The future of defense

Defense and the connected enterprise

September 2019

Select the right professional services firm

kpmg.com/connected

Introduction

This paper is intended to be provocative and to stimulate debate around the future of defense – it does not claim to predict exactly what will happen.

The defense sector has been responsible for many ground-breaking technological advances, from the internet and computers to drones and GPS. Over the years, western nations have invested heavily in R&D in order to keep one step ahead of the adversary and gain first-mover advantage. But today, a combination of military budget restrictions and the exponential growth of technology companies has left defense trailing the civilian world in terms of R&D. Consequently, defense organizations need to be attuned to emerging innovations emanating from outside the defense sector and embrace them as early as possible.

Digital technology is more important to defense than ever, holding the key to an effective and efficient force, in which leaders can make informed decisions, from an accurate and timely common operating picture, to gain advantage on the battlefield. Digital transformation[1] calls for a fully connected organization, in which every function across the front, middle and back 'office' is seamlessly aligned. In the commercial environment this is known as a 'connected enterprise' and there are many examples of businesses employing such an approach to the benefit of their customers.

Given the lethal nature of defense outcomes, the requirements of peacekeeping, and the role of defense forces in aiding civil power, such connectivity should be maximized. The more so due to the scale and breadth of a force and its supporting human and technical infrastructure, including a complex supply chain and wide range of roles from soldiers to fighter pilots, cooks to chaplains, financiers to IT specialists and every other imaginable role in between.

A connected defense force accelerates preparedness by bringing together equipment, resources and training, enabling decision-makers to scan the entire asset base, understand cost-to-serve and time to deploy, throughout the entire tactical, operational and strategic cycles of a military operation. It also supports the rapid adoption of new postures.

There are, of course, many technology advances on the defense radar screen: directed energy weapons, hypersonics, quantum computing and autonomous weapons, for instance. But, from a connected enterprise perspective, one technology is blinking particularly brightly on the civilian technology radar: 5G and its associated ecosystem, which, if grasped early, offers forces an opportunity to address these issues and stay a step ahead of their adversaries.

[1] Digital transformation encompasses profoundly transforming the business and organizational activities, processes, competencies and models through fully leveraging emerging digital technologies and the accelerating impact these are having across society, strategically, with present and future shifts in mind

This paper addresses the future of defense over three horizons, in outline these could be:

Horizon 1: the connected enterprise:

- This horizon addresses the need to connect the disparate elements of a complex defense organization across the front, middle and back offices, in order to deliver on defense's diverse objectives. A highly connected defense force also requires matching capabilities to defend against threats that seek to exploit a connected architecture. Advantage over the adversary may come as much, if not more so, from hyper-converged connectivity as from superior platforms.
- **Key technologies/capabilities:** The critical capabilities of the connected enterprise, outlined in this paper, along with cyber, provide the building blocks. The 5G ecosystem[2] should accelerate the delivery of very near real-time decision support and a common operating picture, as well as hyper-converged connectivity. This era is also set to see the creation of specialized space and cyber forces (where they do not already exist).

Horizon 2 – The 'instantly informed enterprise':

- The 'instantly informed enterprise' builds on the connected enterprise but is distinguished by the efficiency of the connections; i.e., information is readily available to decision makers at each element within the connected enterprise in real time (or as required).
- **Key technologies:** Edge computing brings a step change in network efficiency and effectiveness, as well as speed, plus availability of information to users, based on efficient processing of data at the point of collection/consumption. The internet of things (IoT) connects everything and everybody, giving, for example, instant feedback about asset performance and maintenance.

Horizon 3 - The automated enterprise:

- This horizon combines robotics and real-time availability of information at the edge of the network, to drive automated decision-making on a larger scale. Humans are likely to be increasingly replaced by robots/remotely piloted vehicles of all types, to conduct operations. There will likely also be a significant increase in intelligent automation (IA)/robotic process automation (RPA) to drive efficiency in the middle and back offices.

In this paper we discuss the eight capabilities that can help defense forces become connected and fully aligned behind their mission across the five domains of warfare. These capabilities touch on critical issues like mission-centricity, responsive supply chains, new approaches to talent acquisition/retention, and working with a wider range of allies and partners.

Nothing can ever be certain in a military operation, so there is a continuing need for planning to be flexible, incorporating different scenarios, with sufficient agility to make rapid changes/pivots in strategy and tactics. With a fully connected defense force, leaders can increase their chances of achieving a strong posture with robust logistical support and enhanced decision-making.

Ending where I started, the aim of this paper is to stimulate debate. The 'provocations' it contains have been provided by some of KPMG's highly experienced defense specialists, through in-depth discussions with selected senior defense professionals, along with findings from a Forrester survey of 122 professionals involved with customer-centric strategy decisions at defense organizations in Australia, Canada, Germany, India, the US and the UK. I would like to thank all those who have contributed their time and thoughts.

Mike Stone

Global Chair of Defense and National Security

[2] See appendix

Eight capabilities of a connected defense force

1 **Insight-driven strategies and actions**

2 **Innovative platforms and services**

3 **Mission centricity by design – to be fully force ready**

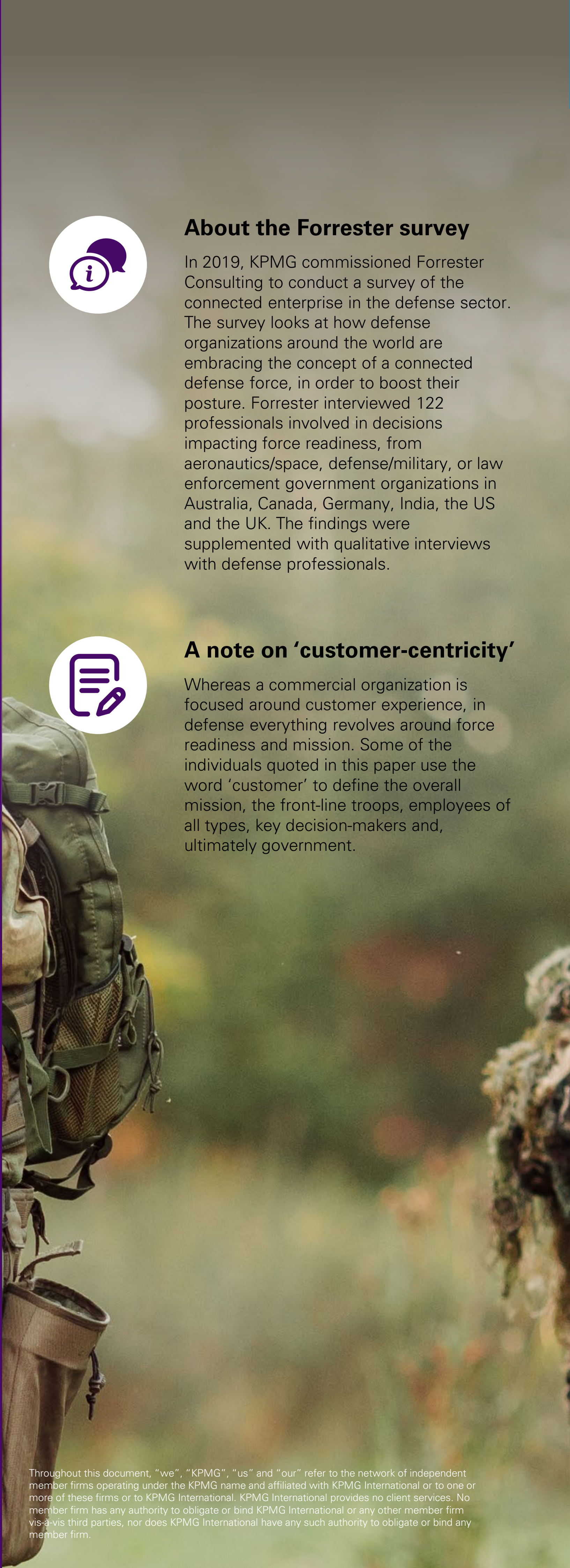
4 **Seamless interactions– between front, middle and back office**

5 **Responsive operations and supply chain**

6 **Aligned and empowered workforce**

7 **Digitally enabled technology architecture**

8 **Integrated partner and alliance ecosystem**



About the Forrester survey

In 2019, KPMG commissioned Forrester Consulting to conduct a survey of the connected enterprise in the defense sector. The survey looks at how defense organizations around the world are embracing the concept of a connected defense force, in order to boost their posture. Forrester interviewed 122 professionals involved in decisions impacting force readiness, from aeronautics/space, defense/military, or law enforcement government organizations in Australia, Canada, Germany, India, the US and the UK. The findings were supplemented with qualitative interviews with defense professionals.

A note on ‘customer-centricity’

Whereas a commercial organization is focused around customer experience, in defense everything revolves around force readiness and mission. Some of the individuals quoted in this paper use the word ‘customer’ to define the overall mission, the front-line troops, employees of all types, key decision-makers and, ultimately government.

Contents

	Page
Challenges to force readiness	5
Three horizons in the future defense journey	8
What makes a connected defense force?	9
Five ways to build a connected defense force	17
Why choose KPMG to help you build a connected defense force?	19
Appendix: Why 5G is the key to unlocking a wider ecosystem	20
Contact us	23

Throughout this document, "we", "KPMG", "us" and "our" refer to the network of independent member firms operating under the KPMG name and affiliated with KPMG International or to one or more of these firms or to KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm.

Challenges to force readiness

Whether on the battlefield, on peacekeeping operations, or assisting with civil unrest or environmental disaster, one of the key outcomes sought by any defense organization is to be able to rapidly mobilize and deploy force elements at readiness, or FE@R, to deliver a strategic outcome or political end. Digital technologies, therefore, need to work across a number of the levers of power or DIME (diplomacy, information operations, military and economic) to deliver the outcome. It requires a huge logistical and operational effort to get relevant military units in place at short notice. To be effective, these units must be connected to each other and to the wider chain of command.

Defense organizations face a number of challenges to achieving the requisite level of readiness, including:

Investing in platforms with insufficient consideration of connectivity

Investing in prestigious capital platforms like battleships, aircraft carriers and fighter jets is extraordinarily expensive. Cost controls often lead to information capabilities being traded out, which can lead to forces being equipped with the latest 'kit', but with connectivity from an earlier generation. By definition, therefore, these assets are less effective than they might be.

Insufficient consideration is often given to the different life cycles of heavy metal and information capabilities when procuring capital equipment. For instance, the life cycle of a warship may be up to 60 years from concept to disposal, whereas that of the information/connectivity will be more like 5-8 years. Finding a way to address this conundrum is vital. Given the growing challenge of cyber warfare, defense organizations risk having shiny new platforms that are poorly connected and vulnerable to cyber-attack.

Information capability procurement is often siloed. Arguably, without a 'strong controlling mind', it will be near impossible to realize the full potential of the connected defense enterprise.

Data everywhere – but what to do with it?

Data is exploding, with volumes doubling every year in an ever-accelerating trend. Thankfully the cost of storing data is going down, although not at the same rate. Data is also extremely valuable and yet most enterprises make effective use of less than 25 percent of their data – often far less in the defense field.

The internet of things (IoT) is contributing massively to the explosion and we are seeing the deployment of huge numbers of sensors into equipment and even clothing, offering the opportunity to link everything to everyone. IoT also offers opportunities, such as predictive maintenance for parts that alert the need for repairs or service, rather than costly and time-consuming scheduled maintenance of whole assemblies. However, the sheer amount of this data leaves many defense organizations struggling to translate it into useful knowledge and insights on the readiness of assets and people, threat assessments, supply chain blockages, and so on. The vision is for data to be collected, processed and analyzed in near real time to create an effective common operational picture; in many cases, however, the overwhelming volume of information hinders rather than helps decision-makers.

> **"The promise is to provide much more decision-support data that is manageable and comprehensible, reliable, and delivered in real time."**
>
> Peter Griffiths, Lead Partner, Defence & National Security, KPMG Australia

Connectivity blockages

Like many large and complex organizations, defense has inevitable 'silos' where information is not shared readily, and communications are slow and selective. Each function is developing its own platforms, but these are often created independently, without strong connectivity to each other and to leaders.

Operational interoperability

Interoperability is a challenge within the different parts of a national defense force – like land, sea, air, front, middle and back office – let alone across other government departments and allies, as well as numerous outsourced parties. Each of these entities often has its own systems and processes and is unwilling or unable to generate or share data with the others, with a general lack of transparency. Dependencies across capability areas are often not well understood, leading to misunderstandings that adversely impact interoperability.

Vendors not partners

There is a constant desire in most forces to reduce spending in the 'back office' in order to free up funds to invest in front-line activities and realize greater efficiencies. This has led to more and more services being outsourced. Traditionally there has been skepticism over the use of third parties in terms of the quality of, and the degree of control over the service provided. Vendors in turn are often loath to share proprietary intellectual property (IP) and data, which holds back both performance and data-fueled insights. From a macro perspective, globalization has led to an ongoing debate around dependence, as result of globalization, on non-allies for items such as micro-electronics and parts. This in turn has raised the question of a national 'industrial strategy' for defense, which calls for longer-lasting relationships with trusted partners within the global supply chain.

Cyber security

The cyber arms race is here to stay. As everything becomes connected, so systems and devices may become more open to hacking; something that requires close attention. Most nations are investing heavily in cyber warfare capabilities from both a defensive and, in some cases, an offensive standpoint. Cyber defense should be one of the fundamentals of procurement, otherwise investments can be wasted.

The definition of cyber warfare is also unclear; for example, is an attempt to disrupt another nation's elections an act of national aggression?

> **"In defense we've traditionally had land, sea and air. You can add cyber and space to that list…We need to invest more in our cyber hygiene to keep up with the bad guys who are trying to constantly barrage our networks and get access to our information."**
>
> CIO, Assistant Deputy Minister Information Management, Canada

Workforce challenges

Certain skills are scarce; in the technology arena these are notably in skill sets such as data analysis, data science, artificial intelligence (AI), algorithms, modeling and simulation. Such talent may be less interested in long-term careers, so defense organizations must find new ways of accessing these vital resources, or risk falling behind. This requires new employment models for instance, episodic careers. Another challenge is that the rate of growth in salaries for technology top talent continues to diverge from public sector norms.

Top obstacles to success

The participants in the Forrester survey were asked to list the top five obstacles to the successful execution of their organization's mission-centric strategy.

Security and compliance concerns

— Regulatory requirements/compliance (20%)

— Concerns around data security and privacy (18%)

Strategy misalignment

— Lack of executive sponsorship (20%)

— Lack of qualified staff (17%)

— Insufficient budget (16%)

People/process misalignment

— Lack of alignment with third-party partners (19%)

— Lack of a transparency and ineffective communication with third-party partners (14%)

Technology and data silos

— Difficulty sharing customer data/analytics between channels, countries, or locations (25%)

— Lack of system integration across channels (22%)

— Legacy systems (18%)

— Customer data is housed in multiple databases (17%)

Business silos

— Lack of real-time understanding of demand across various channels/programs (20%)

— Lack of organization-wide customer engagement strategy (18%)

— Business units are siloed (15%)

Three horizons in the future defense journey

Three horizons in the future defense journey

These three horizons are impacting every aspect of a defense organization, with the connected enterprise at the heart of force readiness.

Horizon 1: The connected enterprise:

Many defense organizations are investing heavily in acquiring 5th generation platforms, such as the F35 Strike Fighter and the P8 Poseidon. These are hugely capable platforms, but their effectiveness is constrained when their connective tissue is based on 2nd or 3rd generation 'tin and string'. Getting inside the adversaries' decision cycle has never been more important and that requires a very near real time common operating picture/decision support capability.

If we can challenge ourselves to think differently, then 5G may provide many of the answers to this dilemma. 5G is not just the next evolutionary step in mobility; it represents a truly revolutionary leap forward for two reasons: the power of the exponent[3] , and secondly, the fact that it will be led by enterprises not consumers. 5G supports a million active connections in every km2, so sensors can now be deployed ubiquitously. It provides the opportunity to link everything to everyone. Its huge bandwidth can also support augmented intelligence with little to no impact on workloads, enabling a much nearer real time common operating picture. As we argue in our article Plan for the 5G revolution, it is as much of an advance, in the enterprise space, as building the railways was 200 or so years ago.

Security takes on even greater importance, given that sensors can not only intercommunicate, but may also need to make decisions independent of humans. Defense organizations, therefore, must be assured that that no malicious code has been injected into IoT. The network slicing capabilities of 5G will allow multi-level secure access within the same bandwidth, with different levels of encryption within each 'slice'.

Defense organizations should now be planning how they intend to exploit these capabilities. One can easily envisage drones providing a 5G envelope for a mobile brigade for instance; this is likely to require just three or four properly equipped drones along with maybe a hundred or so other decoy drones. Another possibility is the linking of real-world field training with the synthetic environment to provide more holistic and realistic training at low cost. The advantages for first movers will be significant.

> **"5G is the next truly exponential leap forward, connecting every part of a defense organization both in the field and in barracks and potentially enabling sensors to make independent, informed decisions…."**
>
> Mike Stone,
> Global Chair of Defense and National Security,
> KPMG International

Horizon 2: The 'instantly informed enterprise':

By this point we can imagine vehicles in the defense estate being automatically checked every 20 seconds or so for their location, fuel and lubricant, ammunition and rations, as well as for vital signs of all on board. This may allow better planning for petrol, oil and lubricants (POL), ammunition and ration dumps and is set to radically change the role of supporting elements of the supply chain – as well as shifting the roles of people away from manual data collection and towards applying judgement to the data.

Secure 5G, and the availability of mobile data centers at the edge, will enable edge computing to come into its own, with data being collected and processed at the edge and only the product being passed back.[4] Every part of the defense force will be in touch 24/7 and information will be analyzed, and insights delivered, within milliseconds, speeding up decision-making and giving leaders far greater understanding of situations.

Horizon 3: The automated enterprise:

As we enter the era of robotic warfare, fewer humans are likely to be needed on the battlefield, with their main role to 'sweep up' after remotely piloted planes, tanks, ships and submarines. Technology skills will be more in demand than ever.

[3] Its speed is already a factor of 10:1 greater than 4G and the physics suggests it can get to 20Gbps (gigabits per second), whilst its latency is less than 1ms compared to around 100ms for 4G if jitter is included

[4] A 3Tb chip is now the size of an individual bag of sugar, seven of these 'daisy chained' would provide a 21Tb data center in a form factor similar to that of a large laptop

What makes a connected defense force?

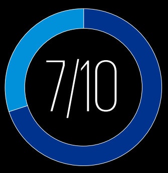
A connected defense enterprise is the foundation of a force ready posture.

5G, AI and remote monitoring are accelerating the move to a force composed primarily of remotely piloted and potentially autonomous vehicles of all types. Consequently, the time available to make decisions will likely continually reduce. That's why it's so important to align the front, middle and back office functions, to keep the front-line force ready and one step ahead of the enemy. As readiness requirements change, supply chains must swiftly adjust, re-posture and/or acquire or attain equipment, ammunition days, flying days, spare parts and rations.

In a connected defense force, every part of the organization – the human, financial and physical supply chains – work with each other in a digital relationship, bringing together equipment, resources and training. The force readiness requirement is connected to these supply chains, helping to predict demand and adapt swiftly to changing circumstances.

Information and data are the lifeblood of operations. Being connected gives total visibility over all assets, to understand cost-to-serve and time to deploy throughout the entire cycle of a military operation. Key decision-makers receive accurate and timely insights, to help them get inside the enemy's decision cycle faster than the enemy can get into theirs.

According to the Forrester study of defense organizations, a connected defense force is high on the agenda. Almost 7 out of 10 say they will be investing in most or all of the key connected defense force capabilities over the next 12 months. And half intend to invest 16 percent or more of their budget in their connected defense force strategy over the time period.



defense organizations are making their 'customer-centric' strategy a priority.

> **"It's [customer centricity] probably our highest priority at this moment in time…we are refocusing the whole way we work and who we work for."**
>
> Domain Functional Manager – Project Controls, Ministry of Defence, Defence Equipment & Support (DE&S), UK

Eight elements of a connected enterprise

1

Insight-driven strategies and actions

Harnessing data, analytics and insights to develop a real-time view to inform strategy and operations.

A connected defense force promises more decision-support data that is reliable, easy to understand and arrives in real time. Simulations can test the preparedness and vulnerabilities of one's own and one's opponents' forces, operations and supply chains. The 'digital twin' simulated environment can even be used for training, using virtual and augmented reality to undergo incredibly realistic exercises.

According to the Forrester global defense survey, a majority of defense organizations (7 out of 10) have detailed data governance and see data and analytics as foundational to their strategy. However, fewer (46 percent) are confident they can turn data into actionable insights to offer a real-time, multi-dimensional view of situational developments. Forces should also attempt to classify aggregated data and gain insights into military capabilities – something that has been previously been hidden as a result of disconnected data sets.

> **"[Our priority is] Becoming a data-driven organization and putting information in the hands of the front lines. Whether that's a warfighter or a corporate analyst. Whether these are situational awareness of your enemy in the field or the effectiveness of the organization's outputs…like finance or HR."**
>
> Director of Service Design, Ministry of Defence, Information Systems & Services, UK

Only 46 percent of defense professionals are confident in their organization's ability to turn data into actionable, real-time insights.

2

Innovative platforms and services

Developing integrated operational capabilities to help the force consistently – and securely – deliver on its mission.

Given the rise in cyber warfare and the increasing ubiquity of IOT, software is becoming a key source of innovation. Sensors are embedded in equipment and via monitors on people, to generate situational and performance data, delivered via cloud platforms that offer a protected environment. These enable defense organizations to adopt new tools and new approaches to data collection and rapidly test solutions. Using cloud, increasingly as-a-service, helps to overcome the aging IT infrastructure in most defense forces, at a fraction of the cost. The impact of the emergence of 5G and edge computing on traditional, ERP systems will need careful assessment, as will striking the right cultural/risk balance between defensive cyber and the opportunity to exploit connected information.

3 Mission centricity by design

The operational readiness of a military force to conduct a mission, unified across land, air, sea, cyber and space.

Centricity ensures that every part of the organization is focused on the mission and on force readiness and posture, which is tied directly to the supply chain and operations. Where historically, those in the field were passive recipients of divisional ideas and concepts, they should now be treated as 'customers' of the middle and back offices, with leaders setting requirements and having resources under their control. A focus on the mission ensures more effective use of finances, encouraging a better understanding of through-life costs and maintenance, and the ability to make trade-offs between different procurement options. For example, it should lead to a greater emphasis upon maintenance, which is likely to bring down net equipment costs significantly, freeing up budget for other activities. It may also mean more spending on cyber to preserve force effectiveness.

A new 'customer' lens is needed to drive 'digital transformation'. The last rounds of transformation took a business process re-engineering and lean lens and were effectively about improving internal processes – with little attention to the customers' perspective.

Less than half (49 percent) of defense professionals feel their organizations can design and deliver seamless, integrated campaigns.

4 Seamless interactions

Seamlessly connecting the front, middle and back offices

Mission-centricity should help connect and align the entire defense department behind its posture. Total visibility can instantly inform leaders of how many battalions, warships, jets and other assets are available – and their maintenance needs – as well as supplies, ammunition and troop numbers and experience. In a 5G connected world, empowered by sensors, decision-makers have better and more complete information at their fingertips, live on a dashboard, with continual situational updates and more reliable predictions, making the force more adaptable to changing circumstances. Through the life cycle of an operation, they can understand deployability and cost-to-serve of their forces. One key advance concerns redeployment training, which is a major logistical task and requires considerable planning, coordination and cost management, and which in the past has often gone well over budget. With more control over each element of the exercise, leaders can optimize spend.

Although some defense forces refer to the 'battle space' and the 'business space', in reality these are a continuum. The information exchange requirement (IER) has previously been constrained by lack of bandwidth in the field, but the field needs access to 'business' systems just as departments of defense and headquarters need access to 'battle' systems. The speed, capacity and low latency of 5G should address this.

> **"The internet of things [is a huge priority]...because in a world where we have many nodes, people, aircraft, tanks, guns, the ability to actually take physical information from them to inform our supply chains, to inform the health of our warfighters I think would be the one thing that would transform this business more than anything."**
>
> Director of Service Design, Ministry of Defence, Information Systems & Services, UK

5

Responsive operations and supply chain

Deploy forces and meet mission needs in an agile, consistent manner, supported by advanced analytics.

The procurement and logistics operation is flexible and resilient enough to support all the forces' needs and be highly responsive to changing demand. Supplies, equipment and ammunition are in prime condition and delivered promptly to the right place. Supply chain managers have total visibility of all human and physical assets and can use algorithms to predict demand and maintenance needs. Intelligent systems like the Lockheed Martin Autonomic Logistics Information System (ALIS) – which supports the F-35 Lightning II fighter jet – enable operators to maintain, plan and sustain the aircraft's systems over its life.

It's of utmost importance to link these assets to strategic outcomes. Can a force deliver its force elements at readiness? Does it have the right mechanisms and available assets to deploy a force – and the right logistic supply chain to support it?

Many of the defense professionals surveyed by Forrester have confidence in their organizations' supply chains. Seventy percent say their supply chains can meet the needs of deployed forces in an agile and consistent manner. And 62 percent claim to have accurate, real-time visibility over global and local military asset inventories, along with a flexible system for supporting these assets.

> **"What you're really after is total asset visibility, from financial to material to human assets. Not just on the readiness side, but on the deployment, to see how you're drawing down on your assets and how you can adjust your supply chain."**
>
> Michael Mitchell, Defence and Security Lead, KPMG in Canada

70 percent of defense professionals surveyed say their supply chains can meet the needs of deployed forces in an agile and consistent manner.

6

Aligned and empowered workforce

A mission-centric organization and culture requires people with the right skills, plus incentives that are closely aligned with force readiness. As field forces reduce over time in favor of robotic warfare, and cyber increases in importance, defense organizations will need new types of talent in technologies like data science, analytics and AI; specialists rather than generalists. The concept of lifetime service will be replaced by a greater number of 'episodic' careers and some recruits may be unconventional individuals that don't match the traditional military stereotype of cropped hair and uniform. It is vital to create career paths for a wider range of people, who must all feel at home in the culture. For instance, can the 'gig economy' have any relevance to a future workforce that doesn't want to commit to lifelong careers?

Two thirds of the defense professionals surveyed by Forrester believe their leadership champions a connected defense force, with appropriate incentives. But only half (51 percent) say they have a clear strategy for attracting and retaining talent to meet future skills requirements.

7

Digitally enabled technology architecture

Future warfare will be very dependent upon digital, so the enterprise architecture must be able to adapt to rapid changes in technology. Third parties and vendors should be closely integrated into the core platform, with complete interoperability. This is especially important given the rise in usage of as-a-service software, with cloud platforms collecting and analyzing data from the field and producing insights on issues like the condition of equipment, and need for fuel, supplies and ammunition. For instance, a supplier of a jet, drone, tank or warship may have responsibility for all the ongoing software that drives maintenance and performance. More and more of the supporting processes behind a force will be automated; the challenge is to drive this into all procurement, which should have an information centric capability at its heart.

Agility is a key capability, yet only 42 percent of the defense professionals surveyed by Forrester say their digital services, technologies and platforms can meet the user promise in an agile, cost-effective, and scalable manner.

Cyber security will be a top priority, with careful vetting and monitoring of your own and third parties' systems. Forces are starting to work with military equipment suppliers and technology companies to create multi-level security environments, for example, involving outsourced data centers. A significant majority (75 percent) of defense professionals in the survey feel they have fundamentally secure data, systems, and products across all channels. As defense moves more and more into the cloud, the challenge will be to maintain this level of assurance in security.

Only 42 percent of defense professionals say their organization's digital technologies can meet user's needs in an agile, cost-effective and scalable manner.

8

Integrated partner and alliance ecosystem

Supply chain members must transition from being vendors to partners, as part of a wider industry strategy that includes significant outsourcing via platforms. This requires a change of mindset in departments of defense and, in particular, in the commercial branches. Relationship management and partnering skills should be at a premium, and trust is the key factor for all partnerships, with an emphasis on a lifetime relationship. Data sharing has been a challenge in the past, and partners do need assurance over their intellectual property (IP), but in turn should open up their data to generate better insights that support force readiness. A connected defense force offers the kind of visibility that will enable tighter management of third parties, to ensure a high quality of service at a fair cost; it may even result in renegotiation of contracts. Trusted sharing across the defense/industry interface becomes a critical success factor in making this a 'whole force capability'.

The defense professionals surveyed acknowledge the growing importance of relationships, with 69 percent stating they actively manage a rich ecosystem of partners and allies to inform future planning and decision-making. However, less than half (49 percent) feel their organization has a comprehensive vendor and supplier engagement program that certifies and monitors contractor performance.

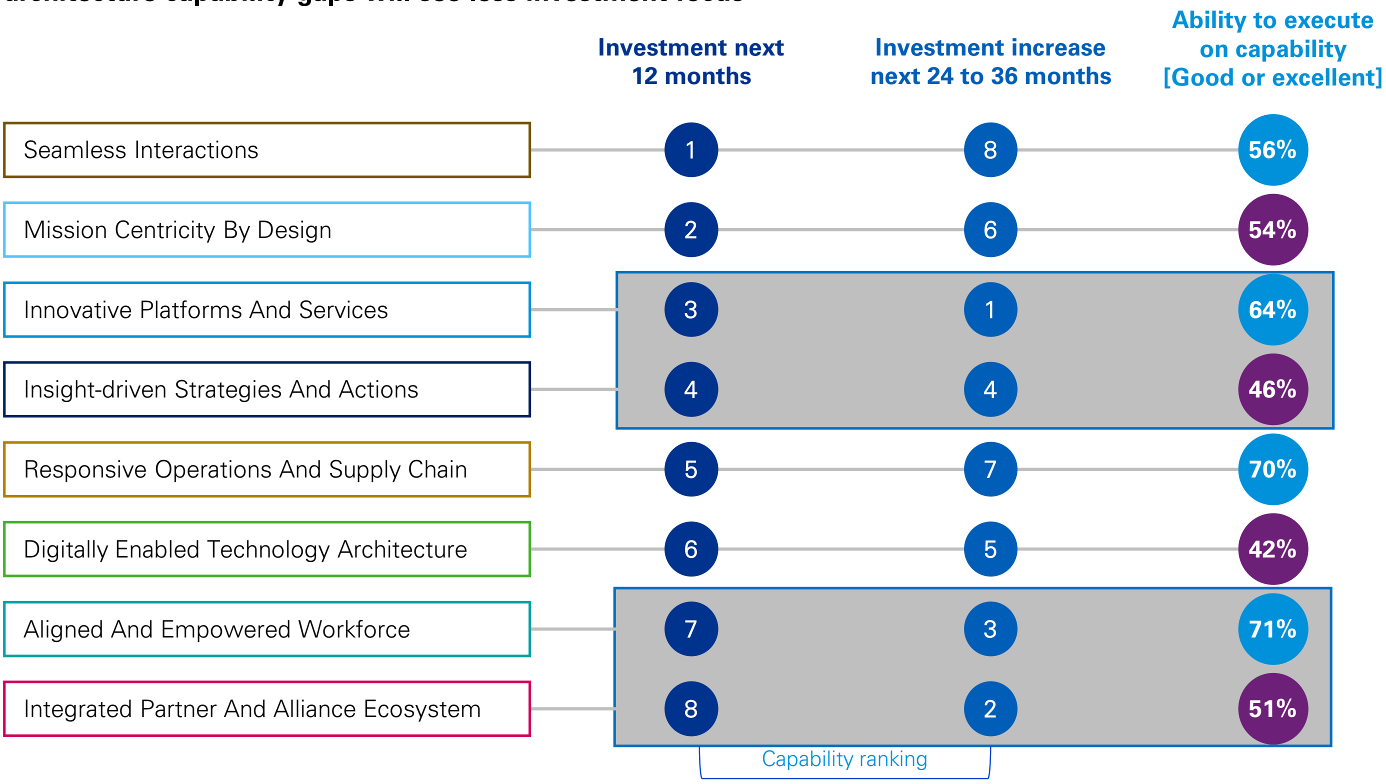
> **"A connected enterprise can help build trust between defense organizations and their many partners. But industry must be comfortable with 'leaning in' to share data."**
>
> Peter Griffiths, Lead Partner, Defence & National Security, KPMG Australia

Just 23 percent of defense professionals say their organization will be investing significantly in relationship management in the next 12 months.

Investment priorities

Defense organizations are increasing their investment in improving capabilities like relationship management, organizational alignment and people, and strategy. However, other capabilities – notably mission centricity and technology architecture capability – are experiencing a relative decrease in investment. This is a concern given the respondents' perceived lack of excellence in these areas.

Investment increases for relationship mgt. will help plug up deficiencies, but mission centricity and tech architecture capability gaps will see less investment focus



	Investment next 12 months	Investment increase next 24 to 36 months	Ability to execute on capability [Good or excellent]
Seamless Interactions	1	8	56%
Mission Centricity By Design	2	6	54%
Innovative Platforms And Services	3	1	64%
Insight-driven Strategies And Actions	4	4	46%
Responsive Operations And Supply Chain	5	7	70%
Digitally Enabled Technology Architecture	6	5	42%
Aligned And Empowered Workforce	7	3	71%
Integrated Partner And Alliance Ecosystem	8	2	51%

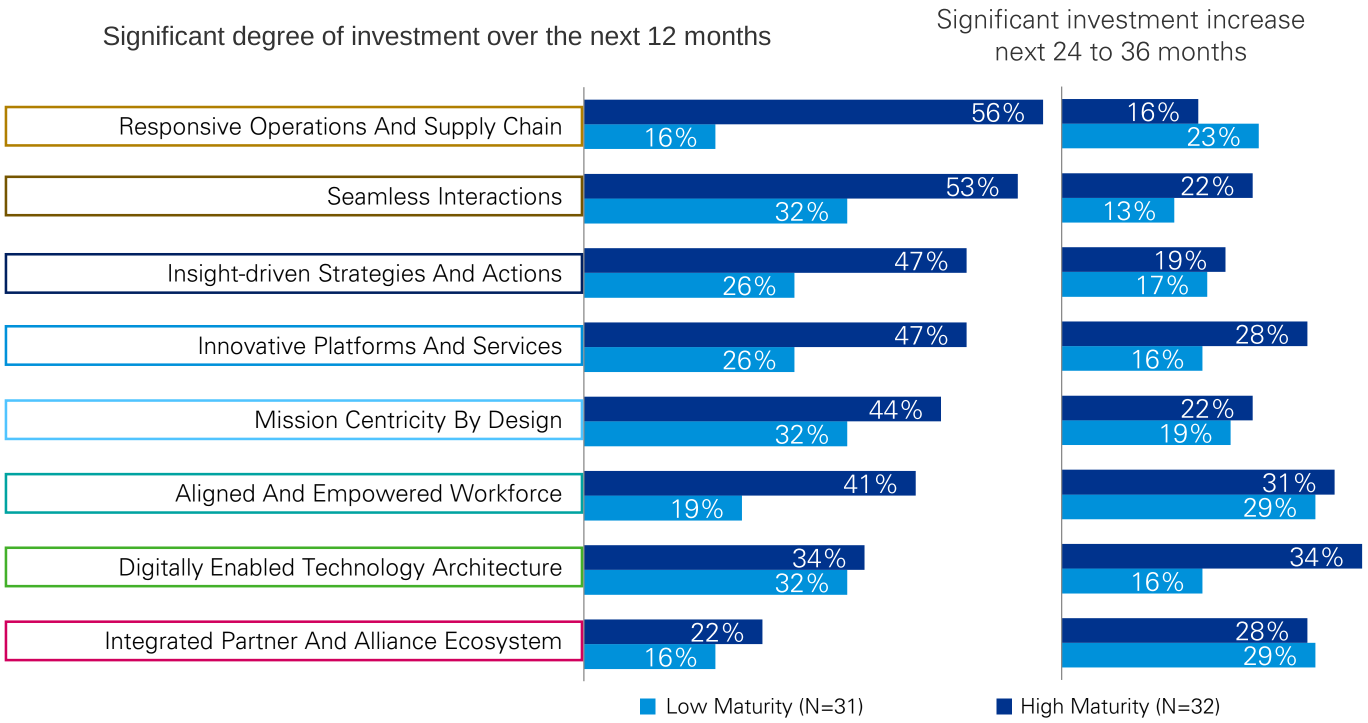
Base: 122 professionals involved with customer-centric strategy decisions at defense organizations

Source: A commissioned study conducted by Forrester Consulting on behalf of KPMG, February 2019

High-maturity organizations invest in capabilities

And those defense organizations considered more mature ‘connected defense forces’ are investing more heavily across all the eight capabilities – although their less mature peers are striving to close the gap over the next 3 years. In a fast-moving environment, no defense force can afford to fall behind in terms of connected capabilities.

High-maturity organizations invest in capabilities



Connected enterprise in action: examples from other sectors

Banking: Ensuring anytime anywhere banking

An omnichannel customer experience is a crucial capability for banks. By restructuring the organization around the customer 'journey', this major bank is now able to exceed the expectations of empowered and tech-savvy customers. Systems have been automated and decision-makers receive important insights on customers, and the bank has strengthened its competitive position.

Not-for-profit: meeting members' expectations

With almost 3 million members, this trade association was losing its market relevance, with fragmented services and an inconsistent customer experience. By identifying and addressing gaps across the front, middle and back offices, and uniting these three areas in a common cause, the organization has created a seamless, efficient digital offering. It is now transforming into the 'association of the future', powered by data analytics to ensure continuous improvement.

Automotive: a new direct-to-customer business model

This global carmaker is rethinking its relationship with customers, launching a new brand that can be owned or shared. By understanding the customer experience, it has designed a new operating model built around a technology platform, that gives customers the service they want, where and when they want it.

Retail: profitable growth from a connected enterprise

In a tough market, a global retailer wants to be more agile and customer-focused, with greater use of shared services. Its new model is both customer and employee-centric, integrating functions and channels and fostering a culture of excellence. The customer experience is now consistently excellent at a reduced cost-to-serve.

Five ways to build a connected defense force

A mere 41 percent of the defense professionals surveyed feel they are going above and beyond in delivering the 'customer' experience – where 'customer' means the overall mission, the front-line troops, key decision-makers and, ultimately, government.

Yet, as one survey participant, from the Investment Portfolio Management Branch, Defense Force Headquarters, Australia, notes, *"There is an ongoing expectation that we are customer-centric, we are customer-driven. We're here to deliver the best outcomes we can for the taxpayer, for our ministers, for our citizens, for our war fighters."*

A connected defense force can meet these demands, but each defense organization has its own path to this state. We believe the following five action points can accelerate this journey:

1 Plan for 5G's revolutionary opportunities

Many defense forces are investing in the latest equipment but not in the latest connectivity. All defense forces should be considering how to exploit 5G to release their potential, by connecting mobile devices and sensors on hardware. It's important for defense leaders to recognize that 5G is a game-changing technology – and invest accordingly.

2 Keep an ear to the ground for emerging technologies

Organizations need to think about when equipment and services will become commercially available – much of this coming from the civilian world – and how this can be applied in a military sphere. This requires a constant radar for innovation and a practical investment and early adoption plan. It may also require new commercial models that lower the barrier for entry for small-to-medium enterprises to enable defense forces.

3

Turn information into insights

Defense forces need a strategy for capturing, integrating, storing and enriching data to provide a real-time, 360º view of the mission. They should also improve the data literacy of the workforce to turn data into insights into action. This means adopting basic statistical and advanced tools to meet emerging analytical needs, along with strong governance, to ensure consistent methodologies and procedures for information security and privacy.

4

Invest in partners

Develop a plan to identify partners, alliances and vendors who can fill any capability gaps within your organization. Such an approach is especially important for areas like microelectronics, where some providers may be seen as having conflicting national versus commercial interests. Establish platforms that can integrate internal systems with partners and third-party providers. And finally, invest sufficient time in building partner relationships, along with firm governance for managing these partners.

5

Reimagine your workforce

With cyber and robotics playing an increasing role in warfare, the balance of defense workforces should shift from fighting forces to digital experts. This means recruiting specialists not generalists, and rethinking career paths to accommodate individuals that don’t fit the traditional military stereotype. And, critically, defense must give its workforce the most up-to-date technological tools – they expect nothing less.

Throughout this document, “we”, “KPMG”, “us” and “our” refer to the network of independent member firms operating under the KPMG name and affiliated with KPMG International or to one or more of these firms or to KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm.

Why choose KPMG to help you build a connected defense force?

We understand your business

We are proud of our heritage supporting defense organizations, and understand their need for an informed, evidence-based transformation approach that is focused on force readiness and connectedness across the entire defense organization.

Our knowledge of the defence business, and our experience cutting across the silos within defense, means we are able to tailor approaches that are relevant to your context and provide a sustainable, connected platform for future innovation.

When supporting you on your transformation journey, we can also bring insights from both our global defense network across our member firms, and from our significant experience in digital transformation across the private sector.

We are focused on delivering your outcomes

Our focus is on supporting you to deliver connected transformation that achieves tangible benefits to defense and national security. We work shoulder to shoulder with you and bring the best of our local, global and alliance capabilities to help ensure your outcomes are delivered. We do this in a manner that prioritizes collaboration and knowledge transfer to empower you to translate insights into real actions and results.

We know how to exploit technology to help you deliver a connected force

Through our global network of alliances, our knowledge of your environment and proven program delivery capabilities, we can help you to exploit emerging cloud-based and mobility technologies and convene the right ecosystems to digitally connect your organization.

More importantly, we also offer a proven transformation methodology and results-driven use of data and technology, to deliver a connected enterprise that can help you gain an edge over the adversary.

Throughout this document, "we", "KPMG", "us" and "our" refer to the network of independent member firms operating under the KPMG name and affiliated with KPMG International or to one or more of these firms or to KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm.

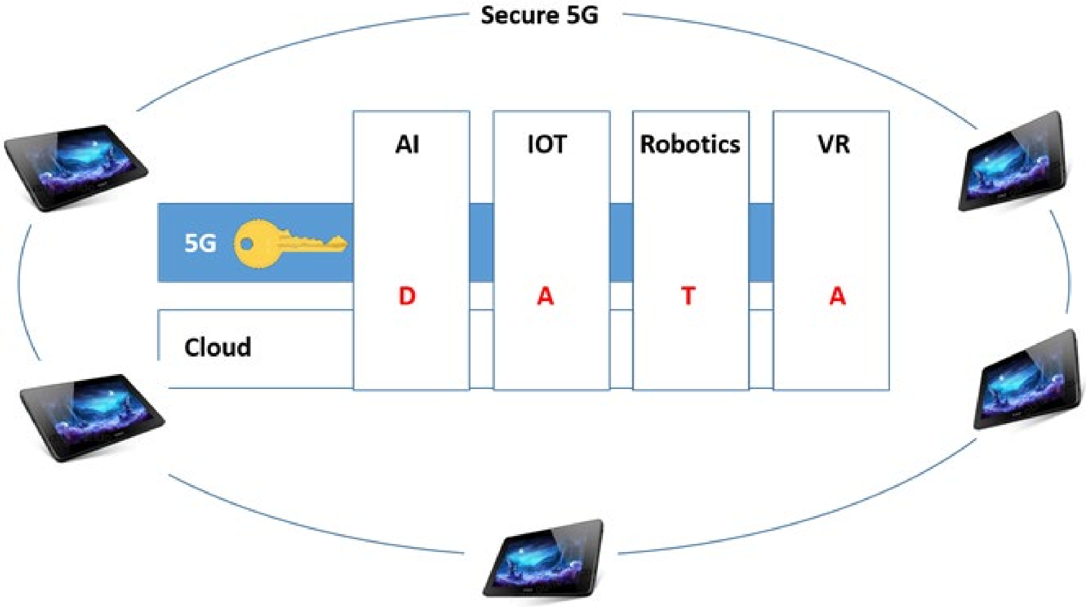
Appendix

Why 5G is the key to unlocking a wider ecosystem

Although 5G, in and of itself, is likely to be the most disruptive technology globally over the next 3-5 years, it is its wider ecosystem that will be truly revolutionary, particularly for enterprises.

5G is the lynchpin of an ecosystem that will connect everything and everyone, everywhere… even Tupperware[5] is going digital! This ecosystem has data at its heart, and it will enable the veritable tsunami of data from myriad sources that 5G is likely to release, to be securely exploited in new ways.

Apart from 5G, this ecosystem consists of other technologies that are all maturing at just the right time. They are: augmented intelligence, the internet of things (IoT), robotics and augmented/virtual reality. The cloud is also an essential ingredient, as is cyber security and privacy. Together this ecosystem will power the fourth industrial revolution, otherwise known as Industry 4.0.



Essentially, there is a confluence of other technologies that are maturing at just the right time to exploit 5G. This should supercharge these other technologies and together the sum of the parts can make the 5G story even more revolutionary. They should, for instance, deliver on, what to date has been, the empty promise of edge computing. Just how will this happen? Well, let’s examine the components.

Although it will take a number of years for there to be a universal rollout of 5G, the networking capability exists **now** to provide campus rollouts of private 5G networks, around such enterprises as ports, airports, factories, warehouses, universities, hospitals, arenas, entertainment centers and even metropolitan areas. These will not be dependent upon a universal rollout and can use fiber to provide long haul to other locations. The speed (the physics suggest up to 20Gbps is possible, but let’s say 10Gbps) and latency (less than a millisecond), as well as its ability to support up to a million active connections in every square kilometer, mean that every aspect of an enterprise can be connected. This can enable sensors and actors in equipment, such as industrial robots to intercommunicate amongst themselves and potentially make decisions independent of humans.

[5] https://www.digitaltrends.com/home/smarterware-smart-tupperware/

Most organizations effectively exploit less than 25 percent of the data that already exists within the organization. Artificial intelligence (AI) is making great strides, but it needs significant bandwidth to be able to operate on these workloads without degrading performance. 5G is set to release new waves of data, but also has the bandwidth to support the AI needed to make sense of it. This offers the potential to augment decision-making, both human and machine, by delivering very near real-time decision support.

At the same time huge strides forward are being made in the IoT arena. With embedded online sensors and actors in equipment, we can now, for instance, envisage full predictive maintenance of machinery, rolling stock etc., so that maintenance is conducted only when a part needs maintenance, rather than on a schedule, leading to huge productivity gains and cost saving. With the ultra-low latency of 5G, it is also possible for sensors to sense unusual vibrations in machines and stop production before damage is done.

Robotics is also advancing apace, particularly in factories and in the healthcare arena where very fine robotic surgery is now entirely feasible. In addition, aerial, land, sea and sub-sea drones are all rapidly advancing and should be controlled by 5G. We can readily imagine in a public safety situation, such as a major urban fire, the existing 4G network being swamped and going down, but 5G offers the potential to provide to first responders a secure communications envelope from an incident control point, supported by drones, plus the potential to then control and use drones to reduce the risk to responders.

Beyond this, augmented reality capabilities are also coming of age. The speed and latency of 5G, offers the ability to overlay additional details onto at, for instance sports events, or in the defense, industrial or medical setting onto heads-up display to enable hands-free enhanced working in real time.

The whole 5G ecosystem needs to be set in a cyber security and privacy envelope to fulfil its game-changing potential. Sensors and actors intercommunicating and making decisions independent of humans can only work if we can be sure that no malicious code has been injected and that the output we are going to get is what was expected. This is no mean challenge, but one of the key characteristics of 5G is the ability to 'network slice' and to enable different authentication on each slice, with negligible impact on the workload.

With good security, the 5G ecosystem should not just be the fundamental underpinning of Industry 4.0, but can also deliver on what to date has been the empty promise of edge computing, allowing parsing of vast amounts of data in mobile data centers at the edge and only passing back the results over the network to the corporate cloud.

So, whilst 5G in itself is a game changer, it is the fact that it unlocks a wider ecosystem of capabilities that is truly revolutionary in the enterprise space.

Throughout this document, "we", "KPMG", "us" and "our" refer to the network of independent member firms operating under the KPMG name and affiliated with KPMG International or to one or more of these firms or to KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm.

Throughout this document, "we", "KPMG", "us" and "our" refer to the network of independent member firms operating under the KPMG name and affiliated with KPMG International or to one or more of these firms or to KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm.

Contact us

Mike Stone

Global Chair of Defense and National Security

T: +44 20 73112807
E: Mike.Stone@kpmg.co.uk

kpmg.com/connected

Throughout this document, "we", "KPMG", "us" and "our" refer to the network of independent member firms operating under the KPMG name and affiliated with KPMG International or to one or more of these firms or to KPMG International.

Designed by CREATE | CRT118904