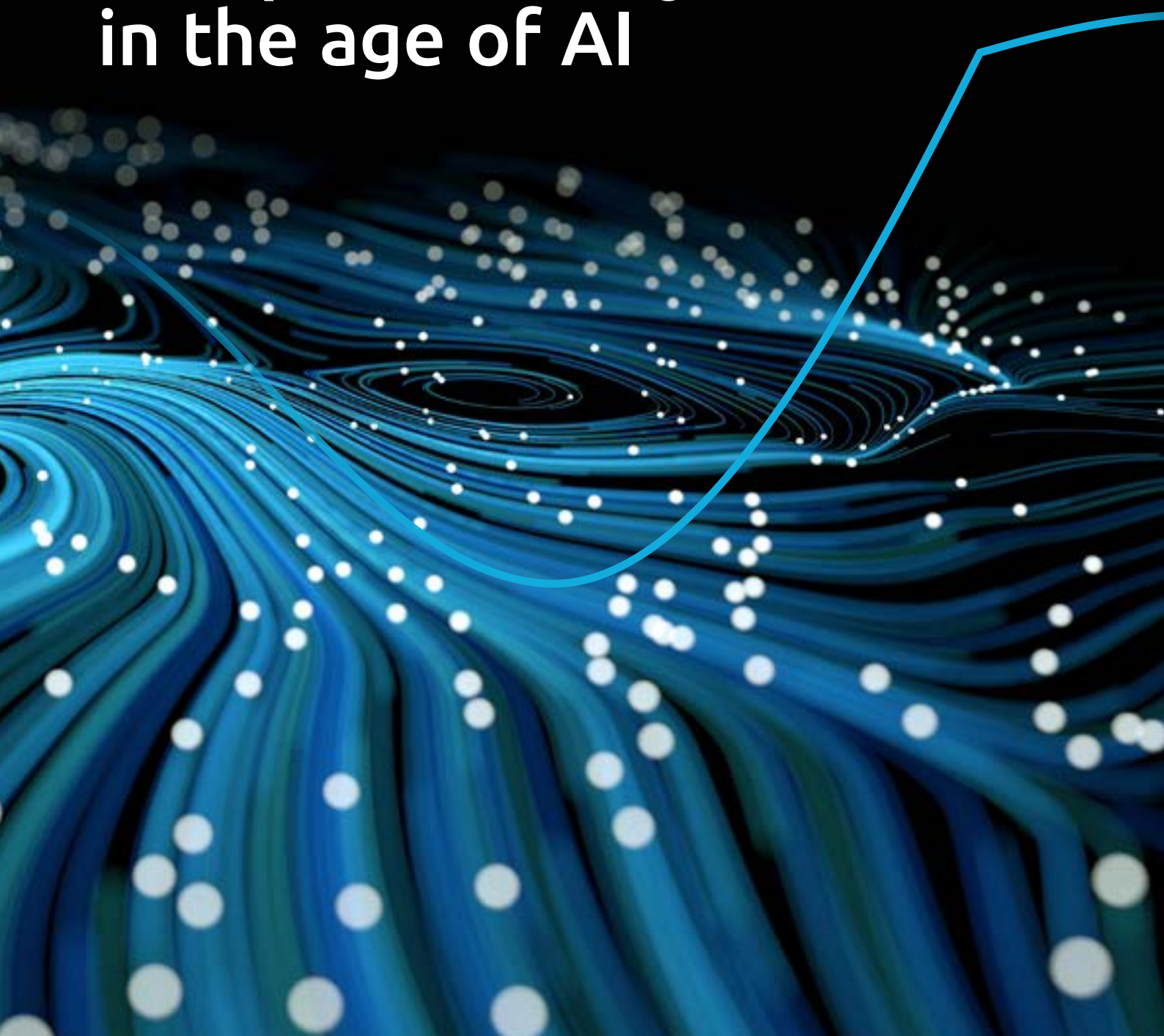
Capgemini

Software is eating Defense

Safeguarding Europe's Security in the age of AI



The world is undergoing a profound geopolitical and technological transformation. Artificial Intelligence has changed defense, and post-quantum cryptography will be essential to protecting its future.

This report provides leaders with a roadmap to navigate this critical juncture and harness the potential of technology to safeguard Europe's strategic autonomy and resilience.

Published on the occasion of the Munich Security Conference 2025

Table of contents

Foreword

Andreas Conradi,
Head of Defense Europe
& Executive Vice President, Capgemini

National security and defense have never been more critical in the face of unpredictable, rapidly evolving threats. And it is the role of cutting-edge technologies, seamlessly integrated across every aspect of defense, that is enabling the industry to address emerging challenges with unmatched agility and precision.

The concept of 'software eats defense' underscores the growing importance of software and digital solutions as strategic drivers of innovation. Governments and armed forces now face not only traditional weaponry but also the weaponization of technology—tools readily exploited by adversaries and increasingly embedded within domestic security infrastructures. Staying ahead and securing the future calls for a forward-looking vision where digital solutions are central to strategic advancements, enhancing capabilities, resilience, and agility in a rapidly evolving landscape.

Nowhere is this more evident than in the emergence of artificial intelligence (AI) and quantum computing (QC). In a relatively short time, the velocity and volume at which AI processes information have become critical to military decision-making, serving as a guiding force in helping armed forces navigate the fog of war. Meanwhile, QC is a rapidly emerging technology capable of obliterating even the most robust security defenses by today's standards.

The convergence of these disruptive yet transformative technologies provide national defense with two invaluable assets. However, it also presents adversaries with two powerful tools for attack—attacks that can unfold quickly, are difficult to detect, and can cause widespread damage in an instant.

To capitalize on the opportunities presented by AI and QC, while future-proofing defense capabilities, we need to operate with the most stringent security standards. Understanding the origins and training of AI, as well as ensuring it remains immune to adversarial influence, is more critical than ever. With the arrival of QC on the horizon, we should confidently act to secure critical and sensitive information. This should not be measured by today's encryption standards, but rather with the question: "Is this 'quantum safe'?"

Securing the future of our democracies requires proactive steps, as conflict will persist, adversaries will mobilize, and AI and QC will continue to evolve. To best prepare for future challenges, we can call on the strategic, innovative, and technological excellence available in the industry to:

Accelerate innovation and embrace transformative technologies like AI and QC

Strengthen technology sovereignty to create the right conditions for technology to thrive

Enhance trust and interoperability by maintaining the highest security standards

Act with urgency to ensure readiness for the future state of conflict

Dr. Benjamin Schulte,
Strategy & Innovation Lead Defense Europe, Capgemini

The transformation of defense and security, driven by new software-defined capabilities, is characterized by a critical tension: the imperative for openness and rapid experimentation with emerging technologies clashes with the necessity of securing these advancements against adversaries, inherent risks, and new occurring vulnerabilities. Proactive adoption and continuous innovation are vital to deter aggression, protect our democracies, and ensure enduring security in an increasingly complex world.

While new technologies should be explored and integrated swiftly, safeguarding their integrity and operational security is equally essential. Against this dynamic backdrop, our report examines the transformative potential of AI and quantum technologies in defense, emphasizing how AI can revolutionize decision-making and autonomous operations while quantum advancements promise unbreakable encryption and enhanced secure communications.

Executive summary

Our world is in the midst of profound societal, technological and geopolitical change.

Our world is in the midst of profound societal, technological and geopolitical change. European leaders are being required to rethink their strategy to reflect a shift to a multipolar world, the re-emergence of high-intensity conflict, and the transformative impact of technology on security, strategic autonomy, and European resilience. The stakes are high, with implications ranging from strategic planning and innovation management to battlefield tactics.

The notion of "software is eating the world" also holds true for defense and security as the recent events in Ukraine have demonstrated. Thus, it can be said that "software is eating defense", with a growing appetite and ever-accelerating pace. Defense innovation historically focused on hardware, especially platform centric capabilities such as tanks, aircraft, and ships.

Today's alpha and omega is the interplay of software-defined and hardware-enabled capabilities, shaping future systems, operations, and decision-making. This shift unlocks unprecedented opportunities and introduces new vulnerabilities that should be proactively managed. The transformative power of Artificial Intelligence (AI) and the emerging threats from quantum computing demand an urgent, coordinated and strategic response. Without robust defense, societies face greater risks of manipulation, threatening stability, sovereignty, and democracy.

Artificial Intelligence is transforming the operational landscape across critical domains, serving as a catalyst for national security, public safety, infrastructure resilience, and crisis management. It enhances decision-making, situational awareness, and predictive capabilities, reshaping how governments, organizations, and industries address security challenges. AI brings with it complex challenges related to data management, supply chains, cybersecurity and human oversight, demanding increasing attention to the secure uses and implementation of the technology.

In parallel, post-quantum cryptography (PQC) offers the protection of the digital foundation upon which AI and other critical systems rely. As quantum computing advances, it threatens current cryptographic systems, endangering secure communications, critical infrastructure, and operational continuity. Unlike AI, PQC may not revolutionize security operations but provides the essential backbone for safeguarding their integrity. The interplay between these technologies is clear: while AI catalyses transformative capabilities, its effectiveness depends on the foundational security provided by PQC. Without this protection, AI's power to enhance security and resilience becomes a potential liability.

Europe's strategic autonomy in a multipolar world will hinge on its ability to navigate the convergence of AI's transformative impact and PQC's protective potential. The secure integration of these technologies will ensure seamless coordination among allies and fortify Europe against hybrid threats and adversarial capabilities. As digital transformation accelerates, the interplay between AI and PQC should be harnessed to strengthen Europe's technological sovereignty and resilience.

This report assesses the security implications of AI integration and PQC adoption in defense and security, emphasizing their interconnected roles in securing Europe's strategic future. It concludes with actionable recommendations for Europe's political, military, and industrial leaders to:

Accelerate innovation and operational integration.

Strengthen technological sovereignty.

Enhance trust and interoperability.

Summary of recommendations

Accelerate innovation and integration	Target Audiences		
Adopt a balanced approach between risk-tolerance and ethics to testing emerging technological solutions			
Adapt procurement procedures to the short development cycle of information technologies			
Train and develop AI systems with realistic, high-quality synthetic data			

Strengthen technological sovereignty	Target Audiences		
Increase domestic production of critical components to reduce external dependencies			
Task an EU agency to coordinate and centralize expertise, streamline adoption, and drive standardization in emerging technologies			
Improve the training and anticipate the need for security and defense workforce in line with the requirements of a rapidly evolving technological landscape			

Enhance trust and interoperability	Target Audiences		
Develop a transatlantic “common data strategy” to facilitate the sharing of AI training data			
Develop a transatlantic shared approach to AI and quantum ethical development and use			
Establish a standardized, robust AI development and management framework for interoperability between allies			

Key  Armed forces |  Policy-makers |  Defense industry

Europe at a technological crossroads

General (ret.) (OF-9) Eric Autellet
Former Major General of the French Defense Staff

We stand today at a critical juncture, witnessing a convergence of societal transformations, technological breakthroughs and geostrategic changes. Europe's strategic context is undergoing a significant transformation and evolving dynamics which require new mindsets, strategies and partnerships. While some principles remain unchanged, tangible aspects like recent technological advances (AI, cloud computing, big data), changing geopolitical context, and societal development are transforming the security and military sphere.

Power and interactions are shifting from global to regional scales, redefining international relations and prompting leaders to prioritize regional security, autonomy and resilience.

The integration of emerging technologies without strategic foresight risks undermining Europe's sovereignty, potentially leading to serious technological and strategic disruption. A balanced and cohesive approach to technology deployment is therefore essential.

The increasingly widespread use of digital assets is now enabling permanent competition, unexpected confrontations and new ways of fighting. Europe has yet to master the digital domain, which will be the next arena for confrontation and war between states. In the near future, the bloc's efforts must focus on on mastering new technologies, in particular the transition to post-quantum cryptography, ensuring that it is not caught off-guard by progress in this domain. It is also urgent to cohesively map European research and development efforts to address these challenges head-on.

Introduction

Is software eating defense?

The world is undergoing a profound transformation driven by rapid technological change. Technology is reshaping society and accelerating change at an unprecedented pace, bringing both significant benefits and challenges. As global power dynamics shift, nations race to secure an edge in this new context of high intensity and high technology. The military domain is increasingly defined by software. While tanks, aircraft, and ships were once the core focus of innovation, software now drives transformation, shaping operational systems, decision-making processes, and overall defense strategies.

Where should we focus today to secure our way of life in the future? New challenges arise every day, some of which may not have even been envisaged just a few years ago. Are we sufficiently aware of these changes, and, more importantly, able to tackle them effectively? What can we do today to mitigate future threats?

AI: transformation or upheaval?

AI is transforming the operational landscape in numerous areas, acting as a catalyst for innovation. To enable it to continue being driving force for innovation and transformative change in national security, public safety, infrastructure resilience and crisis management, its uses should be secured in the long term.

However, this technological advance also introduces complex challenges ranging from AI-powered cyber-attacks to algorithmic biases, either inherent to the data used to train AI systems or maliciously introduced by adversaries to "poison" the data and render the AI ineffective. Secure implementation of AI-driven systems is thus fundamental to mitigate associated risks and ensure that AI improves operational efficiency while protecting and being protected against potential vulnerabilities. These foundational transformations are forcing a profound rethink of our security and defense.

Time to act

This report addresses the strategic, future-defining challenges posed by secure AI and PQC for security and defense, offering a roadmap for political, military, and industrial leaders to act decisively to secure Europe's future. It provides a comprehensive understanding of current and emerging challenges and presents actionable recommendations to inspire proactive measures. As Benjamin Franklin aptly noted, "By failing to prepare, you are preparing to fail." The time to act is now.

It is essential to balance investments in Gen AI with those in cybersecurity and quantum technologies to address current risks effectively."

Patrice Duboé
Executive Vice President / Chief Technology & Innovation Officer - Aerospace & Defense, Capgemini

The future of European security hinges on our mastery of transformative technologies. AI and quantum innovations hould be deployed with precision and responsibility."

Dr. Cara Antoine
Chief Technology, Innovation & Portfolio Officer / Executive Vice President | Capgemini

Quantum: the next challenge

The evolution of the AI-augmented battlefield makes secure communication essential. PQC will play a pivotal role in securing the digital infrastructure that AI and digital systems rely on against emerging threats posed by quantum capabilities. While these applications for now remain theoretical, they hold the potential to disrupt secure communications on a massive scale, rendering current encryption protocols obsolete and jeopardizing military operations. PQC will provide the necessary foundation for maintaining the integrity the digital backbone of future operations.

Quantum computing could render secure communication impossible overnight. Command would thus no longer be possible and secure operations would collapse. Such a catastrophic scenario is not inevitable. PQC can be deployed now on IT and communications systems, reducing the threat to data lost now and systems in the future. PQC operates on classical rather than quantum computers, and thus provides a practical solution today to address the significant threats posed by tomorrow's quantum and computation power advances.

This report will examine these two key trends, their potential impact on the future of software-defined capabilities, and the strategic responses leaders should consider capitalizing on opportunities while addressing associated risks. Drawing on qualitative research, including expert interviews with distinguished defense professionals from European armed forces, NATO, the European Defense Agency, and technology and innovation experts at Capgemini, the report will offer actionable recommendations for strengthening AI security and safeguarding quantum technologies in the years to come.

Securing AI to secure Europe

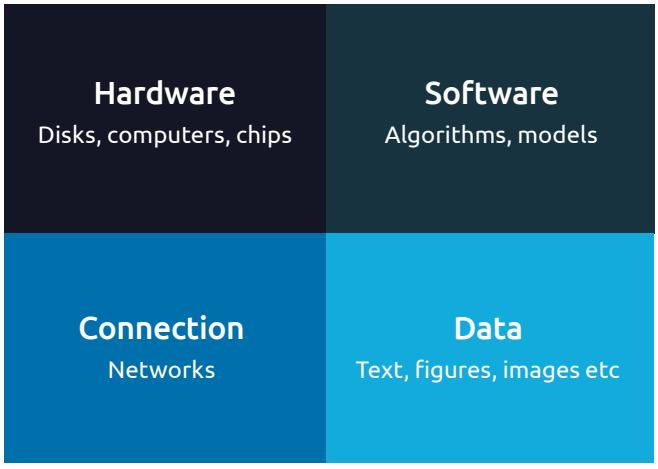
AI is a catalyst for transformation and has led to a revolution in national security, public safety, critical infrastructure, and military operations. It enhances decision-making, situational awareness, and predictive capabilities, enabling proactive responses to evolving threats. AI applications span autonomous systems, targeting and decision support, predictive analytics, and cyber defense, among others.

The conflicts in Ukraine and the Middle East have highlighted the growing pervasivness of AI and its accelerated integration into a variety of systems and platforms, such as Unmanned Aerial Vehicles (UAVs), targeting processes, or the analysis of satellite imagery. The conflicts in Ukraine and the Middle East have showcased the increasing pervasivness of AI and accelerated integrationinto into a variety of systems and platforms, such as Unmanned Aerial Vehicles (UAVs), weapons targeting systems, or the analysis of satellite imagery. This chapter looks at current and upcoming applications of AI and focuses on how to ensure safe and secure uses of AI.

Artificial Intelligence refers to the ability of machines to perform tasks traditionally requiring human intelligence, such as recognizing patterns, learning from experience, drawing conclusions, making predictions, or generating recommendations. These applications may guide or alter the behavior of autonomous physical systems (like automated vehicles) or operate entirely within the digital domain (e.g. ChatGPT), with autonomy ranging from partial human intervention to full independence post-activation.

Source: U.S. Department of State (2023)

Four elements of AI



AI applications in security and defense

Artificial intelligence is already a major tool in a range of critical security and defense areas. It is already transforming all operational domains (land, sea, air, space, cyber, electromagnetic spectrum) and the way missions are conducted (from anticipation to detection and reaction). By multiplying effects (e.g. swarming) and increasing battlefield transparency, AI is offering added value across all functions. Its applications span military operations, military support, disaster prevention and humanitarian aid, intelligence, homeland security and border management.

AI will specially improve **decision support** in all the areas of security and defense. At the **strategic level**, AI will be able to analyze action plans, issue early warnings and help produce simulations to guide operational planning. At the **operational level**, it already processes intelligence to prioritize and validate targets. At the **tactical level**, AI provides real-time data and actionable intelligence to optimize immediate responses.

> *As AI continues to mature, we can expect further disruptions in military operations. The journey towards AI integration is already well underway."*

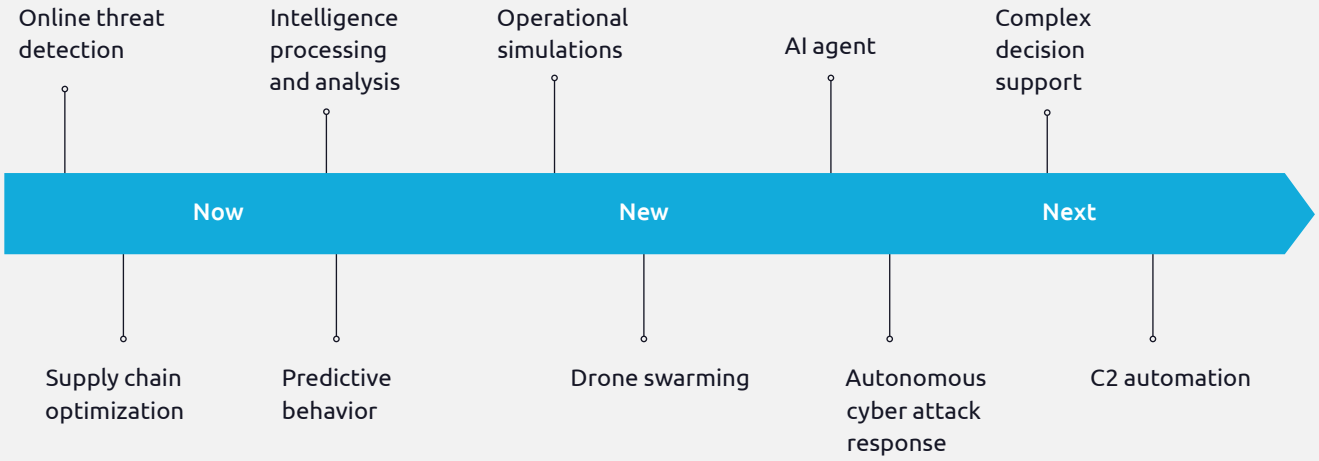
Dr. Bryan Wells
NATO Chief Scientist

The conflict in Ukraine: a testbed for AI

AI is playing a central role in supporting Ukrainian forces in intelligence, operational support and targeting. In the field of counter-espionage, AI systems, in collaboration with companies such as Palantir, analyze vast datasets to identify threats to national security, flagging suspicious behavior of Ukrainian citizens or their potential links with Russia. Moreover, AI is integrated with voice translation tools that process intercepted enemy communications, extracting actionable intelligence to anticipate adversary movements.

In the field of operational support, the Operations Centre for Threat Assessment (COTA), leveraging AI, integrates various data streams, providing real-time information to guide logistics and strategy. Finally, AI improves target acquisition, analyzing drone and social media data to locate and neutralize targets of strategic value on a daily basis.

Current, emerging, and future AI applications



Risks to secure AI uses and mitigation strategies

AI impacts all operational domains, military functions if not the very nature of warfare. Securely implementing and using AI poses specific challenges linked to technology, people and process. This also requires a clear balance between the need to rapidly implement AI in the fields of defense and security while navigating the challenges related to this implementation. These challenges can be structured in four main categories: cybersecurity, supply chain security, data, as well as expertise and human resources, and require targeted mitigation strategies.

Challenges and mitigation strategies

Key challenges to the integration of AI in defense and security can be tackled by a number of mitigation strategies, structured in four main categories: cybersecurity, supply chain security, data, as well as expertise and human resources.

Domain	Challenge	Mitigation strategy
System security	AI is vulnerable to attack	• Harmonize security standards to mitigate threats on AI systems, including model poisoning, oracle attacks, and input perturbation • Increase collaboration between the public and private sectors to strengthen AI against adversarial attacks and improve the cyber security of hardware and software from the R&D to the implementation phase
Supply chain security	Strain on the supply chain/disruptions	• Invest in developing European semiconductor production capabilities to reduce external dependency. • Encourage partnerships with European industry, academia, and research institutions to mitigate risks from strategic competition
Data	• Lack of quality and quantity of data • Difficulty obtaining and sharing data (encrypted, classified, incomplete) • Data requiring advanced storage and processing capabilities • Data poisoning	• Develop a sovereign Cloud for securing sensitive data while guaranteeing compliance with national security protocols • Integrate, in the future, fully homomorphic encryption, enabling classified data to be shared and processed securely without decrypting • Create data centers to meet the sector's growing computing and storage needs. • Use synthetic data in situations where it is impossible to obtain data, in particular to anticipate future scenarios
Expertise and human resources	• Cognitive biases (e.g. automation bias) • Excessive reliance on AI outputs • Obligation to respect international humanitarian law • Maintaining meaningful human control over the use of force • Necessity to trust the AI system	Enhance human oversight and expertise through: • (Re)training programs • High-level expertise cultivation • Integration of technical specialists into military and security operations

Cyber and supply chain security

The secure implementation of AI for defense and security faces important obstacles in cybersecurity and supply chain security. For instance, hostile actors could exploit vulnerabilities in AI systems through deceptive data inputs ("data poisoning") during the development stage, or by targeting the model itself.[1] Because these techniques are not only persistent and evolving threats, but also highly sophisticated and difficult to detect, NATO's AI Strategy highlights that they put critical infrastructure and sensitive operations at risk.[2]

Rising global demand for semiconductors and microchips further strains AI supply chain security, as production is limited by long lead times, complex and capital-intensive design and manufacturing processes, and can be subject to geopolitical tensions.[3] The high costs associated with designing new chips mean that economies of scale are essential, leading to the concentration of production between a few leading companies. A few countries dominate these supply chains, raising concerns about reliance, strategic leverage, and espionage. The U.S., for example, has restricted exports of advanced chips and manufacturing equipment to China,[4] highlighting the importance of controlling critical supply chains for the secure use of AI in security and defense, especially for states without independent supply chains of their own.

AI systems' security should be strengthened throughout their lifecycle. This includes fortifying AI against hostile actors' attacks and improving the (cyber) security of the associated hardware and software. Governments are investing heavily in domestic semiconductor production to reduce dependence on foreign suppliers.[5] The European Union's adoption of the €43 billion European Chips Act, which aims to produce 20% of the world's semiconductors by 2030 in the EU, is one such example.[6]

Cooperation between the public and private sectors is essential to securing AI for security and defense. NATO's AI strategy highlights partnerships with industry, academia, and research institutions to advance technological capabilities, safeguard intellectual property, and mitigate risks from adversarial use or strategic competition.[7] These efforts, aligned with the Munich Security Conference's call for strengthened semiconductor and AI coordination, aim to foster innovation and ensure Europe's access to vital AI components.[8]

We need to get end users and operators into capability development, for clearer operational needs and agile capability development with direct feedback from the theater. This means rethinking how we develop software-defined, hardware-enabled capabilities."

Dr. Benjamin Schulte
Strategy & Innovation Lead Defense Europe, Capgemini

Europe needs to strengthen its European champions to remain digitally sovereign."

Dr. Christian Weber
Principal, Partner Lead and Client Manager Defense, Capgemini Insights & Data Germany

Integrating the results of start-ups into the traditional procurement and industrial world remains a major Challenge."

Andreas Conradi
Head of Defense Europe / Executive Vice President, Capgemini

Data

Data is another major challenge, first and foremost the quantity and quality of available data. Training military AI systems relies on accurate, relevant and AI-ready data for the adequate fulfillment of their functions, but this can be difficult to obtain.[9] Furthermore, the vast quantities of data generated (for example by sensors and collaborative combat operations) require advanced storage and processing capabilities, which are not always available, especially at the edge. These limitations pose significant operational challenges on platforms such as submarines, tanks, and other vehicles where computational resources are highly constrained. Military AI systems depend on access to encrypted or classified data, which adds another layer of complexity and raises the question of who can access and use this sensitive data. Finally, the risks of data poisoning and adversarial manipulation—where attackers corrupt training or test datasets to reduce the performance of AI models—further raise the stakes because of the grave consequences that erroneous AI outputs can have in military settings.[10]

One solution is to develop sovereign cloud infrastructure[11] to secure sensitive defense data in compliance with national and regional security protocols.[12] The future integration of fully homomorphic encryption is another significant step, as it will enable classified data to be shared and processed securely without decryption, protecting critical information even in cooperative situations.[13] The creation of vast data centers with a capacity in excess of one gigawatt is another crucial milestone towards meeting the sector's growing computing and storage needs. These facilities would make it possible to process operational data at an unprecedented scale, while guaranteeing its security and availability.[14] Investing in these strategies could vastly improve data security management and lay a solid foundation for the implementation of secure AI across the defense and security sectors.

The use of synthetically generated data effectively addresses many challenges. It can fill the gap where real data is unavailable or provide lower-classification data for initial model development, enabling a smoother transition to higher-classification environments.

Additionally, synthetic data is often indispensable for preparing AI to handle real-world scenarios that have yet to occur, such as zero-day cybersecurity threats. By simulating battles or unprecedented situations, synthetic data enables training for both AI systems and personnel. To be effective, however, this data should closely mirror real-world conditions, requiring a high degree of "equivalence" to ensure reliability.[15]

> *A commonly used solution to mitigate paucity of data is the use of synthetically generated data."*
>
> **Dr. Mark Dorn**
> Director Defense, Cambridge Consultants

Expertise and human resources

The integration of AI decision-support systems into military and security applications raises issues around human-machine interaction. Secure AI implementation requires high ethical, legal, and human decision-making standards, which should provide the flexibility required to continually incentivize and nourish innovation rather than stifle it.

Key concerns center on human control over the use of force and the mitigation of cognitive biases, such as over-reliance on automated systems while disregarding contradictory information (automation basis), which may distort decision-making.[16] Operators may inadvertently ignore the legal and strategic implications of their decisions and cause errors or unintended outcomes. Integrating AI will also expand internal attack surfaces, as personnel may misuse AI.[17] On the technology end, AI systems can have difficulty adapting to dynamic wartime conditions.[18] The U.S. DoD's Project Maven is a case in point, struggling to independently identify an enemy vehicle under different weather conditions than those it was originally trained on.[19] AI adoption in a military context risks contravening international humanitarian law, in particular the principles of distinction, necessity, humanity and proportionality, which underpin the lawful conduct of hostilities.[20]

Strategies to enhance human oversight and expertise should be developed, complemented by the right skillsets for military and civilian operators to responsibly interact with AI. At the transatlantic level, NATO has, for instance, set up a Data and Artificial Intelligence Review Board (DARB) to provide common standards for interoperability and principles of responsible use of AI.[21]

Strategies will also imply implementing retraining programs, cultivating high-level expertise and further integrating technical specialists into military operations to ensure that AI applications comply with national, international and humanitarian law, and also with specific rules of engagement,[22] and developing a global culture of documented research and evidence-based decision-making.[23]

In defense, the trust factor is crucial. Soldiers and military personnel need to trust the AI systems they're using, just as they would trust any other tool in combat. That's why it's important to invest in AI literacy and ensure users understand how to use these systems responsibly."

Martijn van de Ridder MSc
Vice President | Lead Data & AI Defense Europe

NATO's view on artificial intelligence

Major General Dominique Luzeaux, Dr. Hab.
Digital Transformation Champion and Special Advisor to SACT

In the continually evolving landscape of modern warfare, operational success hinges on effective connectivity and authoritative data management. Recognizing this imperative, NATO has embarked on a comprehensive Digital Transformation initiative. By 2030, this transformation will empower Multi-Domain Operations through enhanced interoperability, heightened situational awareness, and data-driven decision-making. AI emerges as a critical enabler, ensuring the adaptability and readiness of the Military Instrument of Power in the face of future military challenges.

One primary objective is the development of new platforms and systems, fostering interoperability, and creating a unified ecosystem where all allies have equitable access to AI capabilities. This will be achieved through expanded AI access, introducing novel services to the existing service catalogue, including AI-enabling services (data availability, AI Infrastructure as a Service, AI Platform as a Service) and AI services based on Commercial Off-the-Shelf (COTS) AI products and accessible Large Language Models (LLMs).

Specific AI/Machine Learning models are being developed for advanced threat detection. Concurrently, investments are being made in counter-AI technologies to safeguard the integrity and correctness of AI-supported processes and to counter potential adversary attacks on vulnerable AI methods.

The deployment of AI in military warfare presents significant ethical, legal, and moral dilemmas, raising concerns about accountability, responsibility, transparency, and the potential for escalation, miscalculation, and unintended consequences in complex and dynamic environments. To address these challenges, NATO has formulated an AI strategy, outlining six key principles:

1. Lawfulness: Adherence to all applicable laws, regulations, and policies.
2. Responsibility and Accountability: Those involved in the design, development, deployment, or operation of AI systems must remain accountable for their functioning and impacts.
3. Explainability and traceability: The processes employed in the development and training of AI models must be meticulously documented and auditable.
4. Reliability: AI systems must consistently produce reliable and robust results, resistant to manipulation or errors.
5. Governability: The use of AI must remain under human control, with the capability to intervene in automated processes as necessary.
6. Bias mitigation: Rigorous efforts must be undertaken to minimize unwanted bias in the development and deployment of AI systems.

The Technology Readiness Level (TRL) of generative artificial intelligence (AI) systems is generally assessed to be between TRL 7 and TRL 8. This assessment indicates that prototypes of generative AI systems are currently operational and demonstrate their functionality in relevant environments.

While significant advancements have been made in areas such as large language models, opportunities remain to further enhance accuracy, coherence, and creativity. The substantial computational resources required for the training and deployment of large-scale generative AI models necessitate advancements in both hardware and software infrastructure. Moreover, the quality and quantity of training data significantly impact the performance of these models, highlighting the importance of access to high-quality datasets for developing robust and reliable systems. As ongoing research addresses these technological challenges, we can anticipate the emergence of more sophisticated and impactful generative AI applications in the few coming years.

Global trends in AI R&D

Breakthroughs in AI have driven innovation across various domains, especially in machine learning (ML), deep learning (DL) or natural language processing (NLP), and automating basic functions (speech-to-text tools, contextualized translation, summarization).

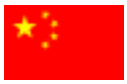
United States

The United States is the dominant power in AI R&D, backed by increased AI-related funding from the Department of Defense (DoD), from $190 million in 2022 to $557 million in 2023.[24] The DoD's November 2023 AI Adoption Strategy aims to integrate AI across military functions.[25] It requires the alignment of strategic objectives with training the workforce for appropriate AI use.[26] The synergy between government and the private sector has kept the US at the forefront of technological advancements ahead of China and Russia.

Finally, in January 2025, the US government announced "The Stargate Project", a private joint venture involving OpenAI, Oracle and foreign investment funds, aiming to invest up to $500 billion over the next four years in infrastructure for AI. The objective of this project is to ensure the country's independence, but also to assert its supremacy in the field of AI, by mastering the necessary physical infrastructures. [27]

Key takeaways

- Market leader in AI R&D
- Leader in private investment volume in AI
- Considerable number of start-ups in the field
- Substantial investment by the government (DoD)



China

China strives for global AI dominance by 2030.[28] Chinese sources claim the country's core AI industry reached a market size of 578.4 billion RMB while growing at 13.9% in 2023.[29] China's "military-civilian fusion" program drives advances in robotics and autonomous technologies by integrating civilian innovations into military applications. This top-down strategy aligns national security goals with targeted productivity plans at both national and local levels.[30] China produced the highest number of publications on AI in 2023,[31] narrowly outpacing the US with 12,450 publications on generative AI compared to the U.S.'s 12,030.[32]

Key takeaways

- Strong government support
- Aims to become the dominant power in AI by 2030
- Leader in scientific publications on generative AI

Russia

Russia is prioritizing AI investments to accelerate military modernization. The Ministry of Defense's Main Directorate for Innovative Development (GUIR) coordinates a network of research institutes, techno-parks and innovation centers to promote dual-use technologies.[33] Since 2021, GUIR has launched over 500 initiatives in command systems, unmanned vehicles and cyber operations. Russia's AI programs are smaller in scale than those of the US or China, and constrained by insufficient funding, corruption and inefficiency.[34] These structural problems limit Russia's ability to take full advantage of emerging technologies, even when there is a focus on specific areas, primarily electronic warfare and psychological operations.[35] Since its invasion of Ukraine in 2022, Russia has put its AI capabilities to the test in combat situations, particularly in geospatial intelligence, unmanned missile operations, military training, and cyber warfare.[36]

Key takeaways

- Priority given to the military sector
- Strong government coordination of R&D efforts
- Suffering from insufficient fundings, corruption, and inefficiency

EU

The **EU** is striving to progressively increase AI investment and R&D through the European Defense Fund (EDF). The EDF supports a €100 million program for an AI-enabled drone equipped with advanced intelligence and €25 million for military 5G networks.[37] National initiatives complement EU-level efforts. France, for example, plans to deploy Europe's most powerful supercomputer in 2025 to boost defense AI capabilities.[38] Moreover, the French Ministry of Armed Forces allocated €2 billion to the development of AI for national security,[39] and created the Agency for Defense Artificial Intelligence (AMIAD) in 2024. However, Europe's private sector is much less developed than its American or Chinese counterparts, and relies on a few major start-ups, such as Germany's Helsing which specializes in AI-based defense software.[40]

Key takeaways

- Increasing investments from the EU
- Development of national initiatives to boost R&D
- An ecosystem hampered by a small number of major start-ups

Shaping security for the quantum age

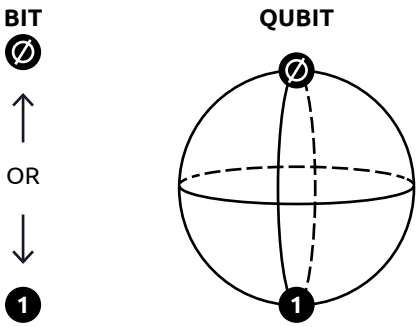
Increasingly "intelligent" AI-powered systems require more secure architectures. Post-quantum cryptography (PQC) is emerging as a key protection measure, supporting the ongoing transformation of Europe's security and defense. As AI continues to reshape these domains, PQC ensures the security of the digital infrastructure supporting AI and other critical systems. It addresses the risks posed by advances in computational power, including quantum computing, protecting sensitive communications and systems from future threats. While AI is already a key enabler in security and defense, quantum computing remains in its early stages, with practical applications only beginning to emerge. The evolution of quantum computing underscores the urgency of adopting PQC to guarantee the long-term protection of key digital systems and communications.

Quantum computing leverages principles from quantum mechanics (a branch of physics), notably the unique behaviors of subatomic particles such as electrons and photons, to enable new, extremely powerful computing architectures.

Source: Information Technology and Innovation Foundation

Instead of processing information **using binary bits of ones and zeros**, quantum computers use **"quantum bits" (qubits) which utilize superposition and entanglement to operate in multiple states at once.** This allows quantum computers to store vastly more information than binary systems.

Source: Information Technology and Innovation Foundation



Security in the quantum age

Quantum computing (QC),[41] with its enhanced computational power far exceeding that of classical computers, promises to solve complex problems in unprecedented ways.[42]

Its anticipated uses range from the creation of new materials, pharmaceuticals, precise financial predictions,[43] traffic optimization or energy transport, to name but a few. Quantum technology could also help secure cyberspace by creating theoretically unbreakable exchange networks. Conversely, cybercriminals using quantum algorithms could break current encryption systems in just a few hours. QC is expected to see initial applications by 2030-2035.

As quantum computation capabilities progress, post-quantum cryptography (PQC) has emerged as the primary solution to secure digital infrastructure against quantum threats. PQC,[44] also known as quantum-resistant cryptography, will be essential to protect against quantum threats that could compromise existing cryptographic methods.[45] Unlike quantum key distribution (QKD),[46] PQC does not rely on quantum mechanics, making it well-developed, commercially available, and already undergoing standardization in the U.S. Today's main concern is "harvest now, decrypt later" attacks, where encrypted data is captured and stored today in the hope of decrypting it once quantum computers are powerful enough.[47] With the looming threat of all encryption methods becoming obsolete,[48] it is vital to prioritize the development and integration of PQC to secure Europe's sensitive data and communications.

As quantum technology progresses, its applications become increasingly tangible across various sub-domains. There remain significant challenges in transitioning from research to practical deployment. Quantum computing, while demonstrating specific advantages, faces major obstacles in error correction and scalability,[49] delaying breakthroughs critical for military and cryptographic implications[50] by at least a decade. Military applications of quantum technologies remain speculative, requiring further maturation and analysis of their operational potential. As a 2020 RAND report concluded, "some niche applications of quantum computers are being explored that may become useful within the next few years, but the most important applications (such as breaking decryption) are likely at least ten years away."[51]

"NATO is spending a lot of time raising awareness among Allies on the consequences of having part of their cryptography obsolete for command and control."

Dr James Appathurai
Assistant Secretary General for Innovation, Hybrid and Cyber, NATO

PQC is a priority today, and after the standards are released by NIST this summer, there is no good reason to delay migration any longer."

Julian van Velzen
Head of Capgemini's Quantum Lab

The following table presents a broad overview of the sub-areas of quantum technology, with Technology Readiness Level (TRL)[52] and time horizons, for context:

Technology		TRL	Horizon
Sensing & imaging	Quantum inertial navigation	4-5	2025-2030
	Quantum clocks	4-6	2030
	Quantum radar	1-2	None
	Quantum RF antenna	4	2025-2030
	Quantum magnetic and gravity sensing	5-6	2025
	Quantum imaging	5	2025-2030
Communication & cryptography	Quantum key distribution	7-8	2025
	Post-quantum cryptography	7-8	2025
	Quantum communication network	1-3	2030-2035
Computing & simulation	Quantum computer	4-5	2030

Technology Readiness Level (TRL) and time horizon expectations
Source: Krelina (2021)

Critical factors in quantum computing advancements

Quantum memory

The number of qubits of memory computers have.

Information loss

The extent of "noise" during operations, understood as the information loss that increases computational errors.

Quantum stabilization

The measure of how long qubits maintain their state before losing information.

Challenges and mitigation strategies

Key challenges to the integration of PQC and quantum technologies development in defense and security can be tackled by a number of mitigation strategies, structured in four main categories: cybersecurity and supply chains, data, and expertise and human resources.

Domain	Challenge	Mitigation strategy
Cyber security	Uncertainty of adversary quantum mastery Prevalence of asymmetric cryptography Uncertainty about the impact of quantum technologies on the security and defense industries	• PQC adoption in governmental and strategic industries' systems • Standardization efforts to safeguard cybersecurity standards overtime • Development of transition roadmaps for PQC adoption • Impact assessment on strategic industries/infrastructures
Supply chain security	Safeguard strategic subcomponent providers	• Support strategic industries that are technological enablers for quantum technology development • Increase domestic capacity in providing these strategic components
Operationalization	Integration with legacy military systems Risk of operational disruption	• Assessment of potential impact and vulnerabilities • Assessment of adversaries technological development
Expertise and Human Resources	The number of researchers or publications does not directly lead to more patents or reflect a thriving start-up ecosystem	• Maintain high degree of public support • Centralization effort to avoid duplications in quantum computing R&D • Support private investment • Have a patent strategy • Support domestic research

Quantum computing faces critical challenges which require timely and strategic mitigation to ensure secure and seamless adoption. An important concern is the cybersecurity threat it poses. While quantum computing is still in its infancy, as is mastering millions of logical qubits, the threat of "harvest now, decrypt later" is of urgent concern. Most modern cryptographic algorithms, which rely on the complexity of mathematical problems (public-key, asymmetric cryptography) or the obstacle of finding the exact private key (symmetric cryptography), are vulnerable to attacks by quantum computers.[53] Asymmetric cryptography, widely employed in applications such as VPNs, email encryption, digital signatures, and online communications, will be particularly vulnerable to quantum attacks as quantum computers are expected to solve complex mathematical problems within the next decade.[54] As the threat grows, calls for immediate PQC adoption are increasing, and the U.S. is already taking the lead through NIST. Specialists express concern about the lack of standardization cooperation within NATO and between the EU and the US, especially for industries requiring secure long-term data storage.

As in the case of AI, **supply chain security** is a critical issue which should urgently be addressed.[55] Europe is an important producer of key technological components such as lasers, which are foundational to quantum computing. To secure Europe's supply chains, strategic industries (semi-conductors, photonics, cryogenics, precision sensing) which are technological enablers for quantum technology should be supported. An EU-wide quantum industry strategy aiming to increase domestic capacity in the production of critical components would reduce dependency on external suppliers, strengthen Europe's position in the quantum technology ecosystem. Safeguarding key production capabilities could strengthen transatlantic quantum cooperation, promoting greater innovation.

The **operationalization** of quantum technologies is uniquely challenging because their practical applications in defense are yet to be fully characterized. Integrating these emerging capabilities with legacy military systems is a complex process fraud with vulnerabilities and risks operational disruption. To address these challenges, a rigorous assessment of potential impacts and vulnerabilities is essential. Fostering research collaboration at NATO level could enhance efficiency, while monitoring and evaluating the technological advancements of adversaries will help anticipate risks and inform strategic decision-making. By proactively addressing uncertainties, defense stakeholders can ensure that quantum technologies are integrated effectively when they mature, while maintaining operational readiness and resilience.

Building **expertise and human resources** in quantum technologies will require more than simply increasing the number of researchers or publications. After all, these metrics do not necessarily translate into patents or a thriving start-up ecosystem. To address this, it is vital to maintain strong public support for quantum R&D, combined with efforts to centralize R&D and minimize duplication. Expanding industry-led internship and professional development programs, and ensuring more efficient and rapid patent applications, could further foster innovation and protect intellectual property. Strengthening transatlantic collaboration in workforce development can help address the talent gap and create a stronger, interconnected quantum ecosystem.[56] Additionally, sustained support for domestic research is essential to develop a skilled workforce and establish a dynamic quantum start-up ecosystem which can serve as an incubator for long-term growth and technological leadership.

NATO has established the ransatlantic Quantum Community, a unique and innovative structure that brings together academics, industry, and government representatives to foster quantum technologies development."

Dr James Appathurai
Assistant Secretary General for Innovation, Hybrid and Cyber, NATO

We need to align academic research with defense priorities and create better incentives for talent to contribute to the military sector. Partnerships with startups and academic institutions could help bridge this gap."

Julian van Velzen
Head of Capgemini's Quantum Lab

NATO's view on quantum technologies

Major General Dominique Luzeaux, Dr. Hab.
Digital Transformation Champion and Special Advisor to SACT

In late 2023, NATO ratified a Quantum Strategy that establishes a framework to position the Alliance as quantum-ready. Current endeavors are centered on forming a quantum community.

The overarching objective is to harness the potential of quantum technologies while mitigating associated risks. The strategy underscores the transformative and disruptive implications of quantum technologies, with a particular emphasis on:

1. **Quantum Sensing for Positioning, Navigation, and Detection:**
   Quantum sensors, distinguished by their exceptional precision, resolution, and sensitivity, have the potential to revolutionize future battlefields. By enabling sensing and surveillance capabilities across various domains and conditions (day/night, adverse weather, GNSS outages), they offer a significant advantage. Additionally, techniques such as ghost spectroscopy, which leverages quantum principles to extract spectral information without direct light interaction, are particularly valuable for detecting faint or elusive objects, such as CBRN materials.

2. **Quantum-Safe Communications and Networking:**
   The integration of Quantum Key Distribution (QKD) and post-quantum encryption offers robust security for communications and networks. QKD, along with complementary technologies like Quantum Random Number Generators (QRNG), and potentially future entanglement-based networks, can underpin secure communications, facilitate interconnections between quantum computing centers, and enable advanced networking capabilities.

3. **Quantum Information Science (QIS):**
   QIS encompasses the research and development of quantum computers (QCs) and their associated software ecosystem, including algorithms, cryptography, programming languages, modeling, simulation, and diverse knowledge applications. Quantum computers are designed to tackle computationally intensive problems, excel in modeling and simulation, and significantly enhance decision-making and operational effectiveness within NATO operations. Future advancements in quantum computing may lead to the development of a Cryptographically Relevant Quantum Computer (CRQC), capable of compromising current public-key cryptography and more efficiently attacking systems reliant on short symmetric keys.

The Technology Readiness Level (TRL) of quantum technologies varies depending on the specific application. Most are currently considered to be at TRL 3 (proof of concept) to 6 (system/subsystem model or prototype demonstration in a relevant environment).

While significant strides have been made in quantum computing, a fully functional, universal quantum computer that can solve complex problems beyond the reach of classical computers is not yet available. Noisy intermediate-scale quantum computers could be available by 2030, optimized for specific classes of algorithms. Full-scale fault tolerant computing should not be achieved before 2040.

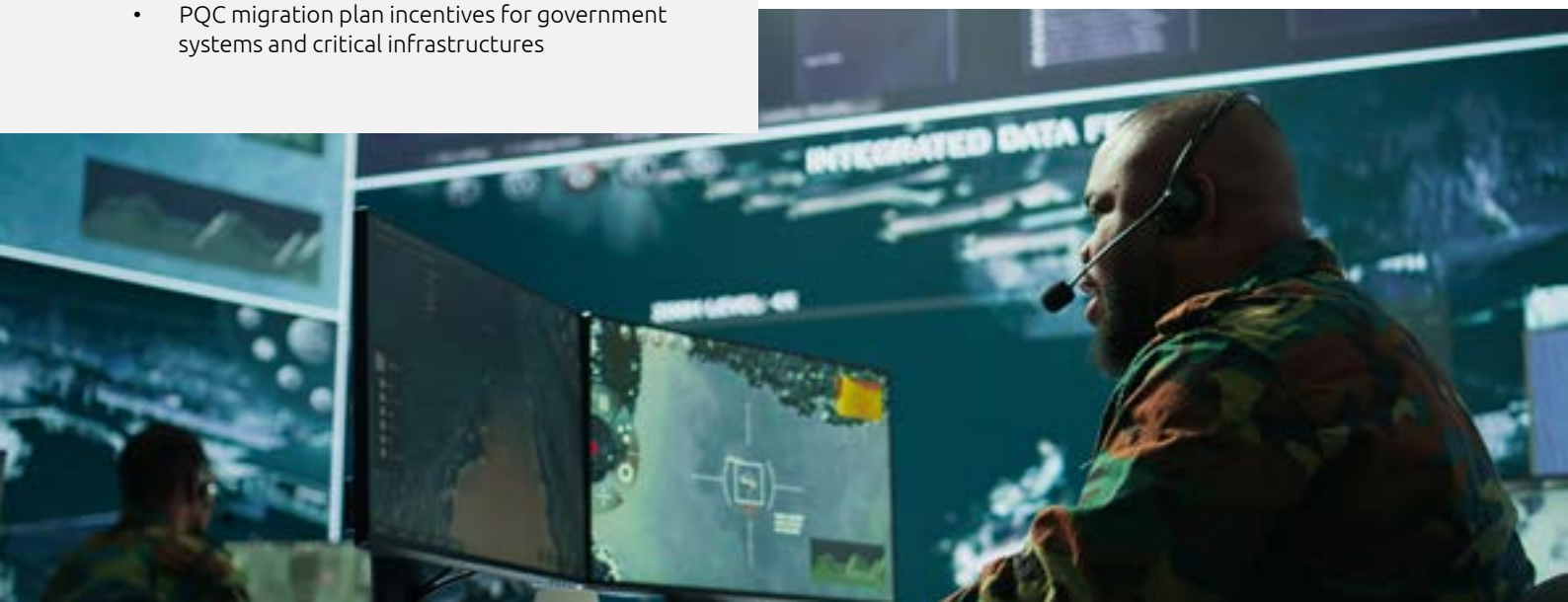
Global trends in quantum and post-quantum cryptography R&D

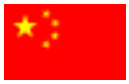
United States

The United States currently leads the pack in quantum computing and sensing.[57] Progress is primarily driven by collaboration among academic institutions, private enterprise, and government under the National Quantum Initiative Act (2018). The largest quantum computers have been built in the U.S. by leading companies such as Google, IBM, Honeywell, Microsoft, and heavyweights in a thriving start-up scene (IonQ, Rigetti, ColdQuanta, PsiQuantum). Through its active engagement in quantum standards development, the U.S. is able to influence global practices via the National Institute of Standards and Technology (NIST), which released the first three post-quantum encryption standards in August 2024.[58] In November 2024, NIST published an initial roadmap for PQC transition, which evaluates the long-term viability of existing cryptographic algorithms. The roadmap clarifies that many current algorithms will be deemed deprecated after 2030 and be disallowed by 2035 for national security reasons.[59] While the U.S. excels in quantum computing, its development of quantum communication systems lags behind China due to lower prioritization and market interest.[60]

Key takeaways

- Market leaders in quantum computer development
- Leader in private investment
- Strong push for PQC standardization
- PQC migration plan incentives for government systems and critical infrastructures





China

China has prioritized quantum communication[61] and computing among its top three national research goals since 2016.[62] China leads the world in quantum communication with over $15 billion in government funding, surpassing other countries despite lower private sector investment.[63] In 2016, it launched the Micius satellite, the first to enable quantum communication with the ground, and established a vast fibre-optic network for QKD in what is considered a step towards advancing a large-scale quantum network.[64] Micius served as a relay for a first-ever quantum encrypted intercontinental video conference between Vienna and Beijing in 2017, demonstrating a major milestone in the development of a global satellite-based quantum internet.[65] While China's quantum ecosystem is dominated by state-owned companies and large technology firms such as Huawei and Tencent, the number of Chinese start-ups in the quantum field has gradually increased as well.[66]

Key takeaways

- Leaders in quantum communication development and testing
- Strong government support
- Highly concentrated technological ecosystem

EU

Alongside AI, biotechnology and advanced chips, the European Union recognized, in 2023, the critical character of quantum technologies.[67] The EU's approach to funding quantum technologies is decentralized,[68] with investment stemming from national governments, the European Commission, and public-private partnerships.

This collaborative strategy encourages Member States to engage in quantum research and innovation but risks duplication of efforts. The EU leads in public funding with nearly €10 billion announced as of 2023.[69] The focus is on supporting start-ups, establishing a federated quantum infrastructure, and creating a coordinated action plan to prevent cybersecurity loopholes.

The EU leverages its strong research capability[70] and state-of-the-art technology capabilities. Indeed, the Union accounts for 44% of total patents granted in quantum computing and provides the U.S. with specialized components (e.g. lasers and electronics) mainly from Germany, France, Italy, Finland and Sweden.[71] The EU however lags behind its global competitors in private investment, with $548 million recorded for the period 2001-2023, compared to $3.58 billion in the U.S. and $745 million in the UK.[72] EU Member States have recently acknowledged the importance of transitioning to PQC in a joint statement of 18 national cyber security agencies.[73]

Key takeaways

- Leader in research publications
- Important subcomponents provider
- Strong government support
- Decentralized approach risking duplication of efforts

AI and quantum technologies at the service of democratic stability and security

Lt. General Stefano Cont
Capability, Armament and Planning Director,
European Defence Agency

Accelerating innovation: a blueprint for transformative technologies

The European Defence Agency provides support to Member States to enable collaborative capability development as well as defense research, technology, and innovation to prepare the future of EU defense. EU capability development tools include proposals for next generation capabilities, for instance via the Capability Development Plan (CDP) and the Coordinated Annual Review on Defense (CARD,) and leverage work related to the Action Plan on emerging and disruptive technologies (EDTs) for defense applications linked with AI and PQC.

The successful development of the Hub for EU Defence Innovation (HEDI) to develop demonstrators and experimentation could be further enhanced by promoting a risk-tolerant strategy designed to push the boundaries of technology and foster groundbreaking advancements. It could operate by funding high-risk, high-reward projects which traditional funding mechanisms may avoid, emphasizing the pursuit of transformative rather than incremental innovation (DARPA-like approach).
A combination of visionary ambition, the freedom to explore unconventional ideas and an adaptive funding mechanism may better position EDA to tap into the innovation potential that exists in the European Defence Technological and Industrial Base (EDTIB) and beyond, thus driving technological breakthroughs, with greater expected impact on defence capabilities, closer and faster to the military end-user.

From neutral to purposeful: application defines dual-use technologies

The concept of dual-use technologies refers to innovations which can be applied for both civilian and military purposes. A dual-use technological approach demonstrates how a fundamentally neutral innovation can take on different characteristics depending on its application.

Such technologies, agnostic in their essence, can be employed in civilian contexts then adapted to military uses. The key to their characterization lies not in the technology itself but in the intent and purpose of its application. This underscores the necessity for the Agency to continue cooperating with other EU institutions, bodies, and agencies in all relevant activities related to dual-use technologies. These two reflections may be instrumental for the preparation of the EU White Paper on the Future of European Defence.

Strategic recommendations

The challenges linked to secure building blocks and uses of AI and quantum computing are substantial and far-reaching. Transversal and multi-dimensional by nature, they cannot be effectively addressed in isolation, but require a whole-of-government, whole-of-society approach. Political and regulatory action will be essential to develop a solid, reliable framework to drive innovation while safeguarding the future.

With the advent of software-defined defense the military will have to rethink doctrine, execution of operations and adapt procurement strategies to evolving realities.

The industrial sector has an equally pivotal role to play in providing expertise, working hand-in-hand with end users to provide them with the platforms and systems needed in an AI-driven, post-quantum setting.

Charting a secure path to the future, **the following recommendations are aimed at Europe's political, military, and industry leaders** and span key areas such as data management, training, testing, expertise, and procurement. Recommendations are structured according to three overarching objectives:

Accelerate innovation and integration

Strengthen technological sovereignty

Enhance trust and interoperability

Accelerate innovation and integration	Target Audiences
Adopt a balanced approach between risk-tolerance and ethics to testing and integrating emerging technological solutions	
Adapt procurement procedures and design and manufacturing processes aligned to the short development cycle of software and AI-defined capabilities	
Train and develop AI systems with realistic, high-quality synthetic data	

Strengthen technological sovereignty	Target Audiences
Increase domestic production of critical components to reduce external dependencies	
Task an EU agency to coordinate and centralize expertise, streamline adoption, and drive standardization in emerging technologies	
Improve the training and anticipate the need for security and defense workforce in line with the requirements of a rapidly evolving technological landscape	

Enhance trust and interoperability	Target Audiences
Develop a transatlantic "common data strategy" to facilitate the sharing of AI training data	
Develop a Transatlantic shared approach to AI and quantum ethical development and use	
Establish a standardized, robust AI development and management framework for interoperability between partner countries	

Key  Armed forces |  Policy-makers |  Defense industry

Accelerate innovation and integration

For NATO, this is a once in a generation chance to address one of its top priorities: accelerating the adoption of new technologies. NATO is leaning in hard, engaging with industry and innovation leaders, to develop a set of proposals that will substantially enhance the speed of adoption."

Dr James Appathurai
Assistant Secretary General for Innovation, Hybrid and Cyber, NATO

END GOAL

Speed up development processes

HOW

Adopt a balanced approach between risk-tolerance and ethics to testing emerging technological solutions.

European military forces should embrace the testing of emerging technological solutions that are not yet fully matured. This willingness to experiment with "imperfect" solutions can provide valuable operational insights which will likely better guide further R&D efforts, and thus accelerate the adaptation of cutting-edge technologies to meet operational needs. AI and software factories—a framework designed to efficiently develop, scale, and operationalize AI use cases while enabling the agile creation of new AI applications—could offer a way forward for defense organizations.

END GOAL

Speed up procurement processes

HOW

Adapt procurement procedures to the short development cycle of information technologies.

The speed of innovation cycles, particularly in AI and software development, has outpaced current procurement procedures—shifting from decades to just a few years. This mismatch poses a risk to Europe's operational readiness and effectiveness in an increasingly fragile world.

The conflict in Ukraine has shown that technological innovations can be adopted within six to twelve weeks, highlighting the need for faster adoption cycles."

Dr James Appathurai
Assistant Secretary General for Innovation, Hybrid and Cyber, NATO

HOW

Decentralize innovation and put the end-user front and center

Military stakeholders, such as battalion and brigade commanders, should be encouraged to engage directly with industry, including start-ups and non-traditional defense players, to generate a direct feedback loop. The Ukrainian army exemplifies how enabling local commanders to directly work with innovators in real-time can lead to quick integration of technology and deployment in the field, showcased by Ukraine's use of autonomous drone swarm operations, open-source intelligence, battlefield and intelligence data analysis and AI-driven training simulations.[74]

Another advantage would be to familiarize the military with the economic realities of industry. Adopting iterative development and testing encourages active involvement of the military sector in the crucial early innovation stages. This way, user requirements can be fine-tuned according to the military's experience in the theatre of operations, which greatly increases the chances of a capability development program being brought to high maturity.

END GOAL

Improve AI defense systems' efficiency

HOW

Train and develop AI systems with realistic, high-quality synthetic data.

Synthetic data sets replicate real-life data without compromising sensitive information. It offers a solution to the lack of structured classified data for specific military operational scenarios. For certain operational scenarios, no real-life data exists (yet), and synthetic data could bridge the gap.

Using synthetic data would allow continuous, tailored AI training and testing. By leveraging synthetic data, armed forces can accelerate innovation, overcome data scarcity, and maintain a technological edge while safeguarding interoperability.

Strengthen technological sovereignty

END GOAL

Secure strategic productions

HOW

Increase domestic production of critical components to reduce external dependencies.

The EU should invest in manufacturing capacity of essential components, such as quantum processors, semiconductors, and data infrastructure to reduce its dependence on overseas manufacturing hubs. The conflict in Ukraine laid bare the vulnerabilities of supply chains. These threaten Europe's high-tech industry and the very development of AI and quantum technologies. Italy's strategy of offering billions in incentives to attract foreign high-tech manufacturers is paying off, with Singapore's Silicon Box setting up a factory in Piedmont. This approach could inspire similar efforts in other EU countries in a crucial step towards more European technological sovereignty.

END GOAL

Speed up EU-wide technological adoption and PQC migration

HOW

Task an EU agency to coordinate and centralize expertise, streamline adoption, and drive standardization in emerging technologies.

This new or readily existing agency could provide clear guidelines, milestones, and timelines—such as preparing for critical transitions like the migration of security systems to PQR as in the US—along with certifications and training. The agency could help consolidate and effectively distribute financial resources towards AI and quantum R&D. This would make European funding more effective by shifting from many small programs to fewer, more focused initiatives, leveraging the EU's extensive expertise and helping improve its global standing in the AI and quantum fields.

END GOAL

Reduce dependency on foreign specialists, minimize operational errors, and mitigate potential risks

HOW

Improve the training and anticipate the need for security and defense workforce in line with the requirements of a rapidly evolving technological landscape.

Security and defense personnel should be provided with rigorous and continually updated specialized training. Besides the traditional military field craft of maneuver and tactics and new dimension of so-called tech craft, the knowledge about emerging and digital technologies and the ability to leverage them and impact operations becomes equally important. Upskilling programs and academy approaches as well as new ways for strategic personnel planning can help close the skill gap in defense organizations. Establishing dedicated units and roles to oversee the use of emerging technologies like AI and quantum computing could furthermore help in providing staff with guidance and accountability.

Enhance trust and interoperability

END GOAL

Ensure interoperable AI defense systems at NATO level

HOW

Develop a transatlantic "common data strategy" to facilitate the sharing of AI training data.

NATO allies should adopt a common transatlantic training data strategy to address critical barriers like classified data access and the overall quality of available data for training AI models, while also embracing new cryptography solutions based on homomorphic encryption and data sharing.

END GOAL

Establish harmonized guidelines on the use of AI in security and defense

HOW

Develop a transatlantic shared approach to AI and quantum ethical development and use.

Transparency is the bedrock upon which to build trust in new technologies. European leaders should ensure that the permissible use cases and the ways new technologies are integrated into military systems are clearly communicated. In the case of AI, for example, this requires AI systems to be trained according to clearly established rules, regulations, and ethical considerations. This ensures political accountability in democratic systems, allowing verification that armed forces and their use of AI align with established principles, which in turn can help boost trust in the AI models used.

As nations advance their own capabilities, ensuring seamless communication and interoperability between systems is essential to sustain operational cohesion and effectiveness"

Dr Bryan Wells
NATO Chief Scientist

END GOAL

Strengthen "AI assurance" within the Alliance

HOW

Establish a standardized, robust AI development and management framework for interoperability between partner countries.

European defense stakeholders should ensure that AI models can be explained to politicians and citizens. The framework should include a thorough threat assessment early in the process to identify risks, mitigation needs, and project viability while guiding subsequent steps like testing and data security. The model should be regularly monitored and adapted to changing conditions or adversarial responses for continuous improvement. Together, these practices will ensure AI systems remain effective, secure, and reliable throughout their lifecycle.

Conclusion: software eats defense is the new reality

As software and AI increasingly drive innovation in defense and permeate military capabilities, creating intelligent and secure defense systems becomes a critical priority for a robust digital backbone. Against this backdrop, this report focuses on two interconnected challenges of this paradigm shift: the need to enhance AI security while simultaneously strengthening quantum-secure communication, in order to unlock the potential and transformative power of increasingly software-defined capabilities. Indeed, NATO has called this a "once-in-a-generation chance" to accelerate the adoption of transformative technologies.

By reimagining how defense organizations operate, innovate, design, and integrate novel technologies, new capabilities can be deployed swiftly, making a significant impact on the operational environment. However, AI systems should be secured against emerging vulnerabilities, while communication networks and the entire technology stack should be made quantum-secure now.

Meeting these needs, however, requires a holistic approach, from strategy and design through testing, training and full end-to-end transformation. Capgemini's deep expertise in both digital technology and physical engineering, strengthens the design, development, and implementation of intelligent and secure solutions across the whole defense value chain; from the theatre to the production shop floor. A safer world cannot rely on the efforts of a single government, defense supplier or technology company. It demands an ecosystem approach where each stakeholder contributes to innovation and progress.

By collaborating with a broad network of defense organizations, startups and leading technology firms, Capgemini offers a cohesive platform for transformation. This interface simplifies solution delivery, speeds up deployment and supports the rapid development and secure integration of software- and AI-defined capabilities, ensuring maximum impact where it matters most. To address our new reality of software-defined defense, we believe in adopting an approach that seamlessly integrates the digital and physical worlds, building smart, intelligent capabilities to safeguard our way of life and deter future conflicts.

This is not a challenge for the future—it requires our attention and action today. We are dedicated to supporting the defense sector in its mission to adapt, innovate and create a safer, more resilient future. Our European heritage also drives our strong commitment to the defense of the continent we share.

Contributors

The report is based on in-depth desk research and qualitative interviews with defense, AI and quantum experts, including from Capgemini.

James Appathurai
Acting Assistant Secretary General for Innovation, Hybrid, and Cyber

James Appathurai is NATO's Acting Assistant Secretary General for Innovation, Hybrid, and Cyber, leading a global team addressing critical areas such as cyber defense, emerging technologies, and hybrid threats. His division focuses on safeguarding NATO's innovative edge by fostering advancements in artificial intelligence, quantum computing, biotechnology, and other disruptive technologies to tackle security challenges that were previously insurmountable.

James's extensive career at NATO includes serving as Deputy Assistant Secretary General for Political Affairs and Security Policy, Special Representative to Central Asia and the Caucasus, and NATO Spokesperson from 2004 to 2010. Prior to joining NATO, he worked in Canada's Defense Department.

General (ret.) (OF-9) Eric Autellet
Former Major General of the French Defense Staff

Eric Autellet has over 30 years of experience in the French Armed Forces, excelling in operational leadership, international collaboration, and strategic planning. His career includes serving as Major General of the Armed Forces (2021), overseeing inter-branch coordination and military readiness, and playing a critical role in key international operations, such as Operation Inherent Resolve in Iraq and Kuwait.

Eric's academic accomplishments include graduating from École de l'Air and advanced studies at the Centre des Hautes Études Militaires (CHEM) and the Institut des Hautes Études de la Défense Nationale (IHEDN). His expertise in defense strategy and his operational excellence have earned him recognition as a Commander of the National Order of Merit and an Officer of the Legion of Honor.

Dr. Cara Antoine

Executive Vice President | Chief Technology, Innovation & Portfolio Officer

Dr Cara Lenore Antoine is a renowned global leader, innovative speaker, and bestselling author, who is passionate about creating positive change in society, the economy and our planet. A technology advocate, education champion and empowering executive, Dr. Antoine enables people and organizations to achieve their full potential in the digital era. With three decades of dedicated experience, Dr. Antoine is a powerful agent of growth and transformation, driving impact at the intersection of technology and humanity.

As the Executive Vice President and Chief Technology, Innovation & Portfolio Officer of Capgemini Europe, Dr. Antoine strategically advises global corporations in the C-Suite across industries on applying innovation to drive and accelerate digital and cultural transformation.

Andreas Conradi

Executive Vice President | Head of Defense Europe

Since March 2023 Andreas has been Executive Vice President and Head of Defense Europe at Capgemini. As such, he is responsible for Capgemini´s business with the Defense Industry as well as Defense Ministries and Armed forces in Europe and NATO. Andreas is a proven defense sector expert with sustained successful track record as top official at the helm of the German Ministry of Defense including as Chief of Staff to Defense Minister Ursula von der Leyen. Based on more than two decades of experience, he has a deep understanding of the structure and function of the public and private defense sector in Europe including the set-up and management of national and international armament programs.

Lt. General Stefano Cont

Capability, Armament and Planning Director, European Defence Agency

Lt. General Stefano Cont is the European Defence Agency's Capability, Armament, and Planning Director, leading efforts to enhance Europe's defense capabilities and technological edge. His leadership spans critical domains, including strategic planning, capability development, and international defense cooperation, ensuring the resilience of European defense systems in the face of evolving challenges.

Lt. General Cont's distinguished military career includes commanding fighter and fighter training squadrons in both Italy and the United States, with over 3,400 flying hours as a command and instructor pilot. He served as the Commander of the 61st Flight Training Wing and Lecce Air Base from 2006 to 2008. He held key positions such as Defense Attaché to the United States, Mexico, and Canada, where he advanced international military collaboration and defense procurement.

His expertise extends to strategic advisory roles, including Head of the Political-Military Office in the Italian Ministry of Defense, where he shaped national defense strategy, industrial policy, and international relations. His academic accomplishments include advanced degrees in Aeronautical Sciences, Political and Military Sciences, International Strategic Studies, and National Security Strategy, complemented by a doctorate in International and Diplomatic Sciences.

Dr. Mark Dorn
Director Defense | Cambridge Consultants

Mark has worked for 30 years providing technology and advice to clients within the defense research, procurement and the industrial supply chain. His focus in recent years has been leading research on the application of AI, to aid military operations. He has also led the development of leading-edge AI solutions to applications such as cybersecurity and autonomy. He recognizes the need to engender Trust in AI and has delivered projects advising clients on approaches to understand the risk to AI, demonstrate technology to monitor and explain AI and develop tests for the algorithms.

Patrice Duboé
Executive Vice President | Chief Technology & Innovation Officer - Aerospace & Defense

Patrice Duboé has been working in Innovation & Technology for more than 30 years in multicultural environments. After leading the Global Capgemini Architects Community, he is now Innovation Executive Vice President and CTIO for Capgemini S&C Europe and for the Global AeroSpace & Defense Industry. He is leading Innovation & Technology teams to deploy Innovation at scale for global corporation & clients with key partners and emerging startups.

Being passionate about sustainable Innovation, IOT, Telecom and Smart Energy, he has also founded a startup, www.leanconnected.com, to deliver autonomous telecom stations providing solar energy & data connections for isolated territories.

Major General Dominique Luzeaux, Dr. Hab.
Digital Transformation Champion and Special Advisor to SACT

Dominique Luzeaux has over 30 years of experience in defense engineering, focusing on complex systems, digital transformation, and advanced technologies. His career spans leadership roles in military acquisition, system engineering, and digital strategy, including serving as Director of the Digital Defense Agency from 2021 to 2023, overseeing key defense digital projects. Dominique Luzeaux's academic achievements include degrees from École Polytechnique and École Nationale Supérieure des Techniques Avancées, alongside a PhD in artificial intelligence. He has also published extensively, with nine books and over 100 articles on topics such as nanotechnology and systems engineering.

Martijn van de Ridder MSc
Vice President | Lead Data & AI Defense Europe

With more than 2 decades of experience in data and AI and more than a decade experience in public security and defense, Martijn is dedicated to help public sector organizations maximize the value of data and AI and transform into data-driven organizations. Amongst others, he advises Chief Data Officers on data & AI strategy definition, implementation and execution driving innovation and growth to data mastery through cutting-edge data and AI solutions. Martijn's mission is to leverage data and AI to improve decision-making, operational readiness, and overall information position for defense organizations across Europe.

Dr. Benjamin Schulte
Strategy & Innovation Lead | Defense Europe

With over 19 years of experience in the defense sector and a PhD in Innovation & Technology Management, Benjamin is a seasoned expert dedicated to driving innovation in defense. After serving as an army officer for 15 years in the German Federal Armed Forces, he now directs the Strategy and Innovation stream in Defense Europe. In this role, he leads the defense innovation ecosystem in Europe, connecting the innovation power of Capgemini and its technology partners with defense clients. His expertise includes developing innovation and technology strategies, conceptualizing and designing new solutions and ventures, and integrating new technologies into operational capabilities, ensuring impactful advancements in defense.

Julian van Velzen
Head of Capgemini's Quantum Lab

Julian is the Head of the Capgemini quantum lab; a global network of quantum experts, partners and facilities focused on three key areas: Sensing, Communication and Computing. From this Lab, Capgemini is exploring and building the path towards a quantum advantage with its clients for business and societal problems that, up until now, are seemingly intractable. Julian has a background in condensed matter physics from the University of Amsterdam, he is part of the group CTIO community, he is the Dutch representative of the European quantum consortium (QuIC), and member of the Forbes Technology Council.

Dr. Christian Weber
Principal | Partner Lead and Client Manager Defense, Capgemini Insights & Data Germany

Christian is an expert in digital innovation and generative AI, specializing in critical application areas within the public sector and industry. These sectors face particularly high demands for IT security and digital sovereignty. His work focuses on ensuring the safe and trustworthy application of the latest AI technologies. Christian draws on his extensive and long-standing experience across military, political, academic, and industrial domains to achieve these goals.

Dr. Bryan Wells
NATO Chief Scientist

Bryan Wells is NATO's Chief Scientist, leading the organization's efforts in science and technology innovation and policy. In this role, he chairs the NATO Science and Technology Board, advises NATO leadership on scientific advancements and their strategic implications, and oversees the Office of the Chief Scientist at NATO Headquarters. His work is critical in ensuring NATO remains at the forefront of technological innovation to address modern security challenges.

Dr. Wells joined NATO in 2019 following an accomplished career in the UK Ministry of Defense, where he served as Head of Science and Technology Policy, Strategic Research, and International Engagement. He has also held prominent roles such as Chair of the European Defense Agency's Research and Technology Steering Board, Deputy Director of NATO Policy, and Director of Counter-Proliferation and Arms Control. Dr. Wells is an Oxford-educated chemist, with a DPhil and postdoctoral research at Merton College.

Leveraging the expertise from Cambridge Consultants, the deep tech powerhouse of Capgemini.

www.cambridgeconsultants.com

This report has been developed in collaboration with ForwardGlobal.

Axel Dyèvre, Senior Partner

Pauline Massard, Partner

Johannes Feige, Senior Consultant

Maxime Huilliard, Consultant

Lucas Keller, Consultant

www.forwardglobal.com

Bibliography

Anderjung, M., et al. (2024). *Computing Power and the Governance of AI, Center for the Governance of AI*, https://www.governance.ai/post/computing-power-and-the-governance-of-ai

Araya, D.(2022). *Artificial intelligence for Defense and Security, Center for International innovation*, https://www.cigionline.org/static/documents/Araya_AI-for-Defence_SpecialReport_Q4fjNfp.pdf

Araya, D., King, M. (2022). *The Impact of Artificial Intelligence on Military Defense and Security, Center for International innovation,* https://www.cigionline.org/static/documents/no.263.pdf

Australian Army (2021), *Army Quantum Technology Roadmap*, https://researchcentre.army.gov.au/sites/default/files/RD5734_Quantum%20Roadmap%20WEB.pdf

Austrian Academy of Sciences (2018), *Secure quauntum communication over 7,600 kilometers,* https://www.oeaw.ac.at/en/news-1/secure-quantum-communication-over-7600-kilometers-2

Avalos, R., S., Gonzales, F., Ortiz, T., *Responsible use of AI for public policy: Data science toolkit, IADB*, https://publications.iadb.org/en/responsible-use-ai-public-policy-data-science-toolkit

Amazon Web Services (date NA)., *What is Deep Learning?,* https://aws.amazon.com/what-is/deep-learning/?nc1=h_ls

Bang, A., Kamal, K. K., Joshi, P., Bhatia, K. (2023). *6G: The Next Giant Leap for AI and ML*, Procedia Computer Science, Volume 218, pp. 310-317, https://doi.org/10.1016/j.procs.2023.01.013

Bode, I., Nadibaidze, A., Zhang, Q. (2024), *AI in Military Decision Support Systems*, Center for War Studies, https://usercontent.one/wp/www.autonorms.eu/wp-content/uploads/2024/11/AI-DSS-report-WEB.pdf

Bondar, K. (2024). *Understanding the Military AI Ecosystem of Ukraine*, Center for Strategic and International Studies (CSIS), https://www.csis.org/analysis/understanding-military-ai-ecosystem-ukraine

Bradshaw, T., Kinder, T. and Pfeifer, S.(2024). *German AI defense start-up Helsing poised to triple valuation to $4.5bn,* FT, https://www.ft.com/content/e09f813b-e568-4afe-8e07-940a707595ca

Bundesamt für Sicherheit in der Informationstechnik, et al. (2024), *Securing Tomorrow, Today: Transitioning to Post- Quantum Cryptography,* https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/PQC-joint-statement.pdf?__blob=publicationFile&v=5

Calais, S., Tay, J. (2024). *Generative AI hardware - the other arms race,* A&O Shearman, https://www.aoshearman.com/en/insights/generative-ai-hardware-the-other-arms-race

Callegari, A., Li, C.(2024), *Stopping AI disinformation: Protecting truth in the digital world,* WEF, https://www.weforum.org/stories/2024/06/ai-combat-online-misinformation-disinformation/

Cambridge Consultants, *Pioneering AI cyberattack response for the UK military*, https://www.cambridgeconsultants.com/project/pioneering-ai-cyberattack-response-for-the-uk-military/

Capgemini (2024), *TechnoVision: Top 5 Tech Trends to Watch in 2025*, https://www.capgemini.com/wp-content/uploads/2024/11/11_27_Capgemini-Top-5-Tech-Trends-2025-Press-Release.pdf

Chen, C.(2021), *The future is now: artificial intelligence and anticipatory humanitarian action*, ICRC, https://blogs.icrc.org/law-and-policy/2021/08/19/artificial-intelligence-anticipatory-humanitarian/

China Industrial Daily (2024). 人工智能发展持续蓬勃向前 AI大模型成为未来产业新赛道 (The development of artificial intelligence continues to thrive, with AI large models emerging as a new frontier in future industries), http://www.ciia.org.cn/news/25369.cshtml

Cohen, R. and Mihalka, M. (2001). *Cooperative security: New horizons for international order.* The Marshall Center Papers, Number 3, https://www.marshallcenter.org/sites/default/files/files/2020-04/mc-paper_3-en.pdf

Dickson, J. and Harding, E. (2024), *Unleashing Quantum's Potential, Center for Strategic and International Studies*, https://www.csis.org/analysis/unleashing-quantums-potential

Dijkstra, E. (2024), *Quantum and Military Communication Security : An Analysis of the Opportunities, Risks, Implementation Challenges, and Prospects of Quantum Computing in Military Communication*, http://essay.utwente.nl/103094/

Drent, M. (2011). *The EU's Comprehensive Approach to Security: A Culture of Co-ordination?,* Studia Diplomatica, STUDIA DIPLOMATICA LXIV(2), https://www.clingendael.org/sites/default/files/pdfs/20111000_sd_drent_approach.pdf

EEAS (2020). *A strategic compass for Security and Defense*, https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf

Engels, R. (2024), *Breaking free from confirmation bias in AI: A call for a better approach to all things AI,* Capgemini, https://www.capgemini.com/insights/expert-perspectives/breaking-free-from-confirmation-bias-in-ai/

EUCPN, *Artificial intelligence and predictive policing: risks and challenges*, https://eucpn.org/sites/default/files/document/files/PP (2).pdf

European Commission (2023), *Commission recommends carrying out risk assessments on four critical technology areas: advanced semiconductors, artificial intelligence, quantum, biotechnologies,* press release, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4735

Everett, M. (2021). EU–US collaboration on quantum technologies, Chatham House, https://www.chathamhouse.org/sites/default/files/2021-01/2021-01-28-eu-us-quantum-tech-everett.pdf

Fraser, C. (2024). AI's baptism by fire in Ukraine and Gaza offers wider lessons, International Institute for Strategic Studies (IISS), https://www.iiss.org/online-analysis/military-balance/2024/04/analysis-ais-baptism-by-fire-in-ukraine-and-gaza-offer-wider-lessons/

Garisto, D. (2024), How cutting-edge computer chips are speeding up the AI revolution, Nature, https://www.nature.com/articles/d41586-024-01544-0

Geurden, M. (2018), A New Future for Military Security Using Fully Homomorphic Encryption, Royal Military Academy, https://www.researchgate.net/publication/327799148_A_New_Future_for_Military_Security_Using_Fully_Homomorphic_Encryption

Gidney, C. and Ekerå, M. (2021), How to factor 2048-bit RSA integers in 8 hours using 20 million noisy qubits, Quantum, 5, https://quantum-journal.org/papers/q-2021-04-15-433/pdf/

Goncharuk, V. (2024), Russia's War in Ukraine: Artificial Intelligence in Defense of Ukraine, ICDS Brief, https://icds.ee/wp-content/uploads/dlm_uploads/2024/09/Layout-AI-in-Defense-of-Ukraine.pdf

Grand-Clément, S. (2023), Artificial Intelligence Beyond Weapons, United Nations Institute for Disarmament Research (UNIDIR), https://unidir.org/wp-content/uploads/2023/10/UNIDIR_AI_Beyond_Weapons_Application_Impact_AI_in_the_Military_Domain.pdf

Hammond, S. (2024), The Scramble for AI Computing Power, American Affairs, https://americanaffairsjournal.org/2024/05/the-scramble-for-ai-computing-power/

Henshall, W. (2024), The U.S. Military's Investments Into Artificial Intelligence Are Skyrocketing, Time, https://time.com/6961317/ai-artificial-intelligence-us-military-spending/

Huttner, B., et al. (2022), Long-range QKD without trusted nodes is not possible with current technology, NPJ Quantum Information, 8(108)

IBM (2021), IBM Quantum breaks the 100-qubit processor barrier, https://www.ibm.com/quantum/blog/127-qubit-quantum-processor-eagle

IBM (2024), Landmark IBM error correction paper published on the cover of Nature, https://www.ibm.com/quantum/blog/nature-qldpc-error-correction

IBM, What are large language models (LLMs)?, https://www.ibm.com/topics/large-language-models

IBM (2024), What is sovereign cloud? https://www.ibm.com/topics/sovereign-cloud

Intel, Artificial Intelligence (AI) Hardware, Intel, https://www.intel.com/content/www/us/en/learn/ai-hardware.html

Jackson, F. (2024), AI Surge Could Trigger Global Chip Shortage by 2026, Research Finds, TechRepublic, https://www.techrepublic.com/article/ai-chip-shortage-global-supply-crisis/

Julienne, M. (2022), Le rêve quantique chinois : les aspirations d'un géant dans l'infiniment petit, Etudes de l'IFRI, https://www.ifri.org/fr/etudes/le-reve-quantique-chinois-les-aspirations-dun-geant-dans-linfiniment-petit

Köpke J. and Küsters A. (2023), Vorteil Ukraine: Wie KI die Kräfteverhältnisse im Krieg verändert, CEP, https://www.cep.eu/de/eu-themen/details/vorteil-ukraine-wie-ki-die-kraefteverhaeltnisse-im-krieg-veraendert-cepadhoc.html

Krelina, M. (2021). Quantum technology for military applications, EPJ Quantum Technology Vol.8(24), https://doi.org/10.1140/epjqt/s40507-021-00113-y

Julienne, M. (2022), Le rêve quantique chinois : les aspirations d'un géant dans l'infiniment petit, Etudes de l'IFRI, https://www.ifri.org/fr/etudes/le-reve-quantique-chinois-les-aspirations-dun-geant-dans-linfiniment-petit

Köpke J. and Küsters A. (2023), Vorteil Ukraine: Wie KI die Kräfteverhältnisse im Krieg verändert, CEP, https://www.cep.eu/de/eu-themen/details/vorteil-ukraine-wie-ki-die-kraefteverhaeltnisse-im-krieg-veraendert-cepadhoc.html

Krelina, M. (2021). Quantum technology for military applications, EPJ Quantum Technology Vol.8(24), https://doi.org/10.1140/epjqt/s40507-021-00113-y

Kumar, M. (2022), Post-quantum cryptography Algorithm's standardization and performance analysis, Array

Legarda, H. and Nouwens, M. (2018), China's pursuit of advanced dual-use technologies, International Institute for Strategic Studies, https://www.iiss.org/research-paper/2018/12/emerging-technology-dominance/

Li, S. (2023), Post-Quantum Security: Opportunities and Challenges, Sensors 23, https://www.mdpi.com/1424-8220/23/21/8744

Makichuk, D. (2021), Quantum radar: A stealth buster or a bluff?, Asia Times, https://asiatimes.com/2021/09/quantum-radar-does-it-actually-work/

McKinsey Digital (2024), Quantum Technology Monitor, https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/steady-progress-in-approaching-the-quantum-advantage#/

Mosca, M. and Piani, M. (2023), Quantum threat timeline report, Global Risk Institute, https://globalriskinstitute.org/publication/2023-quantum-threat-timeline-report/

MRL (2023), How AI and 5G will power the next wave of Innovation, https://www.mrlcg.com/resources/blog/how-ai-and-5g-will-power-the-next-wave-of-innovation/

Munich Security Conference (2024), Lose-Lose? Munich Security Conference Report 2024, https://securityconference.org/assets/01_Bilder_Inhalte/03_Medien/02_Publikationen/2024/MSR_2024/MSC_Report_2024_190x250mm_EN_final_240507_DIGITAL.pdf

Munich Security Conference (2022), Transatlantic To-Do List, https://securityconference.org/transatlantic-to-do-list/#c6870

Muralidharan, S., et al. (2016). Optimal architectures for long distance quantum communication. Nature Magazine Scientific Reports, 6, https://doi.org/10.1038/srep20463

NASA (2023), Technology Readiness Levels, https://www.nasa.gov/directorates/somd/space-communications-navigation-program/technology-readiness-levels/

NATO (2022), NATO's Data and Artificial Intelligence Review Board, https://www.nato.int/cps/su/natohq/official_texts_208374.htm

NATO (2024), Summary of NATO's revised Artificial Intelligence (AI) strategy, https://www.nato.int/cps/en/natohq/official_texts_227237.htm

NIST (2009), NIST Demonstrates 'Universal' Programmable Quantum Processor for Quantum Computers, https://www.nist.gov/news-events/news/2009/11/nist-demonstrates-universal-programmable-quantum-processor-quantum

NIST (2024), NIST Releases First 3 Finalized Post-Quantum Encryption Standards, https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

NIST (2024), Transition to Post-Quantum Cryptography Standards, NIST Internal Report, NIST IR 8547 ipd, https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf

O'Brien, M. (2024), U.S. ahead in AI innovation, easily surpassing China in Stanford's new ranking, AP News, https://apnews.com/article/ai-us-china-competition-stanford-index-uk-india-c8eb9be0253eb39776c3e38d05f1a329

O'Donnell, J. (2024), Why OpenAI's new model is such a big deal, MIT Technology Review, https://www.technologyreview.com/2024/09/17/1104004/why-openais-new-model-is-such-a-big-deal/

OECD Library, AI language models, OECD Digital Economy Papers, https://www.oecd-ilibrary.org/science-and-technology/ai-language-models_13d38f92-en

Omaar, H. (2024), How Innovative Is China in AI?, Information Technology & Innovation Foundation, https://itif.org/publications/2024/08/26/how-innovative-is-china-in-ai/

Omaar, H. and Makaryan, M. (2024), How Innovative Is China in Quantum?, Information Technology & Innovation Foundation, https://itif.org/publications/2024/09/09/how-innovative-is-china-in-quantum/

Parker, E. (2022), An Assessment of the U.S. and Chinese Industrial Bases in Quantum Technology, RAND Corporation Research Report, https://www.rand.org/pubs/research_reports/RRA869-1.html

Omaar, H. and Makaryan, M. (2024), How Innovative Is China in Quantum?, Information Technology & Innovation Foundation, https://itif.org/publications/2024/09/09/how-innovative-is-china-in-quantum/

Parker, E. (2022), An Assessment of the U.S. and Chinese Industrial Bases in Quantum Technology, RAND Corporation Research Report, https://www.rand.org/pubs/research_reports/RRA869-1.html

Parker, E. (2021), Commercial and Military Applications and Timelines for Quantum Technology, RAND Corporation Research Report, https://www.rand.org/pubs/research_reports/RRA1482-4.html

Pupillo, L., et al. (2023), Quantum Technologies and Cybersecurity: Technology, governance and policy challenges, Centre for European Policy Studies, https://cdn.ceps.eu/wp-content/uploads/2023/12/CEPS-TFR-Quantum-Technologies-and-Cybersecurity.pdf

Perez, L. (2024), CDAO Enabling Workforce to Harness Data Analytics, AI, MeriTalk, https://www.meritalk.com/articles/cdao-enabling-workforce-to-harness-data-analytics-ai/

Reinhardt, M. (2022), Sovereign cloud opens the door to transformation in the public sector, Capgemini, https://www.capgemini.com/insights/expert-perspectives/sovereign-cloud-opens-the-door-to-transformation-in-the-public-sector/

Red Hat (2021). What is edge computing?, https://www.redhat.com/en/topics/edge-computing/what-is-edge-computing?

Reuters (2024). Silicon Box picks Italy's Piedmont region for $3.4 bln chip plant, June 28, 2024, https://www.reuters.com/technology/silicon-box-picks-piedmont-region-its-italian-34-bln-chip-plant-2024-06-28/

Rossi, D. and Zhang, L (2022), Network artificial intelligence, fast and slow, https://dl.acm.org/doi/10.1145/3565009.3569521

Ruitenberg, R. (2024), France preps Europe's fastest classified supercomputer for defense AI, DefenseNews, https://www.defensenews.com/global/europe/2024/06/18/france-preps-europes-fastest-classified-supercomputer-for-defense-ai/

Shipps, A. (2024), LLMs develop their own understanding of reality as their language abilities improve, MIT News, https://news.mit.edu/2024/llms-develop-own-understanding-of-reality-as-language-abilities-improve-0814

Sparks, L. (2024), New supercomputing network could lead to AGI, scientists hope, with 1st node coming online within weeks, Live Science, https://www.livescience.com/technology/artificial-intelligence/new-supercomputing-network-lead-to-agi-1st-node-coming-within-weeks

Srivastava, N., et al. (2023), The Potential of Quantum Techniques for Stock Price Prediction, https://arxiv.org/pdf/2308.13642

Swayne, M. (2024). Report: China And Russia Test Quantum Communication Link, Quantum Insider, (2 January 2024) https://thequantuminsider.com/2024/01/02/report-china-and-russia-test-quantum-communication-link/

Swayne, M. (2024). Chinese Scientists Report Using Quantum Computer To Hack Military-Grade Encryption, Quantum Insider (11 October 2024), https://thequantuminsider.com/2024/10/11/chinese-scientists-report-using-quantum-computer-to-hack-military-grade-encryption/

The Economist (2024), How Ukraine is using AI to fight Russia, https://www.economist.com/science-and-technology/2024/04/08/how-ukraine-is-using-ai-to-fight-russia

Tirpak, John A. (2024). Kendall: In US-China 'Race for Technological Superiority,' AI May Be the Key, Air & Space Forces Magazine (29 October 2024), https://www.airandspaceforces.com/kendall-us-china-race-technological-superiority-ai/

Trzcinski, A., et al. (2023), Post-Quantum Cryptography, Technology Primers for Policymakers, https://www.belfercenter.org/sites/default/files/2024-10/Post%20Quantum%20Cryptography_Tech%20Primer.pdf

U.S. Department of State (2023), Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy, https://www.state.gov/political-declaration-on-responsible-military-use-of-artificial-intelligence-and-autonomy-2/

Vallance, C (2024). Google unveils 'mind-boggling' quantum computing chip, BBC, https://www.bbc.com/news/articles/c791ng0zvl3o

Wang, Y. (2024). 中美量子计算发展现状比较 (Comparison of the current status of quantum computing development in China and the United States), Shanghai Institute of Scientific and Technical Information, https://www.istis.sh.cn/cms/news/article/92/27063

Wilkins, A. (2023), Record-breaking quantum computer has more than 1000 qubits, News Scientist, https://www.newscientist.com/article/2399246-record-breaking-quantum-computer-has-more-than-1000-qubits/#new_tab

Zorloni, L. (2024), Europe Is Pumping Billions Into New Military Tech, Wired, https://www.wired.com/story/european-commission-military-tech-spending/

Zysk, K. (2023), Struggling, Not Crumbling: Russian Defense AI in a Time of War, Royal United Services Institute, https://rusi.org/explore-our-research/publications/commentary/struggling-not-crumbling-russian-defence-ai-time-war

End notes

1. Araya, D., King, M. (2022), The Impact of Artificial Intelligence on Military Defense and Security, Center for International innovation, https://www.cigionline.org/static/documents/no.263.pdf – p. 11
2. NATO (2024), Summary of NATO's revised Artificial Intelligence (AI) strategy, https://www.nato.int/cps/en/natohq/official_texts_227237.htm
3. Calais, S., Tay, J. (2024), Generative AI hardware - the other arms race, A&O Shearman, https://www.aoshearman.com/en/insights/generative-ai-hardware-the-other-arms-race
4. Jackson, F. (2024), AI Surge Could Trigger Global Chip Shortage by 2026, Research Finds, TechRepublic, https://www.techrepublic.com/article/ai-chip-shortage-global-supply-crisis/
5. Ibid.
6. NATO (2024), op cit.
7. Munich Security Conference (2022), Transatlantic To-Do List, https://securityconference.org/en/transatlantic-to-do-list/
8. Bode, I., Nadibaidze, A., Zhang, Q. (2024), AI in Military Decision Support Systems, Center for War Studies, https://usercontent.one/wp/www.autonorms.eu/wp-content/uploads/2024/11/AI-DSS-report-WEB.pdf – p. 36
9. Ibid., p.11
10. Sovereign cloud is a type of cloud computing that complies with laws and regulations from the country or region where it operates. See IBM (2024), What is sovereign cloud?, https://www.ibm.com/topics/sovereign-cloud.
11. Reinhardt, M. (2022), Sovereign cloud opens the door to transformation in the public sector, Capgemini, https://www.capgemini.com/insights/expert-perspectives/sovereign-cloud-opens-the-door-to-transformation-in-the-public-sector/
12. Geurden, M. (2018), A New Future for Military Security Using Fully Homomorphic Encryption, Royal Military Academy, https://www.researchgate.net/publication/327799148_A_New_Future_for_Military_Security_Using_Fully_Homomorphic_Encryption
13. Jackson (2024), op cit.
14. Bode, Nadibaidze, and Zhang (2024), op cit., pp.30-31
15. Ibid., p.37
16. Ibid., p.37. The DoD's "Algorithmic Warfare Cross-Functional Team" programme aims at "using computer vision and machine learning algorithms to identify targets in real time based on previously collected data such as drone footage. As with many AI-based systems, echnologies developed under Maven can be used for various purposes, including military planning and targeting."
17. NATO (2024), op cit.
18. See: NATO (2022), NATO's Data and Artificial Intelligence Review Board, https://www.nato.int/cps/su/natohq/official_texts_208374.htm
19. NATO (2024), op cit.
20. Engels, R. (2024), Breaking free from confirmation bias in AI: A call for a better approach to all things AI, Capgemini, https://www.capgemini.com/insights/expert-perspectives/breaking-free-from-confirmation-bias-in-ai/
21. Henshall, W. (2024), The U.S. Military's Investments Into Artificial Intelligence Are Skyrocketing, Time, https://time.com/6961317/ai-artificial-intelligence-us-military-spending/
22. Department of Defense (2023), Data, Analytics, and Artificial Intelligence Adoption Strategy, https://media.defense.gov/2023/Nov/02/2003333300/-1/-1/1/DOD_DATA_ANALYTICS_AI_ADOPTION_STRATEGY.PDF
23. Perez, L. (2024), CDAO Enabling Workforce to Harness Data Analytics, AI, MeriTalk, https://www.meritalk.com/articles/cdao-enabling-workforce-to-harness-data-analytics-ai/
24. Araya, D.(2022), Artificial intelligence for Defense and Security, Center for International innovation, https://www.cigionline.org/static/documents/Araya_AI-for-Defence_SpecialReport_Q4fjNfp.pdf – p. 7
25. China Industrial Daily (2024). 人工智能发展持续蓬勃向前 AI大模型成为未来产业新赛道 (The development of artificial intelligence continues to thrive, with AI large models emerging as a new frontier in future industries), http://www.ciia.org.cn/news/25369.cshtml
26. Legarda, H. and Nouwens, M. (2018), China's pursuit of advanced dual-use technologies, International Institute for Strategic Studies, https://www.iiss.org/research-paper/2018/12/emerging-technology-dominance/
27. De Vynck, G., Tiku, N. (2025), Trump tech agenda begins with $500B private AI plan and cuts to regulation, The Washington Post, https://www.washingtonpost.com/technology/2025/01/21/stargate-500-billion-trump-ai/
28. Omaar, H. (2024), How Innovative Is China in AI?, ITIF, https://itif.org/publications/2024/08/26/how-innovative-is-china-in-ai/
29. Ibid.
30. Zysk, K. (2023), Struggling, Not Crumbling: Russian Defense AI in a Time of War, Royal United Services Institute, https://rusi.org/explore-our-research/publications/commentary/struggling-not-crumbling-russian-defence-ai-time-war
31. Ibid.
32. Ibid.
33. Goncharuk, V. (2024), Russia's War in Ukraine: Artificial Intelligence in Defense of Ukraine, ICDS Brief, https://icds.ee/wp-content/uploads/dlm_uploads/2024/09/Layout-AI-in-Defence-of-Ukraine.pdf
34. Zorloni, L. (2024), Europe Is Pumping Billions Into New Military Tech, Wired, https://www.wired.com/story/european-commission-military-tech-spending/
35. Ruitenberg, R. (2024), France preps Europe's fastest classified supercomputer for defense AI, DefenseNews, https://www.defensenews.com/global/europe/2024/06/18/france-preps-europes-fastest-classified-supercomputer-for-defense-ai/
36. Ibid.
37. Bradshaw, T., Kinder, T., Pfeifer, S.(2024), German AI defense start-up Helsing poised to triple valuation to $4.5bn, Financial Times, https://www.ft.com/content/e09f813b-e568-4afe-8e07-940a707595ca
38. The basis of quantum computing is no longer the bit (0 or 1) but the qubit (quantum superposition of all possible |0> and |1> states). Quantum computing takes advantage of the fact that a particle can be in several places at once, to build a system that can perform several calculations at the same time, rather than simply in parallel like current computers. See Kumar, M. (2022), Post-quantum cryptography Algorithm's standardization and performance analysis, Array, p.15.
39. Vallance, C. (2024) Google unveils 'mind-boggling' quantum computing chip, BBC, https://www.bbc.com/news/articles/c791ng0zvl3o
40. Srivastava, N., et al. (2023), The Potential of Quantum Techniques for Stock Price Prediction, https://arxiv.org/pdf/2308.13642

41. Krelina, M. (2021). Quantum technology for military applications, EPJ Quantum Technology, 8(24), https://doi.org/10.1140/epjqt/s40507-021-00113-y – p.14
42. Dijkstra, E. (2024), Quantum and Military Communication Security : An Analysis of the Opportunities, Risks, Implementation Challenges, and Prospects of Quantum Computing in Military Communication, http://essay.utwente.nl/103094/
43. Trzcinski, A., et al. (2023), Post-Quantum Cryptography, Technology Primers for Policymakers, https://www.belfercenter.org/sites/default/files/2024-10/Post%20Quantum%20Cryptography_Tech%20Primer.pdf
44. Pupillo, L., et al. (2023), Quantum Technologies and Cybersecurity: Technology, governance and policy challenges, Centre for European Policy Studies, https://cdn.ceps.eu/wp-content/uploads/2023/12/CEPS-TFR-Quantum-Technologies-and-Cybersecurity.pdf
45. Mosca, M. and Piani, M. (2023), Quantum threat timeline report, Global Risk Institute, https://globalriskinstitute.org/publication/2023-quantum-threat-timeline-report/
46. For example, practical applications like cryptographic decryption would require millions of qubits to account for imperfections. Currently, the most advanced quantum computers have only a few dozen logical qubits.
47. Estimates for breaking RSA-2048 key in 8 hours would require around 14 000 logical qubits for near 20 million physical qubits. See: Gidney, C. and Ekerå, M. (2021), How to factor 2048-bit RSA integers in 8 hours using 20 million noisy qubits, Quantum, 5, https://quantum-journal.org/papers/q-2021-04-15-433/pdf/
48. Parker (2021), op cit., p.18
49. For the scale, see NASA (2023), Technology Readiness Levels, https://www.nasa.gov/directorates/somd/space-communications-navigation-program/technology-readiness-levels/
50. Li, S. (2023), Post-Quantum Security: Opportunities and Challenges, Sensors 23, https://www.mdpi.com/1424-8220/23/21/8744
51. Trzcinski, et al. (2023), op cit., p.6
52. Dickson, J. and Harding, E. (2024). Unleashing Quantum's Potential, Center for Strategic and International Studies, https://www.csis.org/analysis/unleashing-quantums-potential
53. Ibid.
54. Parker, E. (2022), An Assessment of the U.S. and Chinese Industrial Bases in Quantum Technology, RAND Corporation Research Report, https://www.rand.org/pubs/research_reports/RRA869-1.html – pp.57-69NIST (2024),
55. NIST Releases First 3 Finalized Post-Quantum Encryption Standards, https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards
56. NIST (2024), Transition to Post-Quantum Cryptography Standards, NIST Internal Report, NIST IR 8547 ipd, https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf
57. Parker (2022), op cit., p.72
58. Ibid., pp.83-92
59. Julienne, M. (2022), Le rêve quantique chinois : les aspirations d'un géant dans l'infiniment petit, Etudes de l'IFRI, https://www.ifri.org/fr/etudes/le-reve-quantique-chinois-les-aspirations-dun-geant-dans-linfiniment-petit – p.12
60. Omaar, H. and Makaryan, M. (2024), How Innovative Is China in Quantum?, Information Technology & Innovation Foundation, https://itif.org/publications/2024/09/09/how-innovative-is-china-in-quantum/
61. Parker (2021), op cit., p.23
62. Austrian Academy of Sciences (2018), Secure quantum communication over 7,600 kilometers, https://www.oeaw.ac.at/en/news-1/secure-quantum-communication-over-7600-kilometers-2
63. Wang, Y. (2024). 中美量子计算发展现状比较 (Comparison of the current status of quantum computing development in China and the United States), Shanghai Institute of Scientific and Technical Information, https://www.istis.sh.cn/cms/news/article/92/27063
64. European Commission (2023), Commission recommends carrying out risk assessments on four critical technology areas: advanced semiconductors, artificial intelligence, quantum, biotechnologies, press release, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4735
65. Pupillo, et al. (2023), op cit., p.19
66. Ibid., pp.86-86
67. McKinsey Digital (2024), Quantum Technology Monitor, https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/steady-progress-in-approaching-the-quantum-advantage#/, pp.40,42
68. Parker (2022), op cit., pp.52-53
69. McKinsey Digital (2024), op cit., p.19
70. Bundesamt für Sicherheit in der Informationstechnik, et al. (2024), Securing Tomorrow, Today: Transitioning to Post- Quantum Cryptography, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/PQC-joint-statement.pdf?__blob=publicationFile&v=5
71. Bondar, K. (2024). Understanding the Military AI Ecosystem of Ukraine, Center for Strategic and International Studies (CSIS), https://www.csis.org/analysis/understanding-military-ai-ecosystem-ukraine
72. Reuters (2024). Silicon Box picks Italy's Piedmont region for $3.4 bln chip plant, June 28, 2024, https://www.reuters.com/technology/silicon-box-picks-piedmont-region-its-italian-34-bln-chip-plant-2024-06-28/
73. The issue of availability of quality data to train AI models was recognized in NATO's 2024 revised Artificial Intelligence strategy as a "prerequisite for the development and use of secure, reliable and responsible AI systems".
74. In this regard, the DARB acts as a forum to share best practices and ensure interoperable systems outputs to help "deliver a qualitative advantage". See: NATO (2022), op cit.

About Capgemini

Capgemini is a global business and technology transformation partner, helping organizations to accelerate their dual transition to a digital and sustainable world, while creating tangible impact for enterprises and society. It is a responsible and diverse group of 340,000 team members in more than 50 countries. With its strong over 55-year heritage, Capgemini is trusted by its clients to unlock the value of technology to address the entire breadth of their business needs. It delivers end-to-end services and solutions leveraging strengths from strategy and design to engineering, all fueled by its market leading capabilities in AI, cloud and data, combined with its deep industry expertise and partner ecosystem. The Group reported 2023 global revenues of €22.5 billion.

Get the Future You Want | www.capgemini.com