The Defense Technology Frontier

How Europe Could Lead

February 2026
By Nikolaus Lang, Philippe Lavigne, Greg Mallory, Rami Rafih, Jona Lampert, and David Zuluaga Martínez

BCG | BCG HENDERSON INSTITUTE

Boston Consulting Group

Boston Consulting Group partners with leaders in business and society to tackle their most important challenges and capture their greatest opportunities. BCG was the pioneer in business strategy when it was founded in 1963. Today, we work closely with clients to embrace a transformational approach aimed at benefiting all stakeholders—empowering organizations to grow, build sustainable competitive advantage, and drive positive societal impact.

Our diverse, global teams bring deep industry and functional expertise and a range of perspectives that question the status quo and spark change. BCG delivers solutions through leading-edge management consulting, technology and design, and corporate and digital ventures. We work in a uniquely collaborative model across the firm and throughout all levels of the client organization, fueled by the goal of helping our clients thrive and enabling them to make the world a better place.

BCG Henderson Institute

The BCG Henderson Institute is Boston Consulting Group's strategy think tank, dedicated to exploring and developing valuable new insights from business, technology, and science by embracing the powerful technology of ideas. The Institute engages leaders in provocative discussion and experimentation to expand the boundaries of business theory and practice and to translate innovative ideas from within and beyond business. For more ideas and inspiration from the Institute, please visit our **website** and follow us on **LinkedIn** and **X (formerly Twitter)**.

Introduction

Governments around the world are reassessing their strategic defense capabilities. Many of these countries, particularly in Europe, are playing catch-up after decades of underinvestment in defense and are focusing on strengthening their ability to meet immediate national security needs: closing capability gaps, rebuilding stockpiles, and fortifying existing systems against cyber threats.

Such efforts are essential but incomplete. New and emerging defense technologies—across AI, autonomous systems, space, biotechnology, quantum technologies, and more—are changing the very nature of conflict and altering the future definition of military advantage. It is crucial that policymakers consider these strategic interests in tandem.

Europe—specifically, the UK and all countries that are members of both NATO and the EU—faces unique challenges in navigating this new geostrategic terrain. The region is an established hub of world-class talent with strong research capacity. But our analysis of roughly 250 million research publications, 90 million patent family records, and multiple investment trends, shows that Europe struggles to convert its research potential into deployable defense products. The disconnect between potential and application is due in large part to the lack of consistent demand from domestic military end users.

Such demand, however, is poised to grow. Many European countries aim to more than double their defense spending to 5% of GDP annually by 2035 (with 3.5% taking the form of core defense spending). But what should that investment look like, now and in the years to come? To help answer that question, we have focused our study on the defense tech frontier—identifying the highest-impact new technologies on the basis of insights from a panel of more than 50 senior defense experts in Europe, the US, and other allied countries. We also assessed Europe's relative position across these key technologies—to propose a path for national leaders and policymakers to follow in prioritizing investments.

What Is the Defense Tech Frontier?

Often, policy leaders must make strategic security decisions within the constraints of limited resources. To prioritize and deploy national resources effectively and maximize their defense capabilities, these leaders should aim to identify three key things:

- The technologies most likely to shape the future of warfare
- How rapidly those technologies are evolving
- The point at which those technologies will have an impact on the battlefield at scale

To identify the highest-impact defense technologies of the future, we convened a panel of senior BCG defense experts. We used NATO's nine emerging and disruptive technology (EDT) areas as a starting point for the analysis, ranging from AI to biotech and hypersonic systems. **(See the appendix, "NATO's Nine EDTs.")** From an initial group of 60 applications, we identified 19 that could have the greatest potential strategic impact across three time horizons. **(See Exhibit 1 and Exhibit 2.)**

For each of these technologies, the current level of development is an important factor, but the rate at which they are progressing is equally important. According to the defense experts we surveyed, AI-powered applications—such as sensors and effectors that autonomously detect, classify, and respond to threats in real time, and intelligence analysis and decision support systems that process vast amounts of data to support faster decision making—are evolving especially quickly at the moment. By contrast, human augmentation systems, which enhance soldier resilience and protection, are progressing more slowly than most other applications in the group of 19.

Differences in the rate of progress across technology applications are important because they determine how much runway countries are likely to have for developing homegrown solutions. Since not all countries have the same resources, objectives, and security needs, it's important to base region-specific assessments of these global trends on how each region is positioned to compete, cooperate, or shape the emerging defense-technology landscape.

EXHIBIT 1

High-Impact Frontier Defense Technology Applications

NATO EDT areas	Shortlisted defense tech applications for each EDT		
Artificial intelligence	AI-empowered sensors and effectors	AI intelligence analysis and decision support systems	Human-machine teaming systems
Quantum technologies	Quantum key distribution	Quantum sensing	Quantum AI and large-scale quantum computing
Autonomous systems	Autonomous unmanned aerial, ground, and maritime systems	Highly autonomous swarms and integrated combat networks	
Biotechnology and human enhancement technologies	Advanced biological agents	Advanced soldier capability and survivability augmentation systems	
Space	Advanced anti-satellite systems	Next-generation space-based communication systems	
Hypersonic systems	Advanced global strike systems and hypersonic missile defense		
Novel materials and manufacturing	Meta materials		
Energy and propulsion	Advanced directed energy weapons	Compact field-deployable energy sources	
Next-generation communication networks	6G and advanced networking	Unified multidomain networks	Ad hoc mesh communications and self-healing, secure networks

Sources: NATO; BCG analysis.
Note: EDT = emerging and disruptive technologies.

Europe trails other major military powers in developing emerging defense technologies, but it has not yet been left behind.

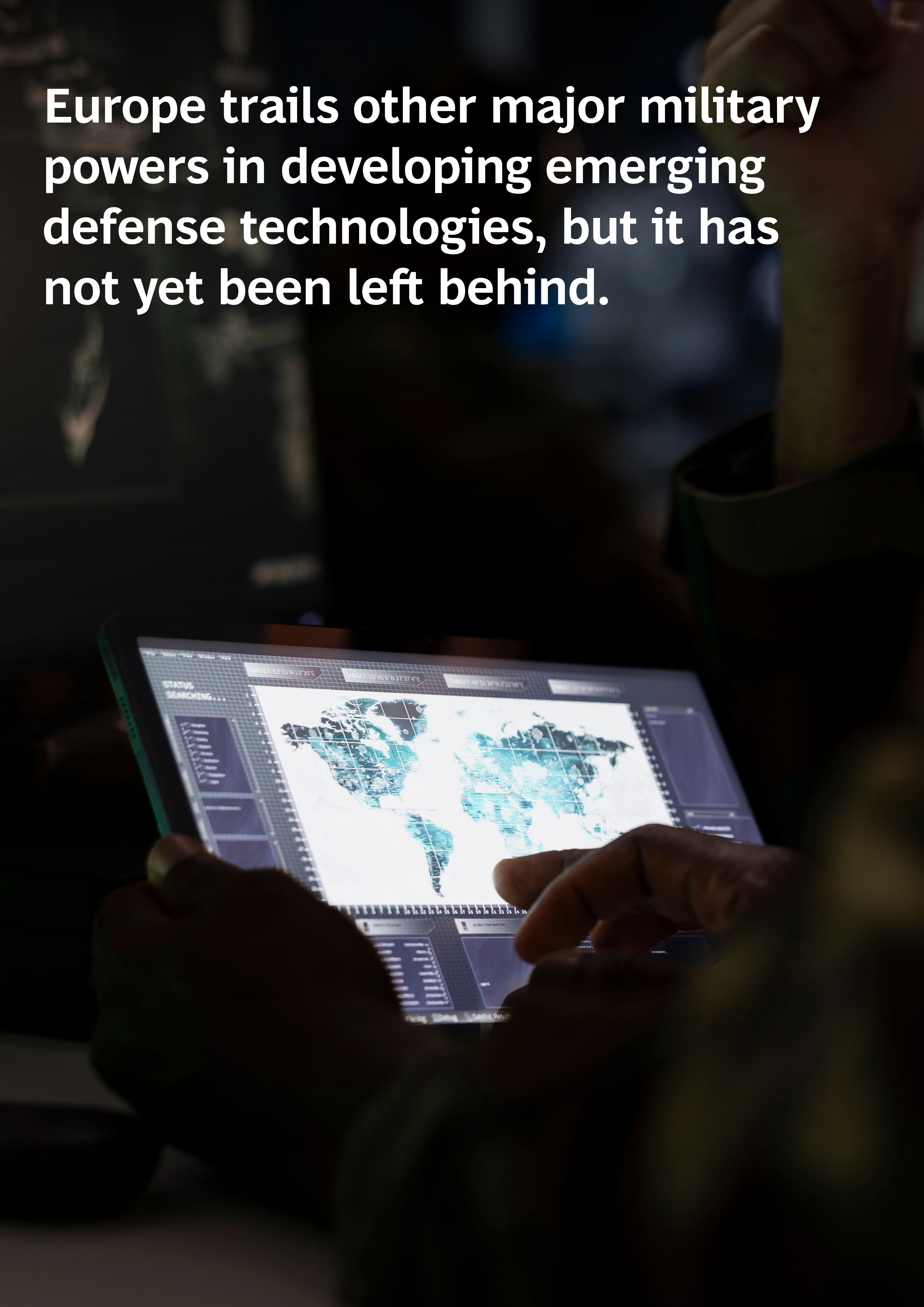


EXHIBIT 2

Defense Technology Applications Are Likely to Mature at Different Points in Time

Relative impact

	Current and imminent (0–5 years)	Middle term (5–15 years)	Long term (15+ years)
	AI intelligence analysis and decision support systems AI-empowered sensors and effectors Autonomous unmanned aerial, ground, and maritime systems	Highly autonomous swarms and integrated combat networks Advanced biological agents Human-machine teaming systems Quantum sensing	Quantum AI and large-scale quantum computing Unified multidomain networks
High	Advanced anti-satellite systems Next-generation space-based communication systems	Ad hoc mesh communications and self-healing, secure networks Quantum key distribution 6G and advanced networking Advanced global strike systems and hypersonic missile defense Advanced directed energy weapons	Meta materials Compact field-deployable energy sources Advanced soldier capability and survivability augmentation systems
≈ Low	~40 applications deprioritized		

Source: BCG analysis.
Note: "Impact" refers to the degree to which the technology can shape outcomes on the battlefield. "Time horizon" refers to the time frame in which this technology will most likely reach maturity (that is, be sufficiently advanced to have real at-scale battlefield impact). A technology that is just being worked on or is in the prototype or R&D stage is not counted toward maturity, nor do the time horizons consider a country's capacity to integrate the technology into its armed forces.

Europe's Significant Research-to-Development Gap

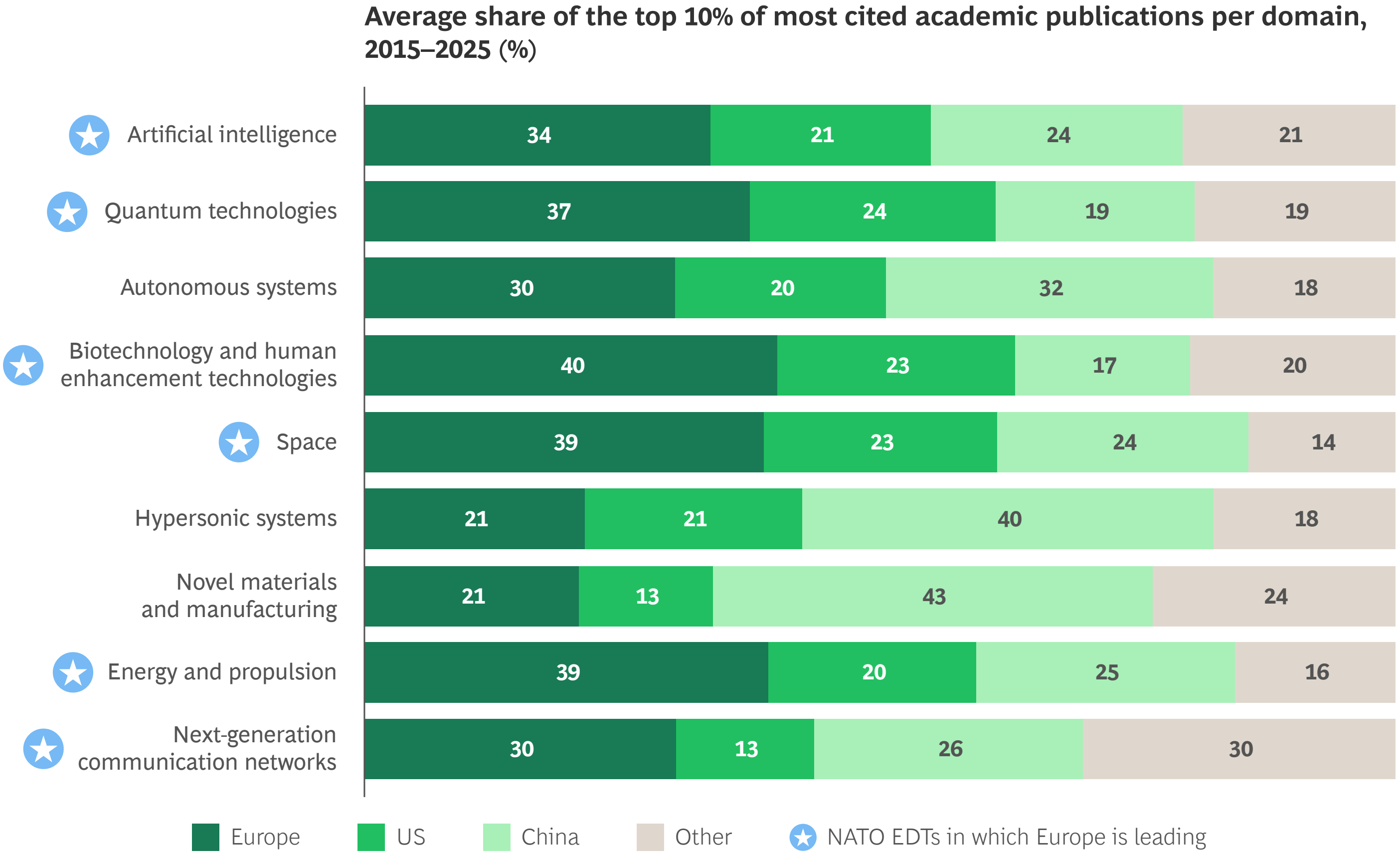
Europe currently trails other major military powers in developing these emerging defense technologies, but the region has not yet been left behind. The defense experts we consulted consistently rank Europe third globally across the 18 of the 19 high-impact applications—the one exception being soldier capability and survivability augmentation systems, where it ranks second.

Research strength in Europe is particularly strong, according to our analysis of some 250 million research publications in the OpenAlex database. Over the past decade, Europe has accounted for more of the top 10% of most highly cited papers across six of the nine NATO EDT areas than any other region. **(See Exhibit 3.)** Europe has a sizable lead in high-quality research in AI, quantum technologies, space, energy and propulsion, and biotechnology and human enhancement technologies.

But for scientific research to lead to breakthroughs, it must be developed, typically into patented products—and this is where our analysis reveals a problematic recurring pattern for Europe. The region's strong fundamental research capabilities tend to yield only limited commercial development. Even in instances where demand exists for sophisticated technologies that Europe is well placed to develop, the region has failed to keep pace. For example, Europe ranks fifth globally in global strike systems and hypersonic missile defense applications, even though some of its top defense companies have collaborated for decades on these weapons.

EXHIBIT 3

Europe Leads in Foundational Research in Six of NATO’s Nine Emerging and Disruptive Defense Technology Areas



Sources: OpenAlex; BCG analysis.
Note: This exhibit shows only countries or regions that are among the top 20 global defense spenders and reach at least a share of 10% of the top 10% of publications from 2015 to 2025. Countries are assigned on the basis of the nationality of the institution that the authors are affiliated with. If there are multiple or different affiliations, the publication is counted for each institutions' home country. “Europe” encompasses the UK and all countries that are in both the EU and NATO. EDT = emerging and disruptive technologies. Because of rounding, not all bar segment totals add up to 100%.

Our comparative analysis of patent data reveals that Europe’s share of high-quality patents is consistently lower than its share of leading scientific publications. We found this underperformance across all nine NATO EDTs, including the ones in which European research is strongest. In the US, by contrast, the opposite is true: the country consistently has a higher share of high-quality patents than of top scientific publications. **(See Exhibit 4.)**

Challenges to Commercialization

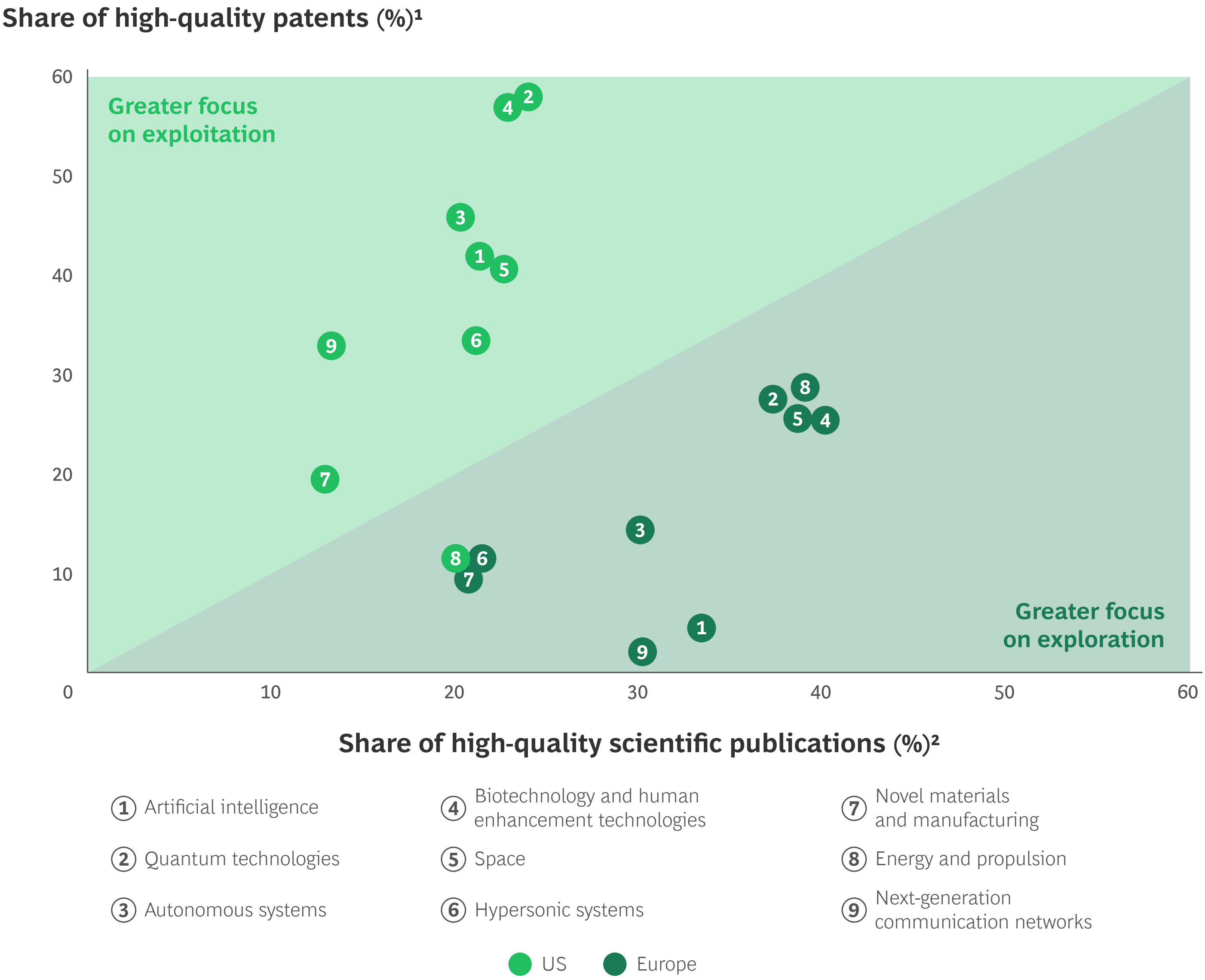
The underlying cause of this asymmetry is no secret. Multiple reports by the European Commission, the Organisation for Economic Co-operation and Development, and the European Investment Bank, all point to a common culprit: weak pathways to commercialization. Insufficient incentives and support for researchers to pursue patents, limited industry demand for frontier technologies, and fragmented markets and intellectual property regimes within Europe all hinder efforts to scale nascent innovations into market-ready technologies.

Europe’s lagging development performance is also evident in its defense startup ecosystem. There are twice as many defense startups in the US as in Europe, and these have benefited from 8.5 times the venture capital investment over the past decade—although that ratio has fallen to 7.5 times since Russia’s invasion of Ukraine. **(See Exhibit 5.)** This suggests that, on average, European companies working to develop novel defense tech applications have considerably smaller valuations than their US counterparts.

Similarly, in terms of transatlantic M&A activity, three times as much capital has flowed from the US to Europe over the past decade than has flowed from Europe to the US—a sign that Europe's defense ecosystem is deficient in scale, capitalization, and commercial maturity.

EXHIBIT 4

Europe Trails the US in Translating Fundamental Research into Patents



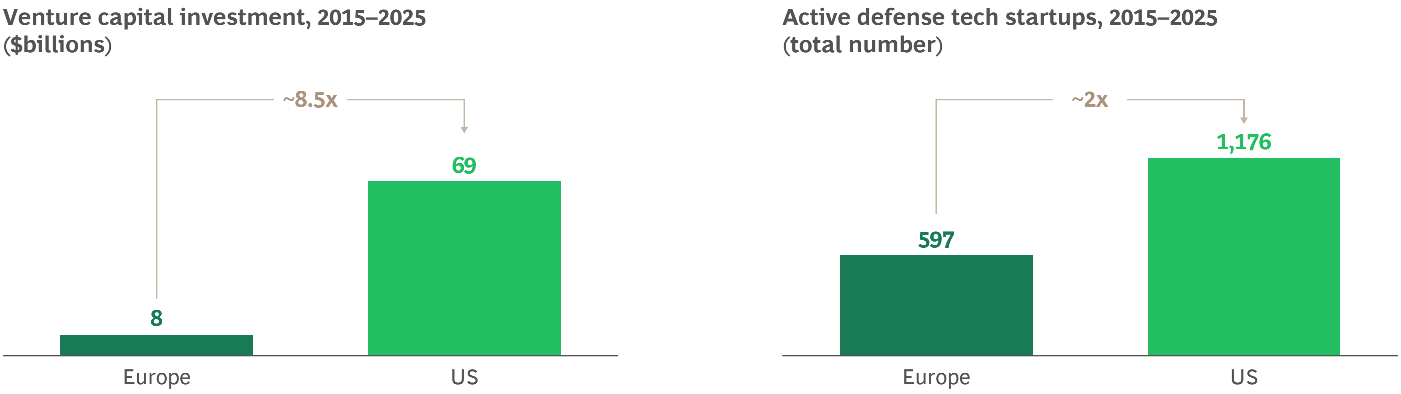
Sources: OpenAlex; LexisNexis PatentSight+; BCG analysis.
Note: "Europe" encompasses the UK and all countries that are in both the EU and NATO. The countries and regions included in the assessment were Australia, Brazil, Canada, Europe, India, Israel, Japan, Russia, South Korea, Turkey, Ukraine, and the US.

[1] Assessments of technological quality are based on Technology Relevance, a trademarked tool created by LexisNexis PatentSight+ that measures a patent's quality on the basis of its rate of forward citations in other patent applications. Patents are grouped by score as follows: 0–0.5 = low; 0.5–2 = moderate; 2–5 = high; over 5 = exceptional.

[2] Percentages reflect the country's or region's share of the top 10% most cited publications.

EXHIBIT 5

The Defense Tech Startup Ecosystem in Europe Is Smaller and Less Well Funded Than the One in the US


Venture capital investment, 2015–2025 ($billions)

Active defense tech startups, 2015–2025 (total number)

Sources: Pitchbook; BCG analysis.
Note: Numbers shown consider venture capital investment and number of active startups within the nine NATO EDTs. “Europe” encompasses the UK and all countries that are in both the EU and NATO. EDT = emerging and disruptive technologies.

These investment trends indicate that private investment and commercial activity in Europe are insufficient to translate its world-class research capacity into effective, scalable, and affordable defense tech products. Indeed, **BCG's Vitality Index**—which measures companies' growth potential along the dimensions of strategy, people, technology, and culture—finds that just one of the ten most vital defense companies in the world is European, the German aerospace company Hensoldt. Of the others, eight are based in the US and one in Turkey.

Still, defense startup activity in Europe shows encouraging signs of revival. The Munich-based defense company Helsing, founded in 2021, combines deep AI expertise with industrial scale and excels at integrating AI into existing platforms. Backed by over €1.3 billion in funding—including a €600 million round in 2025 led by Prima Materia and Saab—Helsing has emerged as one of the most prominent European defense tech startups in the market. Other European defense startups are positioning themselves to become leaders as well.

Founded in 2018 and based in Ottobrunn, Germany, Isar Aerospace develops sovereign European launch capabilities for government and defense payloads—support that is critical to securing the access to space needed to deploy a wide range of modern defense technologies. The Dutch company DeltaQuad, founded in 2012, is developing long-endurance intelligence, surveillance, and reconnaissance (ISR) drones and tactical fixed-wing vertical take-off and landing drones for European defense customers. Portugal-based Tekever got its start in 2001 and bloomed into a unicorn in 2025 by developing unmanned aerial systems for maritime surveillance, border protection, and defense-grade ISR missions. The growth of DeltaQuad and Tekever, in particular, reflects Europe’s growing strength in autonomous systems and operational intelligence.

Our research shows that Europe’s defense heavyweights are making a strategic play for the future, too. In fact, the top ten European defense companies by revenue are now active, on average, in nearly two-thirds of the 19 high-impact defense tech applications. Although many of these applications remain at the early R&D stages, the companies are contributing significantly to building a technologically advanced defense ecosystem in Europe.

A Fragmented Defense Ecosystem

Attracting private investment to help develop frontier defense technologies will ultimately depend on stable and predictable demand from European militaries. In our survey, about two-thirds of Western defense experts agreed that European adoption of military defense technology was weak across all EDT categories. But the challenge goes beyond simply raising spending levels. Europe’s defense market is highly fragmented, which saps the continent’s potential demand pull.

Despite the EU’s encouragement of large swaths of political and economic integration, pockets of fragmentation remain. Across the 27-nation bloc, member states devote some 80% of defense procurement and approximately 90% of research and technology spending on a purely national basis. The result is a mashup of systems and strategies, duplicated programs with small production runs, and limited interoperability.

There are about four times as many different major weapons systems in operation across Europe as in the US. The result is an ecosystem of many relatively small firms that serve fragmented home markets and struggle to achieve economies of scale, attract long-term private capital, and invest enough to turn Europe's strong research base into globally competitive, production-ready defense technologies.

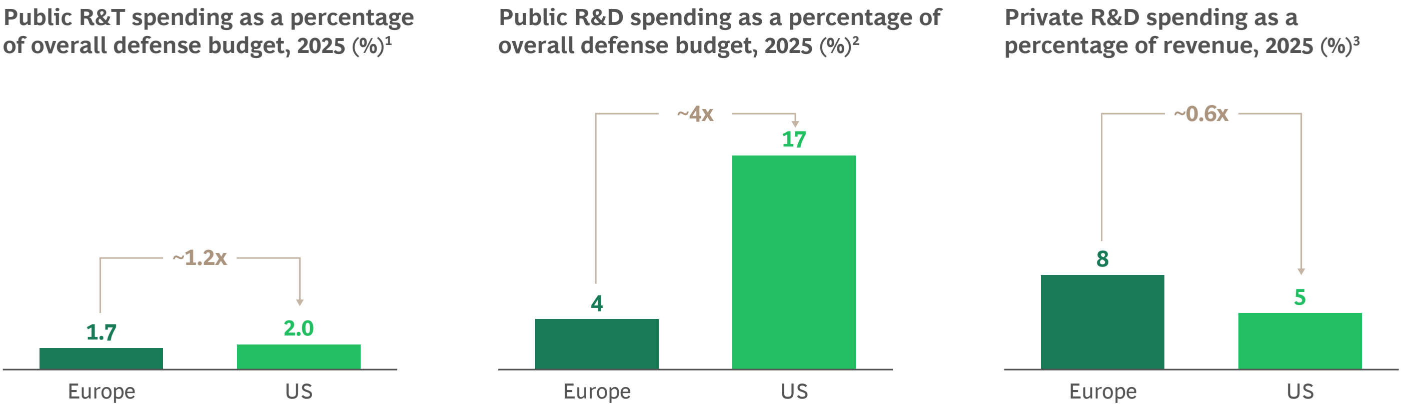
European policymakers have started to address these issues, launching initiatives such as the EU Defence Industry Reinforcement Through Common Procurement Act, a short-term instrument that allocated €310 million in 2024 and 2025 (less than 1% of overall procurement spending in 2025) to subsidize joint procurements. The European Defense Industrial Strategy (EDIS) aims to further encourage harmonization by setting a collaborative procurement target of 40% for defense equipment by 2030, more than doubling the 2021 level (18%).

These welcome efforts are just a start. European military spending on research and technology (R&T)—including activities such as basic research, applied research, and advanced technology development—has grown in recent years, reaching approximately 1.7% of total public defense spending, which is close to the EU's 2% target and is similar to the US budget for R&T. Nevertheless, only 10% of the EU's R&T spending happens collaboratively.

In the broader category of R&D spending—which includes things like product prototype development and demonstrations—the public investment gap between the US and the EU widens considerably. EU countries spend on average about 4% of their defense budgets on R&D compared to the 17% or so that the US spends on research, development, test, and evaluation, a fairly comparable set of activities. In the private sector, the situation is nearly reversed, as the top ten European defense companies by revenue spend on average roughly 7.5% of their revenue on R&D, compared to about 4.5% for their US peers. (A substantial portion of R&D spending occurs in dual-use technologies research, which cannot effectively be subdivided into military and nonmilitary components to provide an additional data point for US-Europe comparison.) This discrepancy reflects the fragmentation of weapon systems in Europe, as well as lower levels of government co-funding, which results in private companies having to make up for the shortfall in public funding. When it comes to R&D spending, European governments typically partner less with the private sector than the US Department of War does. **(See Exhibit 6.)**

EXHIBIT 6

The US Maintains a Sizable R&D Advantage over Europe, Primarily Driven by Public R&D Spending



Sources: US Department of War; European Defence Agency; S&P Capital IQ; BCG analysis.
Note: R&D = research and development; R&T = research and technology.

[1] For Europe, we used the R&T figures as reported by the European Defence Agency; for the US, we used the Department of War's budget activities categorized as "basic research," "applied research," and "advanced technology development" to calculate the R&T figure.

[2] For Europe, we used the R&D figures as reported by the European Defence Agency; for the US, we used the Department of War's research, development, test, and evaluation numbers, which the European Defence Agency considers to be comparable to its R&D figures.

[3] We used S&P Capital IQ R&D spending and revenue data for the ten largest European and US defense companies by revenue to construct the average private R&D spending figure.

Streamlining Procurement

As Europe places bets on strategic technologies, procurement systems that foster innovative and scalable solutions will improve performance. **Prior BCG research** has shown that demand can exert the right pull: shortening procurement cycles to better match the pace of technology development, raising startups' risk tolerance to access government contracts, and promoting longer-term contracts that support capacity-building investment by defense companies.

Such efforts could help shake the stasis that currently afflicts European defense startups in the form of risk-averse trials, lengthy qualifications, and difficult integration into multinational networks. All of these constraints make it difficult for technology pilots to develop into speedy, scalable, and affordable deployment.

Here again, Europe's renewed sense of defense urgency has yielded promising early-stage initiatives. EDIS and the European Defence Industry Programme explicitly seek to push joint orders, prioritize European systems, and accelerate capacity ramp-up; and the ReArm Europe initiative aims to provide large-scale financing to transform these policy ambitions into actual industrial investment and multiyear joint procurement.

The ultimate success of these programs, however, depends on the ability of individual countries to pool demand and align regulatory requirements. NATO and EU officials warn that there is little margin for error: if new rules harden into market barriers or if countries spread their procurement funds too thinly, costs will rise and delivery could lag, undermining efforts to improve adoption.

Charting a Path Forward

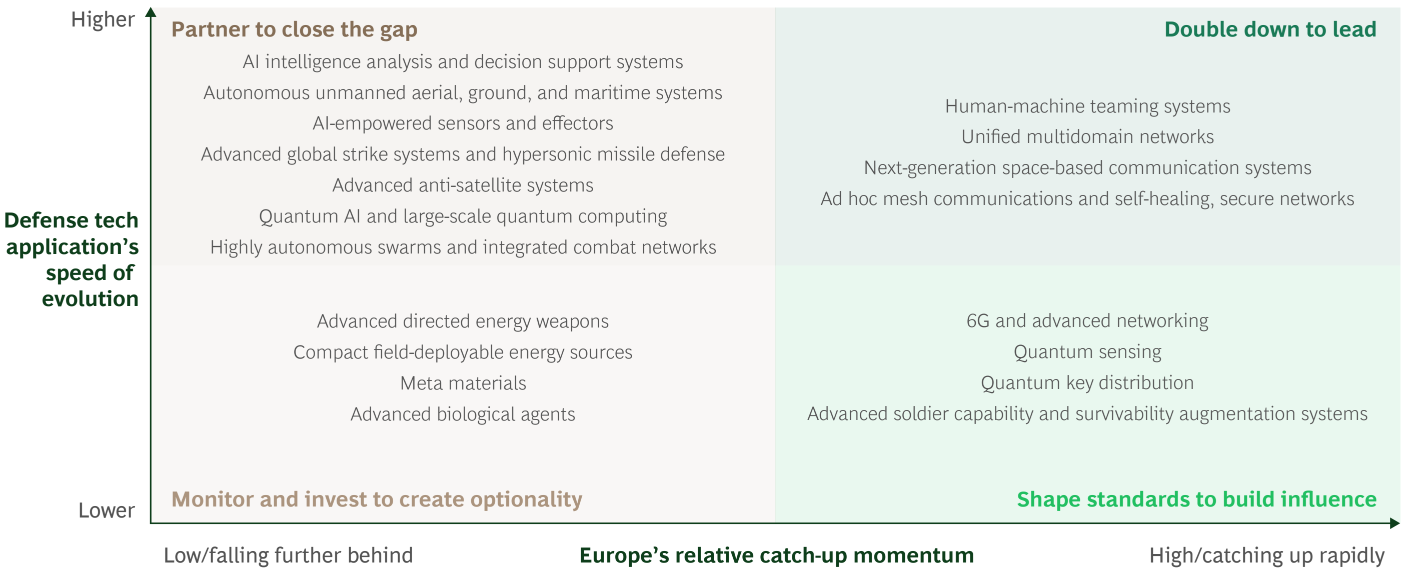
The goal for Europe should not be to lead on all frontier defense tech applications. The region's resources are limited, the capability gaps in legacy systems are too great, and the need to bridge them is too urgent. Policymakers will need tools to help them decide where to place strategic bets—to lead where Europe can, to catch up where it must, and to rely on partners and allies where doing so is most practical.

To help leaders make those decisions, we grouped our 19 high-impact defense tech applications by the speed at which each technology is evolving as well as by the degree to which Europe is either closing the gap with or falling farther behind the global leaders. On the basis of this analysis, we identified four distinct categories, each of which calls for a differentiated strategic posture from Europe **(see Exhibit 7)**:

- Partner to close the gap.
- Double down to lead.
- Shape standards to build influence.
- Monitor and invest to create optionality.

EXHIBIT 7

A Prioritization Framework for Navigating Frontier Defense Technology Investments



Higher

Defense tech application's speed of evolution

Lower

Partner to close the gap

AI intelligence analysis and decision support systems
Autonomous unmanned aerial, ground, and maritime systems
AI-empowered sensors and effectors
Advanced global strike systems and hypersonic missile defense
Advanced anti-satellite systems
Quantum AI and large-scale quantum computing
Highly autonomous swarms and integrated combat networks

Double down to lead

Human-machine teaming systems
Unified multidomain networks
Next-generation space-based communication systems
Ad hoc mesh communications and self-healing, secure networks

Advanced directed energy weapons
Compact field-deployable energy sources
Meta materials
Advanced biological agents

Monitor and invest to create optionality

6G and advanced networking
Quantum sensing
Quantum key distribution
Advanced soldier capability and survivability augmentation systems

Shape standards to build influence

Low/falling further behind

Europe's relative catch-up momentum

High/catching up rapidly

Sources: BCG private and public sector defense expert survey; BCG analysis.
Note: "Europe" encompasses the UK and all countries that are in both the EU and NATO.

Although the exact categorization of each individual defense tech application will inevitably change over time, this framework articulates an approach to setting and revisiting investment priorities. Crucially, such prioritization must account for the specifics of each country's defense strategy, which may single out specific technologies that the nation deems essential to develop domestically. The key is to adopt an approach that balances long-term optionality with short-term urgency, and exploitation of current strengths with exploration of novel possibilities.

Partner to close the gap. In areas where Europe has fallen significantly behind global frontrunners—applications such as AI-driven command systems, autonomous swarms, and hypersonic defense—the region may not be able to make up the difference on its own even with substantial investment. In these cases, European leaders can prioritize developing interoperability, as well access to and strategic participation in global value chains. Collaborating in this way can help the region achieve operational parity while creating opportunities for knowledge transfer.

For example, the European Sky Shield Initiative combines European-made IRIS-T surface-launched missiles with US Patriot and Israeli Arrow-3 interceptors. Europe also uses coordinated funding resources to attract allied partners such as Canada, which became the first non-European country to participate in the €150 billion loan program, Security Action for Europe.

In the private sector, the German firms Hensoldt and Rohde & Schwarz contribute advanced sensor and signal-processing technology to US-led platforms, while retaining intellectual property and know-how in Europe. Such efforts illustrate how layered cooperation can close capability gaps and generate demand that progressively builds domestic expertise.

Double down to lead. Europe is progressing faster than its peers in tech applications such as human-machine teaming systems and space-based communication systems, according to the senior defense experts we surveyed. European companies such as Airbus Defence, Space, and Leonardo, are already working on next-generation communication networks. The German startup Helsing is embedding AI-driven mission software into existing combat platforms, like Saab's Gripen, to enable human-machine teaming.

Maintaining that momentum and translating that R&D strength into real world applications before competitors leap ahead will require sustained investment and coordination. Ensuring adequate demand for finished products is crucial. The European Defence Fund can help by co-financing R&D and funding pre-series production and operational trials. Simplifying export and certification processes would allow European innovations to reach the field faster and compete globally.

Shape standards to build influence. In areas such as quantum sensing, where technological evolution is slower and Europe is well-positioned to lead, the region has a strategic window to influence global standards and embed European design principles into future systems. Europe's institutional strengths in coordination and regulation can help it project influence beyond its borders.

France and the UK have accomplished this recently with their unmanned-systems doctrines, setting out operational parameters that give them influence over how the sector operates now and in the future. The European Secure Software Defined Radio project developed a common tactical communication waveform that NATO subsequently adopted as its standard. This demonstrates how collaborative European engineering, when strategically deployed, can define global interoperability norms.

Monitor and invest to create optionality. Europe may be falling behind in some defense tech applications that are evolving at a slower rate. In cases like these, where there is a longer runway before the technology reaches maturity, Europe can take a portfolio approach: monitor global progress, fund selective proof-of-concept trials, and preserve optionality with limited investment. This is an area where national innovation hubs are particularly valuable. France's Agence de l'innovation de défense and the UK's Defence and Security Accelerator are examples of small, agile grant programs that maintain situational awareness while preparing for sudden breakthroughs.

If Europe successfully balances legacy and new technologies, it will secure its long-term defense posture and regain the ability to shape the technologies and standards that will define tomorrow's security environment. With world-class research strength, rising defense spending, and new policy instruments, the region has the foundation in place for leadership—if it channels that momentum into stronger demand pull, faster adoption, and more coherent procurement across borders.

The benefits extend far beyond military readiness. As research by **BCG's Center for Macroeconomics** shows, the new NATO defense spending target of 5% of GDP by 2035 could accelerate European NATO countries' GDP growth by an average of 0.3% annually over the next ten years. A more dynamic defense innovation ecosystem would act as a **catalyst for Europe's wider industrial base**, too, reinforcing sectors like automotive, aerospace, energy, and advanced materials through new technologies, skills, and supply-chain depth. By closing the commercialization gap—turning world-leading research into scalable products—Europe can boost competitiveness, attract investment, and strengthen economic resilience. In this way, getting defense tech right is not just a security imperative; it is an industrial strategy with continent-wide impact.

Appendix: NATO's Nine EDTs

NATO's emerging and disruptive technologies (EDTs) are nine fast-advancing technology areas that the alliance has identified as having the greatest potential to transform future warfare. NATO defined these EDTs through analytical work that drew on expert consultations, proprietary research, and technological trend assessments to prioritize the fields where innovation will have the greatest strategic impact.

Cyber is an enabler, vulnerability, and battlespace that interacts directly with each of the nine NATO EDTs discussed in this article. Cyber operations are already a clear and present threat in modern warfare—from disabling air-defense networks and spoofing satellite links to corrupting logistics software or attacking critical infrastructure. As defense systems become more autonomous, more connected, and more software-defined, cyber offense and cyber defense become inseparable from physical capabilities. Leading militaries now routinely integrate cyber effects with electronic warfare, space assets, and kinetic strike options. Recent conflicts have shown how cyber intrusions can blind sensors, degrade command networks, paralyze critical infrastructure, and undermine public trust—all before a shot is fired.

Artificial Intelligence

AI significantly enhances the speed, precision, and scale at which military forces can process information and make decisions. It enables automated detection and classification of threats, supports real-time decision support tools for commanders, and optimizes logistics, maintenance, and force allocation. In contested environments, AI strengthens cyber defense through adaptive responses, and it underpins advanced mission systems such as autonomous target recognition and electronic-warfare analysis. Examples include AI-enabled intelligence analysis that rapidly fuses satellite, drone, and sensor data; predictive maintenance systems for aircraft fleets; and automated mission-planning tools.

Cyber shapes the strengths and the vulnerabilities of AI-enabled systems. Hostile forces can target AI models through adversarial attacks, data poisoning, or spoofed sensor inputs—tactics observed in attempts to degrade Ukrainian intelligence, surveillance, and reconnaissance (ISR) feeds. At the same time, AI can significantly enhance cyber defense through automated anomaly detection, malware classification, and rapid triage of intrusion signals.

Quantum Technologies

Quantum technologies promise step-changes in sensing, timing, navigation, secure communications, and computing. Quantum sensors can detect submarines or stealth platforms by sensing minute gravitational or magnetic anomalies. Quantum clocks offer highly accurate navigation even when GPS is denied. And quantum communications enable secure, tamper-resistant links for command and control. Longer-term, quantum computing may enhance cryptography, materials discovery, and optimization for logistics or battlefield decision making. These capabilities could fundamentally alter situational awareness and resilience.

Quantum key distribution strengthens cyber resilience by enabling secure communications, while quantum sensing and timing require uncompromised data pathways. Looking ahead, large-scale quantum computing could break current cryptographic standards, reshaping the future of cyber offense and cyber defense.

Autonomous Systems

Autonomous systems operate with varying degrees of independence from human control, expanding operational reach, persistence, and survivability across all domains. They enable militaries to conduct dangerous, repetitive, or long-endurance missions without putting personnel at risk. Such systems include uncrewed aerial vehicles for surveillance and strike, autonomous ground vehicles for logistics or casualty evacuation, and unmanned surface and underwater vehicles for mine countermeasures or maritime patrol. Increasingly, these platforms operate in coordinated teams or swarms and integrate directly with crewed systems in multidomain operations.

Cybersecurity is central to autonomy. Uncrewed aerial, ground, maritime, and underwater systems are subject to hijacking, jamming, or misdirection. In Ukraine, both sides have used GPS spoofing and electronic intrusion to interfere with drones. Swarms rely on secure intraswarm communications, which makes them especially sensitive to cyber manipulation.

Biotechnology and Human Enhancement Technologies

Biotechnology enables militaries to improve force protection, readiness, resilience, and recovery. It encompasses rapid field diagnostics, biosurveillance tools for emerging biological threats, advanced medical treatments such as regenerative therapies, and materials or systems inspired by biological processes. Human enhancement technologies range from exoskeletons that reduce physical burden, to improved protective gear, to cognitive-support tools that help personnel operate effectively under high stress. In operational settings, these technologies can reduce casualties, increase endurance, and accelerate recovery times.

Cyber intersects with digital biodesign tools, genetic databases, and wearable soldier-systems. Attackers could target bioinformatics platforms, compromise diagnostics or biosurveillance algorithms, or interfere with AR/VR-based soldier enhancement systems.

Space

Space capabilities provide the backbone for modern military operations by enabling global communications, navigation, intelligence, surveillance, and early-warning systems. As adversaries invest in counter-space weapons, the need for resilient architectures, distributed constellations, and rapid-launch capabilities becomes critical to maintaining operational continuity. Defense-relevant applications include ISR satellite constellations for persistent monitoring, space-based missile-warning sensors, protected satellite communications for allied forces, and responsive launch vehicles that can replenish damaged or degraded space assets quickly.

Satellites and ground stations are high-value cyber targets. The Viasat KA-SAT hack in 2022, which disrupted Ukrainian communications on the eve of the invasion, showed how cyber operations alone can degrade space assets. Cyber hardening is essential to protect space-based ISR, missile warning, and command-and-control links.

Hypersonic Systems

Hypersonic systems—whether glide vehicles or cruise missiles—travel at speeds above Mach 5 and can maneuver unpredictably, reducing warning times and challenging existing air and missile defenses. Their development alters deterrence dynamics by enabling rapid strikes on high-value, time-sensitive targets. Correspondingly, defensive efforts focus on developing advanced sensors to detect hypersonic threats, new tracking architectures, and interceptor systems that can operate effectively at extreme velocities and altitudes. This area also includes enabling technologies such as precision guidance at hypersonic speeds.

Hypersonic kill chains depend on real-time sensor fusion, guidance software, and resilient communications. Cyber intrusions at any point—including sensor inputs, data links, or fire-control systems—can degrade detection or delay intercept timelines, compromising integrated air and missile defenses.

Novel Materials and Manufacturing

Novel materials and advanced manufacturing methods improve platform performance, survivability, stealth, and sustainability. Lightweight composites and bio-inspired materials reduce weight while enhancing protection; metamaterials can improve radar absorption or antenna performance; and additive manufacturing allows militaries to produce spare parts or components at the tactical edge, reducing supply-chain vulnerabilities. These technologies shorten development cycles, lower production costs, and enable design innovations that were previously impractical.

Advanced materials and additive manufacturing workflows rely on digital design files and machine-control software. Cyber tampering—such as altering lattice structures or implanting micro-defects—can silently compromise the structural integrity of aircraft, armor, or missile components. Furthermore, research into advanced materials is highly vulnerable to intellectual property theft.

Energy and Propulsion

Next-generation energy and propulsion systems support platforms that require higher endurance, reduced signatures, or greater power output. Hybrid-electric and alternative-fuel propulsion systems reduce reliance on vulnerable fuel logistics and extend mission duration for ground and air platforms. Compact power sources enable emerging high-energy systems such as directed-energy weapons. In the maritime and space domains, advances in high-efficiency propulsion systems provide greater range, agility, and operational flexibility.

Innovations in energy and propulsion increasingly depend on digital control systems. Cyber attacks can disrupt power management, alter thermal regulation in high-energy weapons, or disable hybrid-electric propulsion in vehicles of various kinds, including unmanned aerial vehicles.

Next-Generation Communication Networks

Next-generation communication networks provide secure, resilient, high-bandwidth connectivity across dispersed forces and contested environments. They support real-time data fusion, coordinated multidomain operations, and integrated autonomous systems. These networks rely on advanced spectrum management, anti-jamming technologies, and architecture such as 5G/6G tactical networks, mesh networks that self-heal under attack, and edge-computing nodes that process data locally to reduce latency. Effective communication networks underpin operational tempo and ensure interoperability among allies.

Future 5G/6G and multidomain networks will be prime cyber battlegrounds. Adversaries may saturate self-healing mesh networks, inject false routing data, or jam key tactical nodes—as seen in contested electronic warfare environments in Ukraine.

The nineteen key defense technology applications discussed in the main text of this article map into the nine NATO EDTs detailed above. For a more detailed description of each of the 19 applications and how they are distributed within the EDTs, **see the exhibit**.

NATO's Nine NATO EDT Areas Provide a Framework for Categorizing 19 Technologies with Potentially Great Strategic Impact

Domain	Application	Description
Artificial intelligence	AI-empowered sensors and effectors	Sensors, radar, and weapon systems that use AI to autonomously detect, classify, and respond to threats in real time, increasing speed and precision while reducing operator workload. They enable adaptive targeting and countermeasures in contested environments. Example: Israel's Iron Dome air defense system enhanced with AI-based radar discrimination to identify and intercept incoming rockets.
	Intelligence analysis and decision support systems	AI systems that process vast amounts of data—including satellite images, reports, and signals—to help commanders make faster, more accurate decisions. Example: Palantir's AI tools used by Ukraine to integrate battlefield data and guide targeting.
	Human-machine teaming systems	AI that enables seamless collaboration between humans and machines, such as pilots working with AI copilots or operators working with robotic teammates. Example: DARPA's Air Combat Evolution program, where AI copilots assist fighter pilots in aerial maneuvers.
Quantum technologies	Quantum key distribution	Communication protected through quantum entanglement, making it impossible to intercept without detection. Example: China's Micius satellite successfully demonstrated quantum key distribution between ground stations thousands of kilometers apart.
	Quantum sensing	Ultra-precise sensors that use quantum effects to detect submarines, underground bunkers, or navigation signals without GPS. Example: the UK's Quantum Accelerometer tested as a GPS-independent navigation device.
	Quantum AI and large-scale quantum computing	Use of quantum computing to solve complex defense problems such as route planning, logistics, or materials design much faster than classical computers can. Example: DARPA's ONISQ program to test quantum computing algorithms for defense-relevant optimization problems such as logistics planning and resource allocation.
Autonomous systems	Autonomous unmanned aerial, ground, and maritime systems	Vehicles and platforms that can operate with minimal or no human control, using onboard AI to navigate, detect threats, and execute missions. This encompasses both offensive and defensive applications, as well as technologies designed to counter such systems. They reduce operator workload and enable missions in dangerous or GPS-denied environments. Example: the US Navy's Sea Hunter unmanned surface vessel.
	Highly autonomous swarms and integrated combat networks	Groups of drones or robots operating together across all domains and/or as a swarm, coordinating their actions autonomously for attack or defense. Example: the US Navy's LOCUST drone swarm program, which entails launching dozens of drones that coordinate as a single system.
Biotechnology and human enhancement	Advanced biological agents	Engineered biologics that can be used for defense (as in the case of vaccines and antidotes) or pose threats (as in the case of bioweapons). Example: DARPA's Pandemic Prevention Platform working on rapid-response antibody therapies.
	Advanced soldier capability and survivability augmentation systems	Systems that enhance soldier capabilities, resilience, and protection, including chemical, biological, radiological, and nuclear defense and rapid battlefield medical support. Examples: cybernetic enhancements, exoskeletons, AR-headsets, self-administered and automated care systems, and evacuation drones.

Domain	Application	Description
Space	Advanced anti-satellite systems	Technologies to disable or destroy enemy satellites or protect one's own. Examples: India's 2019 ASAT missile test, which shot down a satellite in low Earth orbit; China's testing of similar systems since 2007; the US's 2024 accusation that Russia is building nuclear anti-satellite weapons.
	Next-generation space-based communication systems	Secure, resilient LEO satellite constellations for global military communications. Example: SpaceX Starlink being used by Ukraine for battlefield connectivity.
Hypersonic systems	Advanced global strike systems and hypersonic missile defense	Weapons that travel at speeds in excess of Mach 5, launched from space or near-space, able to strike land and maritime targets globally with little warning; including systems that can defend against such strikes. Examples: China's DF-17 hypersonic glide vehicle tested for long-range precision strikes and its DF-21 "carrier killer."
Novel materials and manufacturing	Meta materials	Engineered materials with properties not found in nature. Examples: stealth coatings; advanced and negative-index metamaterials that bend electromagnetic waves in the opposite direction of conventional materials.
Energy and propulsion	Advanced directed energy weapons	High-energy lasers or microwave systems that can disable targets at the speed of light. Examples: the US Navy's HELIOS laser weapon mounted on destroyers for drone defense; Israel's Iron Beam.
	Compact field-deployable energy sources	Portable, stealthy/silent, high-capacity power systems to support troops, vehicles, and advanced weapons in the field. Example: Rolls-Royce's small modular nuclear reactor concepts for defense applications.
Next-generation communication networks	6G and advanced networking	Ultra-fast, ultra-reliable networks that surpass 5G, enabling low-latency military data sharing. Example: Nokia and Ericsson developing 6G prototypes for future defense communications.
	Unified multidomain networks	Integrated networks connecting land, sea, air, space, and cyber forces into a seamless combat cloud. Example: NATO's Federated Mission Networking framework that enables allied forces to operate on a shared multidomain command-and-control network.
	Ad hoc mesh communications and self-healing, secure networks	Decentralized, adaptive communication systems that reroute automatically if nodes are destroyed or jammed. Example: Soldier radio mesh networks that continue operating after attacks on infrastructure.

Sources: BCG internal expert panel; BCG analysis.

About the Authors

Nikolaus Lang is managing director and senior partner in the Munich office of Boston Consulting Group. He is the global vice chair of the firm's Global Advantage practice and the global leader of the BCG Henderson Institute. You may contact him by email at **lang.nikolaus@bcg.com**.

Greg Mallory is a managing director and senior partner in BCG's Washington, DC office and the global leader of BCG's defense and security sector. You may contact him by email at **mallory.greg@bcgfed.com**.

Jona Lampert is a consultant in BCG's Doha office and a BCG Henderson Institute ambassador. You may contact him by email at **lampert.jona@bcg.com**.

Philippe Lavigne is a senior advisor in the firm's Paris office, former NATO Supreme Allied Commander Transformation, and a retired four-star general and chief of staff of the French Air and Space Force. You may contact him by email at **lavigne.philippe@advisor.bcg.com**.

Rami Rafih is a managing director and partner in the firm's Riyadh office and the BCG Henderson Institute regional leader for Europe, the Middle East, South America, and Africa and the Global Advantage practice area lead for that region. You may contact him by email at **rafih.rami@bcg.com**.

David Zuluaga Martinez is a senior director for geopolitics at the BCG Henderson Institute, working from BCG's Brooklyn office. You may contact him by email at **zuluagamartinez.david@bcg.com**.

For Further Contact

If you would like to discuss this report, please contact the authors.

Acknowledgments

The authors would like to thank Fabio Dal Pan, Louis Watt, Michael Dahle, Diana Dimitrova, Pelayo Losada, Jerome Rein, Marcus Riseid, Romane Roche, Christian Schwaerzler, Sebastian Schrapp, Annika Zawadzki, Marc Van Grondelle, Ton Van Loon, Peter Bacon, Matthieu Ertaud, Florian Lemoine, and Hugh Eaton for their contributions to this article.

BCG

BCG HENDERSON INSTITUTE