



Future of defense



KPMG International

kpmg.com/connecteddefense



Introduction

With volatility and change being a constant, today's defense forces are in a race to adapt and transform. Success in the future battlefield is heavily dependent upon fast decision-making, driving an agile response to ever-changing circumstances. There is a critical need to accelerate digital adoption working in concert with alliance partners and, where appropriate, commercial providers to help national defense investments deliver their intended capability and capacity. The challenges to western dominance in national security require a coordinated response to the many challenges facing the sector. In this report, we seek to imagine the world of defense towards the end of this decade, looking at rapid digital modernization, geopolitical forces, battle space and weapon systems, the emerging space and cyber domains, supply chains, the growing threat of climate change, and the future of work.

Speed is becoming a major competitive differentiator: speed of communication, of decision-making, and of weapons themselves. Wireless 5G, 6G and possibly 7G, as part of edge computing, allow defense forces to process enormous volumes of information and deliver real-time insights to key decision makers, helping them respond to challenges like hypersonic missiles. This calls for larger computer platforms and the latest software, as well as equal access to superfast telecommunications for all partner countries.

Simulation and forecasting are enhancing planning, command and control, with advances such as digital twins enabling war gaming across multiple scenarios, with hundreds or even thousands of variables. At a stroke, a commander can determine the impact of decisions or events in real time and make more confident moves.

With every force, country and corporation harvesting huge amounts of data every day, it is important to make use of this information to help improve defense effectiveness, while keeping it secure and private. Not only is this important for the benefit of citizens, it is critical in helping avoid sensitive information and data getting into the hands of adversaries.

Another major development is the transition from humans to robots, with machines and autonomous vehicles likely to feature prominently on the future battlefield. And, as healthcare becomes ever more digitalized, we expect to see tech-enabled humans emerge following injuries.

In a virtual world, what's real and what's reliable? Digital technologies can open the door to infiltration and misinformation. To combat these emerging threats, defense forces should look to develop capabilities to detect hacks and spot untrustworthy information, people and organizations.

We expect future defense forces to be connected from front to back, and we conclude this paper by looking at the kinds of capabilities that can help forces thrive, such as data and analytics, mission centricity, responsive supply chain and logistics, technology architecture, and, of course, people, including relationships with allies and industries.

**Signals of
change**

**Future
operating
model**

**KPMG
Connected
Enterprise
for Defense**

**Get in
touch**



Connected capabilities can enable an effective defense force

A connected defense force uses the power of digital capabilities and the cloud to seamlessly connect the organization from the back office to the front, enabling fast, informed decision-making and agility to help respond decisively to volatility. We believe this requires maturity in eight critical capabilities:

Insight-driven strategies and actions	Harness data, advanced analytics and actionable insights with a real-time understanding of mission and defense organizations to help shape integrated decisions.
Innovative platforms and services	Develop compelling stakeholder value propositions on cost, platforms and capabilities to engage some of the most critical stakeholders and help drive maintenance of a force-ready posture.
Mission centricity by design	Design seamless, intentional experiences for stakeholders, employees and partners, supporting force delivery propositions and helping to deliver strategic objectives.
Seamless interactions	Interact and engage with stakeholders, allies and partners across platforms and domains to plan and execute on common objectives and help achieve measurable results.
Responsive operations and supply chain	Operate with efficiency and agility with the goal of fulfilling the strategic mission in a consistent and cost-effective way.
Integrated partner and alliance ecosystem	Engage, integrate and manage third parties to help increase speed to market, reduce costs, mitigate risk and close capability gaps to deliver the strategic mission.
Aligned and empowered workforce	Build a mission-centric organization and culture that inspires people to deliver on the strategic mission and productivity dividends.
Digitally enabled technology architecture	Create intelligent and agile services, technologies and platforms, enabling the strategic agenda with solutions that are secure, scalable and cost-effective.

Lastly and importantly, defense organizations should examine the organizational barriers that could be preventing them from taking advantage of this digital future. It is easy to agree that speed of adoption is a key goal for many defense forces, but it can be much harder to address the root cause of barriers in structure, governance and legacy practices that can inhibit progress.

Signals of change

Future operating model

KPMG Connected Enterprise for Defense

Get in touch



Contents

05
Signals of change



24
KPMG
Connected
Enterprise for
Defense



Digital modernization **06**

Rapidly evolving geopolitical landscape **09**

Future battle space and weapon systems **11**

The emerging space domain **12**

The cyber domain **14**

Agile supply chains **16**

Climate change **18**


The future of work **19**

High-maturity organizations continue to outpace their less mature peers **25**

Evaluating your capability maturity **26**

Making it happen **27**

21
Future
operating
model



28
Get in touch



Signals of change

Future operating model

KPMG Connected Enterprise for Defense

Get in touch



Signals of change

What is shaping the defense landscape over the next decade? Digital modernization is helping forces become faster, more agile and better connected, while geopolitical shock waves are ushering in a new era of great power competition. Supply chain ruptures and security concerns are contributing to a rethink of sourcing footprints, and climate change is impacting forces' ability to operate, creating potential conflicts and necessitating assistance to civil society. This section explores these and other signals of change and assesses what is expected to be their impact on defense organizations.



Signals of change

Future operating model

KPMG Connected Enterprise for Defense

Get in touch



1. Digital modernization

Main trends

- Speed is a significant differentiator to gather and process data and generate insights for decision makers — enabled by data management and analytics.
- Robotics, autonomous vehicles and nanobots are augmenting and in some cases replacing humans.
- The metaverse/simulation helps defense forces build quicker and more accurate scenarios to test out decisions.
- Cloud, 5G/6G and multi-domain connectivity are powering a connected defense force.

Summary

Faced with the challenge of emerging weapon systems and platforms such as hypersonic missiles, forces are under pressure to make quick, informed decisions, to adapt to changing situations, processing huge amounts of information on ever-more powerful and smaller computers using sophisticated software. These capabilities should be available to support forces in anticipating and responding effectively, while helping to avoid mistakes. These high-speed systems and platforms are likely to be enabled by completely wireless 5G, 6G or even 7G secure networks — although not all countries are expected to develop these technologies at the same pace.

Like many organizations, defense forces are still exploring the power of data gathered from a wide variety of sources. By following the examples of big tech companies and pulling different strands of data together, defense and intelligence organizations can generate essential insights that aid both strategic and battlefield decisions. However, more data and faster processing can lead to more opportunities for adversaries to distribute compromised communications that could influence both combat decisions and public opinion. All defense organizations should ensure that data and messages are trusted and tamper-proof.

In our view, the management of data becomes a key component of future success. It impacts frontline decision-making, which is reliant on fusing together multiple internal and external data sources.

Data analytics is also leading to transformation in health management, with faster triage and treatment for battlefield injuries — including chemical and biological — and real-time tracking of personnel conditions and well-being via sensors in uniforms. Medical officers should be able to identify dehydration and other physical signs (which is particularly important as climates get hotter) and swiftly decide whether individuals can operate effectively and for how long.

Among the exciting new emerging technologies are the convergence of ‘wet’ (i.e. human body) with ‘dry’ technologies like silicone and computing, where humans are augmented with implants, 3D-printed artificial limbs and eyeballs, connected to and controlled by the human brain, enabling injured or even healthy fighters to become stronger. These are just some of the many new technology developments around the world. Governments, defense forces and private industry players should look to collaborate on investing in innovation to help ensure their technology is high-quality and scalable. As these innovations become mainstream, it’s vital to protect intellectual property (IP) to help prevent them from getting into the hands of adversaries for possible negative uses.

Robots and autonomous vehicles are gradually replacing humans, having already proven their worth in hostile conditions like on the planet Mars. They are also getting smaller, with clouds of AI-powered, microscopic bots/nanobots incorporating facial and uniform recognition. With the ability to ‘loiter’ in the same spot for hours and be completely invisible to their targets, the use of nanobots is likely to increase, and detection is expected to become a high priority.

Digital twins have the potential to simulate battlefield developments, helping defense leaders to test out tactics ahead of or in parallel with real-life events, feeding in data from conflicts and from training exercises, and producing insights for leaders on the frontline. As the software gets more advanced, and the data processing speeds increase, this approach will likely become more and more reliable. In our view, quantum computing will make it possible to input and process thousands of variables simultaneously, helping to dramatically improve decision-making accuracy.

Signals of
change

Future
operating
model

KPMG
Connected
Enterprise
for Defense

Get in
touch



How to respond

To help be future-ready, defense organizations should rapidly adopt secure digital operating models that give decision makers at all levels greater insight, choice, transparency and accuracy. This is especially important given the expected rise in conventional great power competition, and the need to make defense spending more impactful, both nationally and as part of alliances.

In our view, achieving a connected force calls for scaled adoption of the eight capabilities that KPMG has developed for successful, digitally-driven organizations, with particular focus on cloud transformation, connectivity and data. Indeed, data is a key enabler of future defense activity, expanding the use of cloud at differing security levels, powered by 5G networks and integrating with legacy, on-premise infrastructure and systems. Data governance is critical to delivering reliable insights that support rapid and effective decision-making. For more on KPMG's [eight critical capabilities](#) of a connected defense force, see the [Introduction](#) and [Future operating model](#) sections of this report.

Defense forces are progressively shaking off the constraints of on-premise infrastructure in a bid to leverage innovation in the commercial sector, connecting edge technology — deployed on the future battlefield — with central command. Given the emerging and varied security and network demands, early and concurrent investment in enterprise architecture, we believe data and cyber is required to access the full benefits of the cloud.

The cloud can help overcome challenges of distributed defense operating environments, linking core transaction systems in logistics, personnel and finance, bringing analytics capability to the user, and disentangling the on-premise constraints. In our view, a successful shift to the cloud is dependent above all on an operating model change, together with robust cyber security. Some jurisdictions are likely to opt for a multi-cloud

approach, retaining sovereign control over key and highly classified remaining networks, while others may choose private cloud solutions. This approach is accelerating at pace in all major defense departments and will likely continue for the next 5 years and beyond.

Secure, multi-domain connectivity is another important objective of a modern defense force, seamlessly linking complex weapon systems, command and control systems, and allies and supply chains. In this fifth-generation battlefield, all forces, platforms and systems connect in near real-time, giving commanders and decision makers a new level of complete, accurate and actionable information. Most defense departments are progressively buying fifth-generation assets but lack the connected tissue to enhance the impact of these investments.

Given the increasingly global nature of defense, organizations should aim to master data governance and management to help cope with multiple data inputs across distributed systems and platforms. A reliable, responsive command and control system requires programs of work that can pull and analyze data from disparate sources simultaneously — often via sensors — to enable near real-time decision-making and predictive analyses. For many, this means stepping up to a new level of governance and collaboration.

By incorporating smart artificial intelligence (AI) and machine learning (ML) into core platforms, the next generation of weapon systems is expected to be able to swiftly align with mission intent, helping to minimize the possibility of unintended application, and communicating with command-and-control systems in near real time.

With the increased adoption of control towers, commanders at all levels can simulate possible courses of action to aid decision-making and plan alternatives, using digital twins as an essential planning capability.

Tackling commercial leakage

Defense forces can lose hundreds of millions of dollars due to overpayment of invoices as a result of inadequate, manual reconciliation processes. This is especially relevant given the expected growth in defense spending in the coming years. KPMG's AI-driven technology enables defense organizations to audit suppliers, identify leakages and help them recoup significant investments against agreed contractual terms.

Signals of change

Future operating model

KPMG Connected Enterprise for Defense

Get in touch



Insights at your fingertips

Effective strategic, operational and tactical decisions are mostly dependent on fast, accurate insights from increasingly large volumes of often unstructured data. KPMG member firm professionals have supported the development of a Health of Capability Dashboard (HoCD) to provide forces with a single digital platform to help them better understand how prepared they are and simulate the impact of different decisions on their capability levels. It helps forces manage their capital investment program, giving an end-to-end view of the development, operation and sustainment of assets. Forces can simulate the 'future' performance of equipment and visualize usage patterns, with AI and machine-learning constantly refreshing the database. Information is delivered in easy-to-read dashboards and visualizations, giving greater confidence in critical decision-making.

Signals of change

Gaining a digital edge

An extensive data program is transforming a national defense force's data management and building a stronger, professional data workforce and culture. The program is delivering secure and resilient information systems that enhance data sharing and collaboration across government and strategic partners. By leveraging the capability to gather increasing quantities of data from military drones, aircraft, land vehicles and maritime vessels, the force can provide vital battlefield insights. Data is now treated as a strategic asset that can significantly boost performance. Working with a number of other industry-leading suppliers, KPMG member firms have acted as a preferred systems integration supplier in this two-year, US\$300 million plus program that is helping to change the face of information management across the defense force.

Future operating model

KPMG
Connected
Enterprise
for Defense

What should defense organizations do?

1

Accelerate investment in digital modernization, which has become a key driver of defense capacity and effectiveness, integrating countries' platforms, systems and capabilities, which should be interoperable with allies and coalition partners and linked to selected industry partners. This typically requires the reprioritization of scarce investment dollars. If not acted upon, this can significantly degrade all other investments.

2

Recognize that concurrent planning and investment in both capability-specific accelerators and core transaction systems are vital to provide data of the quality required to enable digital accelerators to be effective in delivering the enterprise and mission objectives of the organization.

3

Look beyond conventional platforms, assets and force structure, and appreciate the benefits of greater digital capability and transparency of decision-making at a whole-of-department level. New, bespoke capabilities and structures in space and cyber should also be integrated into new platforms and capabilities.

Get in touch



2. Rapidly evolving geopolitical landscape

Main trends

- There is a re-emergence of great power competition — and the response of traditional and emerging alliances.
- Investment trade-off between conventional and new capabilities is a reality.

Summary

Continued geopolitical instability, with a jostling for position in the Indo-Pacific region and conflict in Eastern Europe, is expected. The re-emergence of great power competition is likely to be the primary influence on the defense arena over the near term, a shift in emphasis from the rogue state and counter terrorism agenda of the past decade.

In our view, much will hinge on the response of traditional (NATO) and emerging alliances (AUKUS: UK, US and Australia, and the QUAD: US, India, Japan and Australia) and support from the US. The North Atlantic Treaty Organization (NATO) is once more being tested in a post-Brexit world by events in Ukraine and other eastern states, volatility in North Africa (Libya, Syria and Yemen), enduring challenges in the Middle East and broader commitments to peacekeeping.

AUKUS and the QUAD are well established in the Indo-Pacific region and seek to build capability and

promote greater security cooperation in the region to counter growing threats. In our view, this calls for a cooperative strategy involving the sharing of innovation and intellectual property amongst alliance partners, joint training and activity, infrastructure investments in capabilities deployment, and highly connected systems.

In light of evolving geopolitics, western defense departments should balance investment in conventional platforms, assets and force structure with new bespoke capabilities and structures in domains such as space and cyber. Such uncertainty can demand diplomacy, economic levers and information campaigns, in addition to defense.

The past 3 years have seen greater economic coercion, including infrastructure programs — such as China’s Belt and Road initiative — that place significant obligations on beneficiaries, as well as direct action in the form of tariffs, trade blockages, sanctions and in-country interventions. Such measures may well be accompanied by cyber spying to better understand plans and vulnerabilities and support diplomatic, and, potentially, military action.

In response, western countries should keep abreast of such developments and establish countermeasures, including stronger cyber security and appropriate political and economic action.

Developing a robust sovereign industrial defense capability

A successful defense force needs a strong industrial base to provide it with hardware and, increasingly, software. KPMG member firm professionals worked with a national force to better understand how it was supported by local defense industry across a wide range of areas like combat clothing, munitions, submarines, land combat vehicles and radar. The KPMG team helped develop a shared vision for each capability and assessed the industrial base. They then co-produced a number of plans to align government, defense and industry plans, recommending where defense/government can support industry, facilitating further consultation and collaboration. The nation is now on a path to a well-aligned government/industrial defense strategy.

Signals of change

Future operating model

KPMG Connected Enterprise for Defense

Get in touch



Rising defense spending

In the face of considerable instability, worldwide defense expenditures increased by 3.4 percent in 2021 to reach US\$1.92 trillion, offset by surging inflation, which resulted in a 1.8 percent net reduction in real terms.¹ Both established and emerging countries bolstered their capabilities:

- The Chinese Defense budget reached US\$207 billion and accounted for 43 percent of Asia's total regional spending in 2021. Total regional spending came to US\$488 billion in 2021, more than double the 2008 total of US\$226 billion.²
- In 2021, European defense spending grew by 4.8 percent in real terms, higher than in any other region. This marked the seventh consecutive year of real-terms growth. The increase, combined with reduced spending in other regions, means that European spending represented 18.7 percent of the global total.³
- US defense budget authority fell to US\$754 billion in 2021, from US\$775 billion in 2020.⁴

- Inflation rose from 3.1 percent to 6.4 percent in 2021, which meant that the budget contracted by 6 percent in real terms.⁵

This upward trend is expected to continue in direct response to the Eastern European challenges and over the next 5 years.

Hybrid warfare

Western adversaries are engaging in coordinated and synchronized actions aimed at targeting systematic vulnerabilities; employing wide-ranging means of attack (military and other instruments of power); exploiting thresholds of detection and attribution (cyber attacks, trade responses, political posturing); exploiting the borders between peace and war (think special military operation versus war in Eastern Europe); and, in aggregate, are seeking to influence global decision makers while undermining potential targets. In our view, hybrid approach to operations requires nuanced whole-of-government/alliance responses to be effectively countered.

What should defense organizations do?

1

In order to meet heightened readiness requirements, departments of defense are expected to undertake more procurement faster, funded by increased defense budget allocations, with most western nations now at or on a path to meet or exceed the 2 percent of GDP target. This will require more agile and responsive procurement approaches, the assumption of risk as speed becomes a more paramount consideration and the need to balance requirements against the reality of medium-term threats.⁶

2

There will also likely be a build-up of sovereign defense capabilities to reduce reliance on challenged global supply chains and boost domestic industries. We expect to see governments increasingly take a whole-of-country (and associated alliances) focus in responding to geopolitical pressures.

3

Finally, there should be a growth in international and industry-specific alliances to accelerate defense force capability builds. Governments should define their contributions to future possible coalition scenarios, while maintaining appropriate independent domestic defense strength. This places more importance on existing alliances such as NATO, AUKUS, the Five Eyes (US, UK, Australia, Canada and New Zealand) and ANZUS (Australia, New Zealand and US), and will likely demand focused development of multilateral capabilities in order to help counter geopolitical threats.

Signals of change

Future operating model

KPMG Connected Enterprise for Defense

Get in touch



3. Future battle space and weapon systems

Main trends

- Future weapon systems introduce a new dimension in range, lethality, and speed.
- Connectivity between weapon systems, fighting platforms and decision makers is key, with the Internet of Things (IoT) sensors gathering data on humans and equipment.

Summary

In our view, the future battle space will be dependent on a wide range of interoperable technologies, weapon systems and platforms, which seamlessly support rapid deployment and redeployment of systems and assets, informed by highly effective battle space awareness capability. Once again, data is poised to be a key enabler, supported by secure access to connectivity and effective cyber security.

Over the past year, the range, lethality and speed of weapon systems increased further and remain a big part of military modernization in many countries — including collective blocs of nations seeking to gain advantage over potential adversaries. Examples include:

- Hypersonics (missile delivery systems being developed in the West, Russia and China) with the capacity to radically enhance kinetic weapons.
- Direct energy weapons (DEWs), such as lasers and microwave. The demand for DEWs is surging globally, having reached US\$4.1 billion in 2020, led by the US with a market share of 41.6 percent,⁷ followed by China, France, Germany, and the UK.
- Autonomy/swarm capabilities that allow for mass concentration of weapon platforms operating autonomously to respond to changing threat profiles and combat dynamics.
- Already in high use, unmanned vehicles will likely continue to grow, acting as delivery systems for advanced weapon systems on land, sea, air and space.
- Active Electronically Scanned Array (AESA) radars and secure sensors to support and manage these assets.

The next 5 years should see further development of long-range delivery systems, requiring additional investment in air and missile defense assets and systems — which had been relatively sidelined during recent counter-insurgency campaigns.

There is a growing emphasis on the connective tissue between weapon systems and fighting platforms. Defense organizations may be developing next-generation weapons and assets with fifth-generation sensors, data gathering and analytics, but they are doing so with second and third-generation connectivity to legacy systems. In the next decade, any potential conflict is likely to take place in a highly connected, intelligent battle space, calling for fully connected command and control systems to deploy weapon systems, linked to effective detection and sensing capabilities.

Government has traditionally pioneered investment in research and development, providing many new technology ideas adapted by the commercial sector, such as the internet and mobile phones. Today, however, commercial companies have taken the lead in innovation. In light of this trend, government needs to be a fast follower in platforms and technology, which influences procurement, partnership arrangements and through-life maintenance. Government should also align budgeting cycles with commerce, to help ensure effective and timely adoption.

Government and industry are converging to deliver multi-domain operations, a trend likely to intensify as conventional operations become more complex. Industry is already playing a significant role in combat service support and sustainment of systems and platforms. This capability should be swiftly integrated into deployed force packets, complete with transparent data integration.

With new weapon systems becoming increasingly software enabled, there has been a rise in sensors on people, vehicles, aircrafts and maritime platforms, in order to gather the data to coordinate weaponry. This trend is expected to be further amplified as forces adopt more autonomous systems and platforms over the next 10 years. The P-8 Poseidon maritime patrol aircraft, for example, requires secure connectivity and cloud access to feed relevant decision platforms and forums,⁸ and the next

Signals of change

Future operating model

KPMG Connected Enterprise for Defense

Get in touch



generation of German tanks will maintain connection to air force and navy assets and commands.⁹ Consequently, defense organizations should invest in interoperability of these new assets so they can work with older weapon systems and with partner forces operating in coalition.

We believe that a next-generation weapon system needs a next-generation supply chain that integrates industrial and national partners to efficiently and cost-effectively acquire assets, making them available in a timely fashion, keeping them up-to-date, and establishing and maintaining connectivity between assets and platforms.

What should defense organizations do?

- 1** Integrate next-generation weapon systems and platforms into the fifth-generation battlespace of both the individual country and alliance-based operations. Historically, the investment in integration has lagged capital investment and should now be an equal consideration in procurement and sustainment.
- 2** Implement whole-of-joint capability awareness and insight in the hands of commanders and decision makers at all levels in the chain of command. Connectivity and situational awareness are as important as the platforms themselves and can be central to success in conflict.
- 3** Invest in platforms and systems that seamlessly integrate into the fifth-generation battlefield of the future, and incentivize industry partners to deliver this outcome. Too often this has been subverted by intellectual property (IP) considerations and commercial competitive advantage — defense has the opportunity to take proactive leadership to help ensure better outcomes.

4. The emerging space domain

Main trends

- In a changing geopolitical landscape, western nations are striving to establish space as a combat and command domain.
- Key focus areas are: agreeing opportunities and challenges in space, harmonizing civilian space activity, and orchestrating ambition and maturity across nations.

Summary

Once a feature of great power competition during the cold war era, the ‘space race’ has re-emerged. Although most western nations have established space commands, commercial operators are the major driving force for innovation in this domain.

Countries that fail to create their own space domain operations will likely continue to rely on traditional and emerging alliances to protect their commercial and civilian space assets. These are mostly communication and Earth-monitoring satellites within Earth’s orbit. But, as commercial and civil activities expand within

the solar system, space is likely to demand greater defense force activity over extended distances.

The skills required by space commands happen to be some of the most in-demand Science, Technology, Engineering and Mathematics (STEM) capabilities globally and across all industries. Consequently, defense organizations need to rethink the way they attract, train and retain their workforce. For example, the US Space Force (USSF) marked its first anniversary with a STEM outreach project that will impact recruitment for decades. According to Space Force News, “The campaign was part of an enterprise-wide effort to bring STEM and space into elementary school classrooms; stand up an organization to streamline innovation and commercial partnerships; and launch a university partnership program to tap into research and innovation at the collegiate level.”¹⁰

To help acquire the pace and depth of innovation required to build effective space operations influence, space forces should form partnerships with industry, leading to greater engagement with startups.

Signals of change

Future operating model

KPMG Connected Enterprise for Defense

Get in touch



Forging a digital workforce to protect and defend the space domain

With its December 2019 establishment and release of subsequent strategic directives, the US Space Force (USSF) strives to become the first truly digital military service — in all facets of its enterprise (i.e. digital engineering, digital workforce, digital headquarters, and digital operations). Increasingly comprised of digital natives who demand rapidly accessible and intuitive applications for all parts of life, the USSF and its service members (called Guardians) are reliant on cutting-edge digital tools and techniques to operate complex weapon systems and the launch enterprise; field space domain awareness, electronic warfare, missile warning, C2, cyberspace, ISR, SATCOM, and orbital warfare capabilities, as well as navigate its business process functions.¹¹

Other countries that look to enhance their own military space operations must consider equipping its workforce with leading digital capabilities by consistently keeping the war-fighting mindset and integrated capabilities at the top of its decision-making calculus. There are plenty of solutions and platforms that exist in the global market, and picking those that directly tie back to the war-fighting missions of service branches is most critical. As the competency requirements for success in the space domain continue to evolve at a rapid pace, KPMG member firms continue to develop leading learning and development solutions to help accelerate workforce adaptation to new circumstances and operational imperatives.

What should defense organizations do?

- 1** Protect the sovereign and commercial interests of governments and citizens as civilian activity in space increases in frequency and value.
- 2** Help ensure the provision of continuity of communications to support allies in theaters of war, operating fifth and subsequent generations of weapon systems. Collaboration between allies has long been a feature of civilian space operations and extending this approach to defense can help create opportunities to enhance existing alliances, partnerships, and treaties.
- 3** Be ready to respond to new, technology-driven security risks in the space domain.
- 4** Prioritize innovative industry partnerships for co-development of space technology, assist in challenging traditional development models, and invest in skills that establish 'commercial-grade' capabilities and employee experiences within defense.
- 5** Develop an effective, flexible framework of norms, policies, and doctrines, enabling nation states to agree to terms of engagement and define threats to pursue the goal of peaceful and profitable operation. Success in space will likely be highly dependent on encouraging a culture where experimentation and fast failure become the norm to empower defense forces.

Signals of change

Future operating model

KPMG Connected Enterprise for Defense

Get in touch



5. The cyber domain

Main trends

- Cyber security is critically dependent upon achieving cyber-worthiness, helping to ensure that a system, collection of systems, or an entire platform can operate securely and effectively in a range of environments.
- Interoperability with allies is a key strategic strength, enabling vital data to be shared securely.
- To maintain cyber security, suppliers of equipment and software should be carefully vetted and monitored — ideally by a dedicated cyber-worthiness team.

Summary

Cyber threats to sovereign assets from state and non-state actors are becoming more frequent and complex. Defense forces have a major role to play in preventing or diminishing the impact of these attacks on the economic, social and cultural fabric of the nation — using both offensive and defensive cyber capabilities.

Cyber-worthiness goes beyond the traditional approach to cyber security (which looks at general resilience) by assessing the cyber risk of specific missions to achieve confidentiality, integrity and availability of resources.

Commanders need a framework for recognizing and processing cyber risks to understand vulnerabilities and make informed decisions in near real-time — helping key defense assets and systems to detect and survive cyber attacks and maintain readiness.

Given the scale of data gathered by next-generation weapon systems, automation plays a significant role in helping to effectively analyze and provide insights at the point of collection. Bandwidth remains a challenge on the battlefield, as medium orbit and geosynchronous satellites often fail to cover the required capacity. One option is to flood low Earth orbits (LEO) with mass bandwidth, although this can be used by other — possibly adversary — forces.

Sovereignty, security and sharing

Connectivity introduces a number of challenges, including security of data held in other countries, and the ability to act without another government's consent. Edge computing brings additional risks from unfriendly nation states potentially involved in the manufacturing of hardware and data storage. Malware is less of a concern for top secret and

secret data, which is not generally connected to the internet; however, this is not the case for lower-level data, which carries a higher risk.

Although a global cyber governance network may become the norm, such an approach may conflict with the political agenda of individual country forces. As advanced weaponry becomes more prevalent, defense organizations need a more holistic approach to assessing and managing the risks posed by cyber attacks, both to the weapon systems and their human operators.

In managing sharing and interoperability, each nation should establish cyber standards and decision-making frameworks for data/IP and try to make these as flexible as possible to adapt to those of their allies. Ideally, alliances such as the Five Eyes will move towards common certification and accreditation.

When buying equipment from foreign manufacturers, defense forces should evaluate the intrinsic cyber threat, consider how to integrate hardware and software into existing systems, and ensure they have the capabilities to operate these assets. The overall risk to force readiness can ultimately determine the purchasing decision.

The evolution of commerce and risk in new domains such as Web 3.0 and the metaverse could place additional demands on space operations in the next 5 years. As the volume of commerce and collaboration via the metaverse grows, it's more important than ever to maintain connectivity to the metaverse in conflict zones.

Secure data processing power requires cooperation with allies and trusted partners to store and encrypt data and may benefit from the help of third-party service providers. Alliances such as AUKUS feature strong cyber cooperation.

Cyber-worthiness frameworks

Cyber-worthiness aims to achieve continued readiness in the face of a cyber threat or attack — including adversary actions in cyberspace ahead of, instead of, and even in the absence of, armed conflict. By taking a holistic view of cyber capabilities — including people, processes and technology — cyber-worthiness gives defense leaders a framework for risk management and continuous improvement, supported by robust and timely analysis to enable near real-time decision-making.

Signals of change

Future operating model

KPMG Connected Enterprise for Defense

Get in touch



Assessing system risk for operational integrity

The client's operating objectives required cyber resilience capabilities, and the development and deployment of modernized systems for activities with sophisticated inherent cyber threats. KPMG member firms use the proactive resilience framework 'Prosilience' Reference Architecture' to provide a method for assessing and mitigating risks in IT systems. Leveraging this framework, KPMG member firm professionals helped the client take stock of every device with system access, understand how the devices are connected, and improve the quality of response to threats by maintaining awareness of the client's security posture on a daily basis.

Cyber-worthiness authorities

Both government and civilian organizations may be tasked with assuring cyber-worthiness of rapidly evolving hardware and software. This involves protecting a range of nationally important industries, organizations and government organizations, such as mining, energy, water, environmental protection, and financial services.

Cyber-worthiness authorities' responsibilities may include evaluating hardware, monitoring behavior patterns and online traffic, performing investigations following cyber breaches, and guiding and training relevant personnel to improve national preparedness against future cyber attacks. Through increased collaboration with vendors and partners, they can build greater trust in the cyber security of defense assets.

What should defense organizations do?

- 1** Adopt a holistic view of cyber capabilities — including people, processes and technology — giving defense leaders a framework for risk management and continuous improvement, supported by robust and timely analyses to enable near real-time decision-making.
- 2** Invest in the attraction and retention of cyber expert resources, including commercial industry partnerships with capable and cleared defense industry participants. This capability remains a vital component of future defense forces and one in direct competition with commercial industry.
- 3** Adopt an agreed cyber-worthiness standard between allies that includes mechanisms for certification, sets minimum standards for operating systems, and establishes processes for remediation, including cooperation between allied nations (where appropriate) to combat cyber threats.
- 4** Adopt a more dynamic evaluation approach to cyber-worthiness that allows the flexibility to test systems in a sandbox environment without always progressing through the full evaluation over extended time periods. Based on risk and need, this can be managed effectively.

Signals of change

Future operating model

KPMG Connected Enterprise for Defense

Get in touch



6. Agile supply chains

Main trends

- The supply chain disruptions that began during the COVID-19 pandemic have caused defense forces to reconsider their manufacturing footprint to help improve reliability of supply. Over the past two decades, the US share of global microchip production has fallen from 37 percent to just 12 percent.¹² Faced with a continued shortage,¹³ the US government has pledged US\$53 billion to boost domestic chip production, as part of the *CHIPS and Science Act of 2022*.¹⁴ Such changes will, however, take time.
- It's not just availability that is under the spotlight. Supply chain integrity is an increasingly important consideration to assure procurers that suppliers and their products are genuine, and that IP remains secure. A 2019 study found that the US Defense Department had earlier lost US\$875 million to scams involving shell companies.¹⁵ In the innovation race, defense forces should ensure that all value chain players are on their side.

Summary

Supply chain and procurement are two critical areas that can benefit greatly from digital transformation, providing affordable, enhanced capabilities. This is especially relevant given the increasing dependence upon industry partners to provide future platforms, systems and support. An effective partnership should address the entire capability lifecycle to produce faster, better integrated and more cost-effective defense forces, improving cross-functional working and including suppliers and alliance partners in decision-making.

Defense forces can adapt faster to changes in demand by incentivizing suppliers to decrease lead times, operating with lower inventory levels, and reducing the design and development life cycle. Other ways to speed up new capabilities include AI, ML and digital simulation, rigorous testing and evaluation protocols, a cross-functional approach to development, and a robust battle rhythm that supports rapid decision-making.

Base operations

Automated replenishment of all inventories on bases, from groceries and maintenance equipment to weapons, is likely to become the norm, with receiving gates notified of approaching deliveries via a geo-fence alert. Once through the gate, most, if not all, activities associated with receiving and storing inventory should not require any human intervention, freeing up people for strategic tasks.

Deployed operations

Geo-fences at deployed locations support inventory management in a near-autonomous, if not wholly autonomous, way. In emergency response situations, sensor-tagged inventory can decrease the number of logistics personnel required without compromising operational flexibility. In both situations, the force can respond quicker to rapidly changing demands or requests for emergency support. The ability to receive demand signals from the front line, via IoT sensors, depends heavily on 5G communications technology. Domestic operations can typically rely on wired or wireless options; however, in conflict regions, such facilities may be limited, calling for the use of satellites to enable autonomous demand and supply.

Autonomous delivery vehicles could also be managed via two-way communication between the log post and the vehicles' IoT sensors. Successful autonomous operational logistics typically depend on agreements and governance between allies, so that sensors can communicate with supply posts operated by allies. The use of common parts, sensors and communications protocols between allies should also enhance deployed autonomous operations.

Logistics supply and warehousing

Defense forces are modernizing their warehousing and storage facilities through a combination of IoT sensors attached to inventory, connected material handlers, and physical robots moving items. Advanced analytics can help optimize inventory levels, drive dashboarding, enable faster response to demand signals, identify potential supply risks, and support mitigation planning. The smart, fully digital warehouse has become progressively more affordable, with a 3- to 5-year return on investment.

Signals of change

Future operating model

KPMG Connected Enterprise for Defense

Get in touch



Developing a smart, connected military base

The client's logistics base included a large warehouse district, maintenance depot and basic services district including training, catering and retail facilities. Over a multi-year project, KPMG member firm professionals helped modernize warehouses through advanced technology management systems, including automated, 5G smart warehouses driven by AI robotics and IoT. The depot modernization involved close alignment with force outcomes to help ensure that equipment was well maintained and ready for swift mobilization. Every part of the system is now connected, giving leaders a clear view of the base to enhance force readiness.

Signals of
change

Transportation and optimizing channels

The last mile in defense (delivery to the battle space) requires integrated delivery in and out of theater within nation states, with inevitable disruptions. Predictive analytics and control towers help identify and implement a swift response, such as supply agreements with allies and finding alternative local sources. Digital twins support robust scenario planning and enable earlier mitigation, making defense more responsive to global and local disruptions.

Control towers

Control towers provide decision makers with near real-time analyses to make strategic, operational and tactical choices consistent with government objectives. Automation and discrete digital management tools help make component parts move faster — but can miss the opportunity to integrate the whole picture for decision makers. However, standardized data management and analytics help build confidence in decisions made through the hierarchy, across silos and with partners and suppliers. Control towers harness publicly available data, as well as data from IoT sensors (including via 5G transmission in deployed

situations), weapon management systems (WMS) and maintenance management, enterprise resource planning (ERP) systems, as well as human resources (HR) and learning systems to deliver standardized intelligence. The use of visualizations further informs decision-making, geared to the specific circumstances facing individual decision makers.

Sovereign capability

Faced with geopolitical tensions and the pandemic, governments have had to re-evaluate their sovereign industry capabilities as a potential alternative to offshore supply chains. Many countries today aspire to greater levels of local supply and support — a trend expected to continue to satisfy broader strategic defense objectives. With supply chain disruptions potentially impeding access to critical components, consumables and systems, on-shoring and near-shoring are on the rise, with new agreements between allies and neighbors. Partnerships with established defense suppliers and other industry leaders can improve interoperability and communications with allies and enable defense departments to leverage economies of scale while deepening sovereign capability.

Future
operating
model

KPMG
Connected
Enterprise
for Defense

Get in
touch



What should defense organizations do?

- 1** Accelerate the adoption of supply chain automation and planning tools to support their core logistics operations over the next 5 years. There are ready-made tools from the commercial industry that can be adapted for defense, cost-effectively helping to augment next-generation weapon systems and platforms and support the digital modernization focus. The benefits for defense can be significant — improved situational awareness, more integrated support systems, greater efficiency and ultimately better support to warfighters.
- 2** Adopt near real-time systems that provide accurate and reliable data on assets, spare parts and weapon systems, which are delivered via an integrated control tower. These systems can support a better understanding of dependencies and risks and can lead to better decision-making.
- 3** Consider using digital twins and enhanced data visualization to support all levels of staff in taking full advantage of the integrated information presented.
- 4** Continue investing in sovereign industry capabilities in response to the challenges of great power competition and the vulnerabilities exposed by the pandemic. Countries should strive to make investments that support national objectives, regional obligations and international alliance and treaty commitments.
- 5** Consider how to maintain, if not expand, forces' ability to meet rising demands for support with disaster relief and other non-core defense tasks.

7. Climate change

Main trends

- Defense forces have an important role to play in supporting national climate goals by addressing emissions in existing platforms, infrastructure and estate, and incorporating sustainability and decarbonization into future acquisition programs.
- Forces should anticipate the need to adapt to a world where climate change can drive conflicts, influence battle conditions, and impact supply chains.
- Readiness plans should enable forces to support civilian populations during climate change-related disasters.
- Military facilities are increasingly at risk of damage caused by natural disasters such as hurricanes, tornadoes, fires and flooding. Protecting existing infrastructure and designing more climate resilient bases in the future are high priorities for many —

especially considering facilities need to be close to water. Innovations include wind-resistant, circular buildings, and mobile structures that can be moved in the event of an extreme weather event (in the same way that ships move aircrafts to safer places when severe winds are forecast). Indeed, the traditional large, stationary military site may become a thing of the past.

Summary

Conflicts will likely be increasingly driven by climate change-related issues such as mass migration and food supply disruption. Extreme weather events call for military support, use valuable resources, and can also damage defense forces' own facilities. In 2018, Hurricane Michael caused approximately US\$44 billion of damage to the Tyndall Air Force Base in Florida in the US.¹⁶ Future climatic conditions are expected to severely test defense forces. While facing climatic threats, defense forces should be

Signals of change

Future operating model

KPMG Connected Enterprise for Defense

Get in touch



able to adapt to remain effective and resilient — a complex and costly challenge that requires long-term planning and decisive prioritization.

Defense accounts for significant greenhouse gas emissions, and forces should try to decarbonize a diverse set of assets without constraining their operational capabilities. Doing nothing could leave forces highly exposed to budget increases from carbon taxes (reducing funds for critical investments), and continue their dependence upon traditional energy, which may be both scarce and expensive.

Defense also has a significant environmental impact in terms of pollution, waste, plastic and water use, through both its own activities and those of its suppliers. The UK Military of Defense (MOD), for

example, accounts for half of central government’s carbon emissions, two-thirds of water use and 56 percent of waste.¹⁷ These challenges present an opportunity to drive greater social value through stricter contractual ESG requirements with private sector manufacturing and service providers.

There are also plenty of opportunities to improve defense forces’ carbon footprint through energy transition. Fighting units supported by energy and water efficient assets as well as distributed energy generation tend to require lower logistical support and are less vulnerable to fuel and other supply shortages. Electric vehicles are becoming more cost effective and reliable and can offer performance improvement over conventionally gas-powered vehicles.¹⁸

What should defense organizations do?

- 1** Consider the impact of climate change and broader environmental damage on the operation of forces (both in training and deployed). Maintain a strong emphasis on procurement and future force design, given expected accelerated defense spending over the next 5 years.
- 2** Be cognizant of climate-related impacts in preparing future deployment scenarios.
- 3** Military infrastructure may need to be built or renewed to adapt to likely climate-based impacts, requiring multi-year planning and investment profiles to help safeguard personnel and assets.

8. The future of work

Main trends

- The future workforce should integrate humans and machines, calling for both technical and creative skills.
- New types of leadership are required to empower people and attract talent.

Overview

The future defense workforce should be able to adapt swiftly to changing combat methods driven by technology. These changes call for closer integration between people and machines, constant re-skilling, and a culture that values creative, flexible thinking to

predict and respond to different scenarios. People with technical-creative skills in areas like space, AI and cyber play a critical role, but of course are also highly sought after.

The debate over defense force culture is likely to intensify. Mirroring trends in the private sector, the employee experience is taking greater priority to help avoid staff attrition and attract a wider range of talent into the sector. Concerns over bullying, injury rates and veteran suicides attract a negative view and call into question traditional defense cultures. Leaders are expected to play a significant part in this shift, taking a greater interest in shaping individuals’ careers, and granting greater trust and autonomy to

Signals of change

Future operating model

KPMG Connected Enterprise for Defense

Get in touch



workers. Aligning mission objectives with physical and psychological safety has become a bigger priority for many forces, and leaders are being called to show that they are taking such issues seriously.

Similarly, leadership beyond hierarchy is critical to help solve new types of problems, both on and away from the battlefield. Technically or creatively talented individuals should gain greater power to lead teams

and make key decisions, and progress in their careers without having to take on classic 'leadership' roles.

This in turn influences training and learning, where critical thinking, collaborative problem-solving and diversity of thought are all valued. Classic rote learning should adapt to more innovative approaches involving technologies like augmented reality (AR)/ virtual reality (VR), gaming and learner data.

What should defense organizations do?

- 1** Employ digital labor to help overcome skill gaps in traditional and emerging capability areas and adopt a focus on capabilities rather than roles to change the proportion of full-time, part-time and contractor workers. Talent platforms should be employed to identify in-demand skills and potential digital solutions to acquire moving forward.
- 2** Consider capabilities such as sovereign necessities skills to be developed as a matter of national urgency, in collaboration with the defense industry. A more tailored approach to career management can help adapt to a wider range of roles and a more diverse range of people entering defense forces.
- 3** Defense forces should adapt the work environment to be more aligned to the hybrid working trend accelerated by the pandemic to help make them more competitive against the global skills shortages.
- 4** Provide opportunities for employees to grow skill sets within the defense industry and beyond, comparable to the 'commercial-grade' employee experience.
- 5** Consider the ethics of AI, which increasingly impact battlefield decisions, and the relationship between soldier and commander.

Embedding ongoing learning

The urgent demands of workforce modernization require a robust and far-reaching solution to rapidly prepare defense organizations' workforces for the needs of tomorrow. The US Marine Corps is only one combat force of many to announce a personnel and talent management transformation to meet shifting needs.

The KPMG Learning Service (KLS) is a modern learning experience and environment. KLS comprises a global learning technology platform, learning content and curriculum, learning transformation services, along with data and insights to enhance organization adoption. The KLS can be offered as a platform or managed service, with a strong focus on employee experience and tailored learning access to academies and aggregated content providers.¹⁹

Signals of change

Future operating model

KPMG Connected Enterprise for Defense

Get in touch



Future operating model

In adapting to the signals of change, defense forces should develop new, often digital capabilities that can enable them to build highly connected, mission-centric operating models. The ability to process data and produce real-time insights is paramount, along with transparency and, increasingly, interoperability within the force and between alliance partners.

Signals of change

Future operating model

KPMG
Connected
Enterprise
for Defense

Get in touch

Future of defense | 21



Future operating model

2030 defense forces are expected to be significantly more digitally enabled than today, bringing fifth- and sixth-generation battlefield capabilities that can harness the full potential of new weapon systems and platforms. The war in Ukraine has highlighted the inadequacies of discrete units acting without full integration and support, which has led to an expensive, wasteful and broadly ineffective war of attrition.

Future operating models should be more connected, with greater visibility across functions, data-driven scenario planning, and common standards for measuring performance and cost-effectiveness. Leaders in the future should be able to deploy scarce specialist resources across the force and use real-time insights to make better decisions.

Over the remainder of this decade, we believe defense forces' information sharing will be paramount, with partners from both alliances and private industry able to securely access data and analytical tools via the cloud.

In order to manage these innovations, we expect defense forces will need to securely capture, process and manage ever-larger volumes of digital information to deliver near real-time insights to support strategic, operational and tactical decision makers.

The mass volume of digital information will likely also challenge the ways defense organizations plan, integrate, manage and retire assets and investments. The traditional operating model of integrating and accommodating a plethora of programs can add significant complexity, slow the rate of improvement and inevitably suboptimize intended outcomes. A new model of operating authority informed by enhanced digital information transparency should be considered to support the ever-larger volumes of data, information, and programs more effectively.

The following capabilities can help you achieve a connected defense organization:

Innovative platforms and services: Gather and use data to develop a real-time, multi-dimensional

view of situational developments to inform strategy and operations. Priorities include improving infrastructure to adopt cloud at different security classifications; capturing data from advanced weapon systems and platforms; data governance to ensure information is up-to-date and reliable; and building environments to rapidly visualize and employ insights.

Insight-driven strategies and actions: Use insights and scenario-planning to develop integrated strategic operational capabilities. These capabilities support tactical and strategic decision-making and help provide a common voice for defense departments to communicate with government. Alliances, both international and industry specific, are likely to be key to success, requiring countries to agree precise capability contributions for future coalitions, while maintaining domestic security and independent capability in the region.

Mission centricity by design: Become far better connected to theater requirements — expressed as joint operating plans and strategies, which will help determine 'raise, train and sustain' functions for the forces. A mission-centric approach should help deliver seamless stakeholder, mission and campaign operations.

Seamless interactions: Integrate investment plans across operations, services and functions, taking a holistic view of decisions to enhance returns. This helps optimize the use of resources to meet national and mission objectives, and gives industry a reliable, long-term view of investments, enabling them to plan ahead.

Responsive operations and supply chain: Shift towards mission-centric offerings within more demand-driven and automated networks, enabling forces to respond to grey-zone challenges, the possibility of high-intensity conflict and domestic crisis while controlling costs and meeting community expectations.

Signals of change

Future operating model

KPMG
Connected
Enterprise
for Defense

Get in touch



Know your supplier

In an age of increasing ESG requirements, and concerns over foreign involvement in manufacturing and software, many defense forces are seeking higher levels of supply chain transparency. Analyzing existing and prospective suppliers can be further complicated by disparate and incomplete data. KPMG in the UK's 'know your supplier' is a managed service solution for defense forces, using cloud-based platforms, advanced analytics and ML. Using client, third-party and open-source data, KPMG member firm professionals can help assess suppliers and give defense forces a holistic, integrated view of their supply chain using dynamic dashboards.

Aligned and empowered workforce: Like all sectors, defense faces competition for new and different skills, while balancing humans and technology. Digital labor is expected to replace certain activities and help address skill gaps, while a focus on specific tasks — rather than roles — is likely to change the mix of full-time, part-time and contractor workers, matching their capabilities to specific needs. By tailoring careers to individuals, defense organizations can attract and retain a more diverse range of people.

Digitally enabled technology architecture: Embrace secure, digital technologies and platforms, removing the constraints of on-premises infrastructure and deploying commercial sector innovations on the future battlefield — with central command. Given security and network demands, we believe early investment in enterprise architecture, data and cyber will help maximize benefits. We expect the cloud will link core transaction systems in logistics, personnel and finance, bringing analytics capabilities to the user. A successful shift to cloud is dependent on an

operating model change combined with robust cyber security. Some jurisdictions are likely to opt for a multi-cloud approach, retaining sovereign control over key, highly classified remaining networks; others may choose private cloud networks.

Integrated partner and alliance ecosystem: We predict that a more digitally enabled, agile defense force will be built on improved relationships with suppliers, original equipment manufacturers (OEMs), alliance partners and whole of government. This will be dependent on improved data and insight into requirements and performance to help determine which capabilities are needed. Such integrated defense planning should greatly help to mitigate risks to the delivery of capabilities and address supply chain and logistics challenges.

Acquiring these capabilities calls for more agile procurement methods and greater program risk; not everything can meet 'five-nines' reliability. In our view, greater supply chain agility allows defense forces to respond to changing risk parameters and government demands.

Signals of change

Future operating model

KPMG Connected Enterprise for Defense

Get in touch



KPMG Connected Enterprise for Defense

Digital transformation in defense requires adapting to a connected operating model.

Signals of change

Future operating model

KPMG Connected Enterprise for Defense

Get in touch



High-maturity organizations continue to outpace their less mature peers

Compared with their less-mature peers, high-maturity defense organizations that are investing in the eight capabilities are more likely to:



Base: 31 respondents at low-maturity defense organizations and 32 respondents at high-maturity defense organizations

Signals of change

Future operating model

KPMG Connected Enterprise for Defense

Get in touch



Evaluating your capability maturity

Each of the eight enabling capabilities are underpinned by a set of sub-capabilities. The first step in defining a winning model is understanding your relative maturity in each sub-capability against the required maturity to help deliver your winning business model. KPMG offers three levels of maturity diagnostic depending on the needs of your organization.

Signals of change

Strategy and Capability Options

Strategic	Strategic Planning and Investment	Mission Capability Integration	Positioning and Strategic Alignment	User Segmentation	Capability Development
	Insights				
	Enterprise Data and Analytics Strategy	Data Collection and Enrichment	Data Insights and Visualization	Technology	Data Governance and Management
	Mission				
	Mission Strategy	Force Design and Delivery	Campaign Planning	Stakeholder Engagement	Enterprise Performance Management

Future operating model

Portfolio Management

Operational	Prioritization	Digital Enablement	Communication, Content and Relationship Management	Capability Integration	Security, Privacy and Fraud Prevention
	Responsive Supply				
	Demand-led Distribution Model	User Fulfillment	Procurement	Inventory Capabilities	Asset Management
	Ecosystem				
	Partner Strategy and Ecosystem Design	Vendor and Supplier Management	Partner Integration and Alignment	Ecosystem Management	

KPMG Connected Enterprise for Defense

Organizational Alignment & People

Enabling	Organization Design	Culture	Leadership	Innovation	Talent Strategy and Capabilities
	Technology Architecture				
	Agile Mindset	Technical Architecture	Service Integration and Performance	Automation and Enablement	Security

Get in touch



Making it happen

KPMG Connected Enterprise for Defense is an insight-led, customer-centric approach to digital transformation.

Our approach is centered on improving all eight connected capabilities across the enterprise to the level that can help provide significant organizational value. These connected capabilities map to the operating model and can allow you to prioritize, shape and execute your digital transformation.

KPMG professionals' experience working in digital transformation has informed a set of accelerators, including a range of configurable Software-as-a-Service (SaaS) solutions from leading technology providers, which enable us to provide a more efficient option for delivering transformational outcomes.

With the mission at the core, there are five critical questions defense organizations should ask themselves:

- 1** Are you connecting commanders with the insights they need to make data-driven decisions on future capability needs?
- 2** Are you connecting and empowering your employees to deliver the mission?
- 3** Are you connecting your front, middle and back offices to execute in support of the needs of the battlefield?
- 4** Are you connecting your ecosystem of partners to jointly deliver on the mission?
- 5** Are you connecting to geopolitical and digital signals of change?

To learn more, contact us or visit:

kpmg.com/connecteddefense

Signals of
change

Future
operating
model

KPMG
Connected
Enterprise
for Defense

Get in
touch



Get in touch



Peter Griffiths
Global Head of Defense and National Security
KPMG International
pwgriffiths@kpmg.com.au



Brenda Walker
Head of Global Government
KPMG International
bwalker@kpmg.com



Albert Morales
Principal, Advisory Services
KPMG in the US
albertmorales@kpmg.com



Omer Tauqir
Head of Defense and Defense Industries
KPMG in Saudi Arabia
otauqir@kpmg.com



Jonathon Gill
Head of Aerospace and Defense and Partner
KPMG in the UK
jonathon.gill@kpmg.co.uk



Grant Riley
Partner, Advisory
KPMG in New Zealand
ranriley@kpmg.co.nz



Stefan Hefter
Partner, Consulting
KPMG in Germany
stefanhfurter@kpmg.com



Carsten Schiewe
Partner and Head of Solution and Alliance Management
KPMG in Germany
cschiewe@kpmg.com



Peter Robinson
Head of Defense and Defense Industry
KPMG in Australia
pforobinson@kpmg.com.au



Grant Abrams
Partner and Ottawa Market Leader for Management Consulting
KPMG in Canada
gabrams@kpmg.ca



Abhishek Verma
Partner, Aerospace and Defense
KPMG in India
abhishekverma5@kpmg.com



Melissa McClusky
Lead Defense Partner
KPMG in Australia
melissamc@kpmg.com.au



Gautam Nanda
Associate Partner,
Aerospace and Defense
KPMG in India
gautamnanda@kpmg.com

Signals of change

Future operating model

KPMG Connected Enterprise for Defense

Get in touch



Sources

- ¹ IISS. (2022, February). *The military balance 2021*. IISS. Retrieved 2022, from <https://www.iiss.org/publications/the-military-balance/the-military-balance-2022>
- ² Ibid
- ³ Ibid
- ⁴ Ibid
- ⁵ Ibid
- ⁶ GlobalData. (2022, March). *Ukraine Conflict — Executive Briefing (third edition) — Understand the impact of the Ukraine Crisis on the world economy and key sectors*. Thematic Research GDGEO-TR-X003. Retrieved 2022, from <https://www.globaldata.com/ukraine-crisis/>
- ⁷ Naval Technology. (2021, July). Laser directed energy weapons likely to receive the most investment in the future: Poll. Naval Technology. Retrieved 2022, from <https://www.naval-technology.com/news/laser-directed-energy-weapons-likely-to-receive-the-most-investment-in-future-poll/>
- ⁸ Boeing. (2022). *P-8 Objective and Capabilities*. Boeing. Retrieved 2022, from <https://www.boeing.com/features/2022/08/p-8-objective-and-capabilities.page>
- ⁹ Rheinmetall. (2022, June). *Panther KF51 main battle tank: Future tankology*. Rheinmetall. Retrieved 2022, from https://www.rheinmetall-defence.com/en/rheinmetall_defence/systems_and_products/vehicle_systems/armoured_tracked_vehicles/panther_kf51/index.php
- ¹⁰ Space Force News December 29, 2020
- ¹¹ United States Space Force (2021, May). *USSF History*. United States Space Force. Retrieved 2022, from: <https://www.spaceforce.mil/About-Us/About-Space-Force/History/>
- ¹² Laudicina, Paul. (2022, January). *Semiconductors: How the U.S. can make up for lost time*. Forbes. Retrieved 2022, from <https://www.forbes.com/sites/paullaudicina/2022/01/29/semiconductors-how-the-us-can-make-up-for-lost-time/?sh=211cebcb6478>
- ¹³ Shein, Esther. (2022, June). *Unfortunately, the global chip shortage will continue*. TechRepublic. Retrieved 2022, from <https://www.techrepublic.com/article/global-chip-shortage-continues/>
- ¹⁴ Heater, Brian. (2022, August). *Biden signs CHIPS bill in bid to supercharge US semiconductor production*. TechCrunch. Retrieved 2022, from <https://techcrunch.com/2022/08/09/biden-signs-chips-bill-in-bid-to-supercharge-us-semiconductor-production/>
- ¹⁵ De Haldevang, Max. (2019, November). *The US Defense Department lost \$875 million to scams involving shell companies*. Quartz. Retrieved 2022, from <https://qz.com/1755722/defense-department-has-lost-875-million-to-shell-company-scams/>
- ¹⁶ <https://www.defense.gov/News/News-Stories/Article/Article/2642717/combating-climate-change-factors-into-defense-budget-request/>
- ¹⁷ <https://www.nao.org.uk/wp-content/uploads/2020/05/Environmental-Sustainability-Overview.pdf>
- ¹⁸ <https://www.army.mod.uk/news-and-events/news/2021/07/army-hybrid-vehicles-power-forward/>
- ¹⁹ Department of the Navy, United States Marine Corps. (2021, November). *Talent Management 2030*. Department of the Navy, United States Marine Corps. Retrieved 2022, from https://www.hqmc.marines.mil/Portals/142/Users/183/35/4535/Talent%20Management%202030_November%20help%202021.pdf
- ²⁰ A commissioned study conducted by Forrester Consulting on behalf of KPMG, January 2019.

Signals of
change

Future
operating
model

KPMG
Connected
Enterprise
for Defense

Get in
touch



Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia



The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2022 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

KPMG refers to the global organization or to one or more of the member firms of KPMG International Limited ("KPMG International"), each of which is a separate legal entity. KPMG International Limited is a private English company limited by guarantee and does not provide services to clients. For more detail about our structure please visit kpmg.com/governance.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

Throughout this document, "we," "KPMG," "us" and "our" refers to the global organization or to one or more of the member firms of KPMG International Limited ("KPMG International"), each of which is a separate legal entity.

Designed by Evalueserve.

Publication name: Future of defense

Publication number: 138447-G

Publication date: December 2022