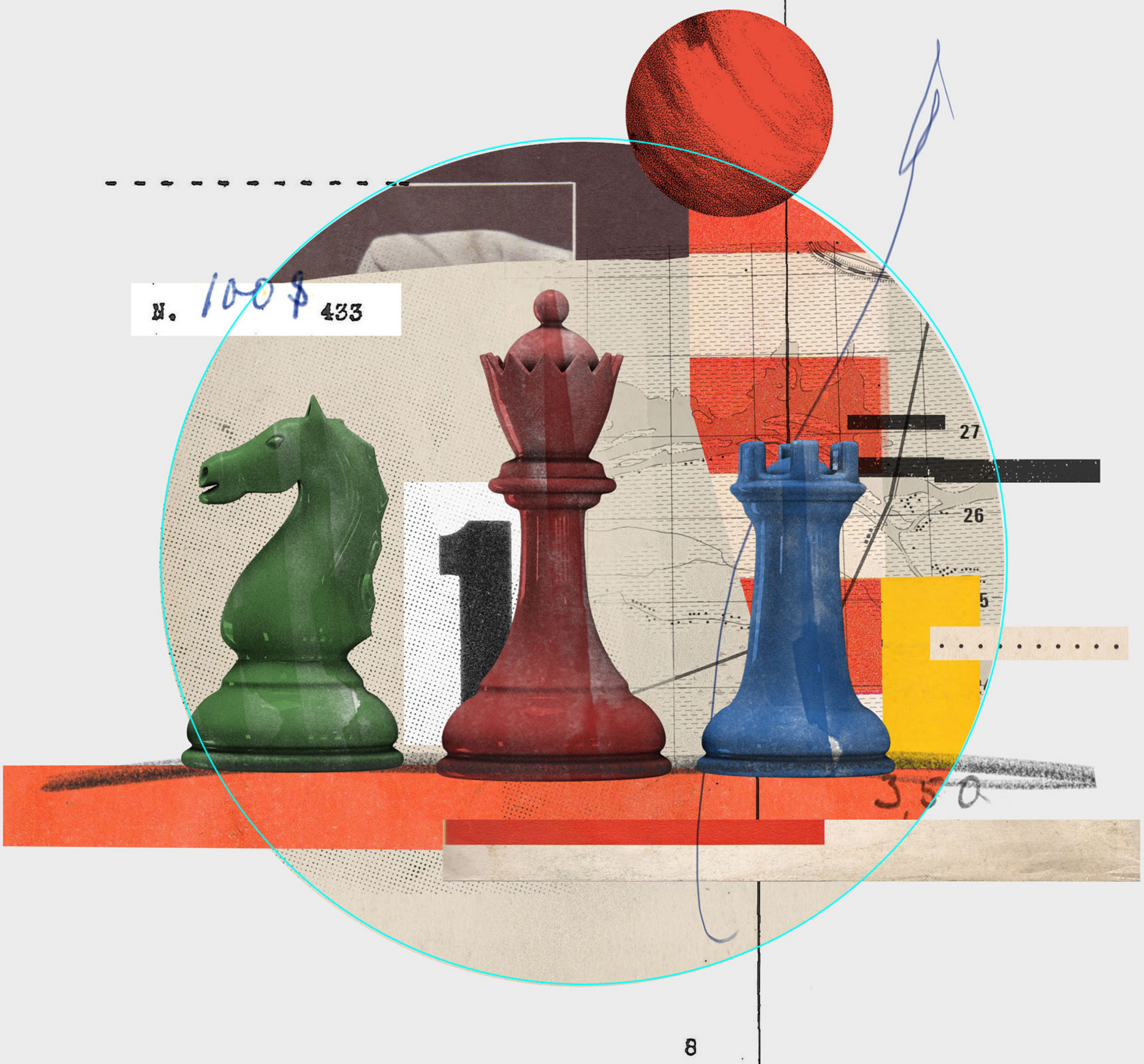
Deloitte. Insights

A report from the
Deloitte Center for Government Insights



Sum of its parts

Military interoperability and the future of warfare

A Deloitte series on the Future of Warfighting

About the authors

Roger Hill | roghill@deloitte.ca

Roger Hill is a principal in Deloitte's Government and Public Services Industry. Hill serves as the Lead Client Service Partner for the US Army account. He also serves as the Department of Defense Sub-Sector Lead. He has over 23 years of experience providing expert risk and financial advisory services to the Department of Defense (DoD), Intelligence Community (IC), Department of Homeland Security (DHS), and the Department of Justice (DoJ). Hill possesses extensive knowledge of Federal accounting, auditing, internal controls, budgeting, and financial systems. His focus over the past 23 years is assisting the Department of Defense and Intelligence Community Agencies with executing audit readiness/remediation, improving internal controls, integrating budget and performance information, and introducing both functional and system solutions to transform core FM processes.

Darren Hawco | dhawco@deloitte.com

Darren Hawco is an executive adviser in Deloitte's Consulting practice. He is a retired senior military officer and executive with extensive public, military, and allied services experience. Hawco is particularly skilled in intelligence, operational, tactical planning, as well as capability design, crisis, and operations management. Hawco holds a Master of defense policy and a Master of Public Administration focused in defense policy and public administration from Royal Military College of Canada/Collège militaire royal du Canada.

Adam Routh | adrouth@deloitte.com

Adam Routh is a manager with Deloitte's Center for Government Insights and a PhD student in the defense studies department at King's College London. His research areas include space policy, the future of defense, and great power competition. Routh's research has addressed US national space policy, space governance, the challenges and requirements of the future military force, and emerging technologies. His analysis has been featured on the nightly news and the John Batchelor Show, and published in *National Review*, *The Hill*, *The National Interest*, *Space News*, *The Space Review*, *Real Clear Defense*, and *Defense News*, among other outlets. Routh previously worked for the defense program at the Center for a New American Security (CNAS). Prior to CNAS, he worked in the private sector where he facilitated training for Department of Defense components. He also served as a team leader with the US Army's 75th Ranger Regiment.

Joe Mariani | jmariani@deloitte.com

Joe Mariani is a research senior manager with Deloitte's Center for Government Insights. His research focuses on innovation and technology adoption for both national security organizations and commercial businesses. His previous work includes experience as a consultant to the defense and intelligence industries, high school science teacher, and Marine Corps intelligence officer.

Akash Keyal | akkeyal@deloitte.com

Akash Keyal is a senior research analyst with the Deloitte Center for Government Insights. He focuses on delivering key insights on topics related to defense, security, and justice.

Contents

Introduction

A CH-47 HELICOPTER WHIPS up the dust as it touches down in the Sahel. Weary French paratroopers trudge aboard after a long patrol searching for terrorists as part of France’s Operation Barkhane. Plugging in his headset, the paratrooper commander is surprised to be greeted by a cheery “allo mate” from the English crew chief. These British helicopters are just part of a broader push for interoperability between UK and French militaries that includes a combined expeditionary force and shared R&D projects.[1] And against other defense challenges, like peer warfare or gray zone threats, interoperability will need to be magnified compared to what’s necessary for a fight against violent nonstate actors. To be sure, for all nations, interoperability is likely to be a defining feature of the future of conflict.

Today’s defense challenges, from near-peer warfare to defending a rules-based international order and gray zone threats, exist at a scale and scope that no military can meet alone.

Interoperability is not new. Already, the bulk of military operations conducted throughout the world are multilateral affairs. But while these multilateral operations may yield greater legitimacy and more operational effectives, these benefits are often overshadowed by the increased costs and difficulties of interoperability. The joint UK-French expeditionary force mentioned above, for example, struggled with everything from basic equipment interfaces to more challenging differences in rules of engagement and command philosophy.[2] As a result, while most militaries value interoperability, there has been little incentive to make it a top priority. That is, until now.

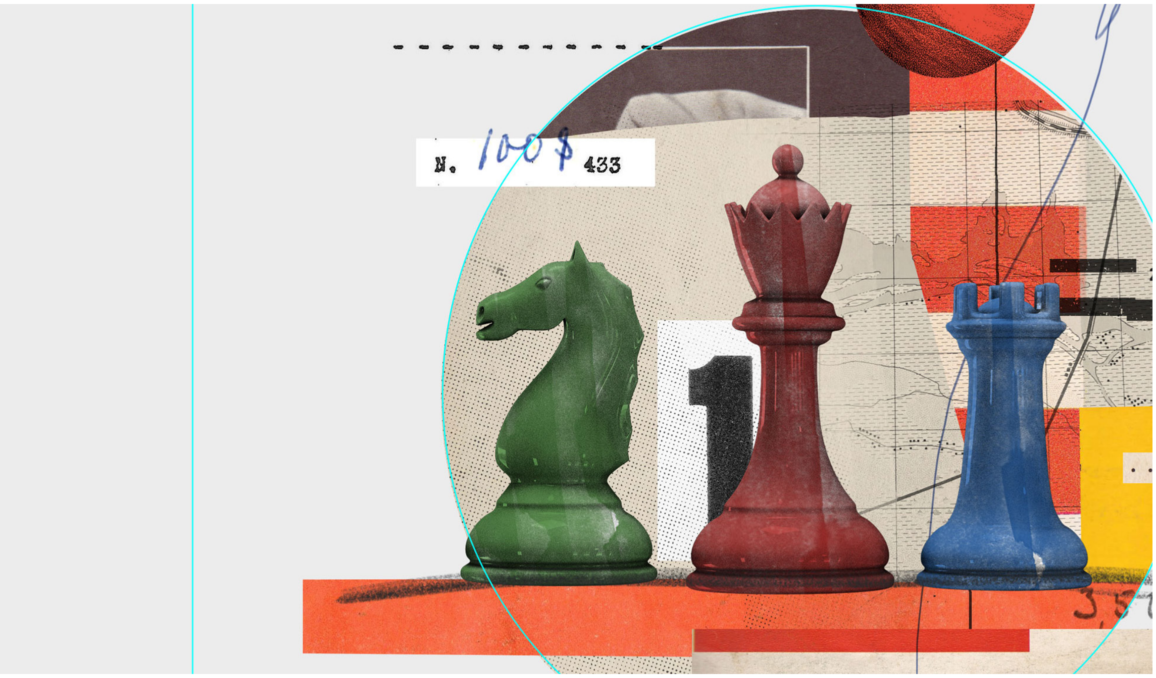
ABOUT THE FUTURE OF WARFARE PROJECT

The Deloitte Center for Government Insights is undertaking a yearlong research project focused on helping defense organizations prepare for the next 15 years of defense challenges. While defense challenges are ever shifting, our research has identified interoperability—within militaries, within government, between nations, and with industry—as being key to meeting uncertain threats.

Through more than 60 specialists representing 12 countries across North America, Europe, and Asia, this project will produce more than a dozen insights articles offering ways of improving interoperability across key military areas. Research will detail how specific defense organizations can improve interoperability across defense challenges based on country-level expertise. The goal is to not only promote discussion at the international and intranational levels, but demonstrate, in part, how greater interoperability can be realized.

Today's defense challenges, from near-peer warfare to defending a rules-based international order and gray zone threats, exist at a scale and scope that no military can meet alone. No nation has enough precision-guided munitions to sustain a protracted peer engagement by itself; at the other end of the spectrum, no military can by itself address the flood of mis- and disinformation permeating social media platforms. Success against today's national defense and security challenges requires militaries to operate outside themselves, to be interoperable with other nations, other government agencies, and even commercial industries in new ways.

In the future of warfare, interoperability is more than just a political expedient; it is a strategic advantage. Interoperability gives militaries more options and greater strategic agility in meeting any threat, in any domain, with any mix of partners that context might dictate. But to realize that vision takes hard work to shift the basics of how defense organizations plan, equip, and operate. Nations that put in the hard work now will find themselves better able to meet the demands of the future, whatever they may be.

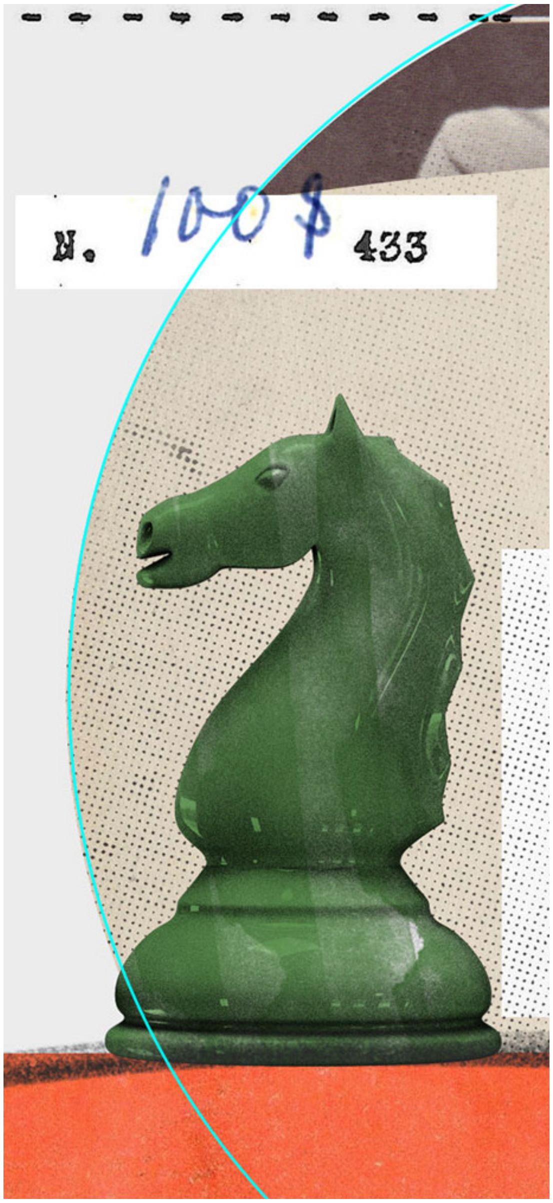


The future of warfare requires interoperability

DEFENSE ORGANIZATIONS HAVE always changed to align with changing national interests and missions. Each time the mission changes, the organization, equipment, and even culture can shift as the needs of military power adjust to new threats.

Today's leading defense challenges, assessed from strategy documents of 12 countries across North America, Europe, and Asia include near-peer warfare, gray zone threats, limited-scale warfare, and defending the rules-based international order.[3] What makes these defense challenges particularly difficult for today's militaries are their large scope and scale. Scale is easily seen in peer warfare or in the debasement of the rules-based international order, both of which can have global military, diplomatic, and economic ramifications. Gray zone cyberthreats are another example of how the scope of modern defense challenges can extend well past just military targets. The 2020 SolarWinds attack started with a single industry vulnerability but through shared cyber tools made its way throughout industry and government agencies, exposing unprecedented amounts of sensitive information along the way.[4]

What makes these defense challenges particularly difficult for today's militaries are their large scope and scale.



FOUR LEADING DEFENSE CHALLENGES

For the purposes of this research, we have identified the four leading defense challenges below:

- **Near-peer/peer warfare** is warfare between two near-equal or equal adversaries and is often associated with great powers. The equal position of the belligerent parties often encourages the use of alliances, which can ensnare other countries, and the use of a wide spectrum of military, diplomatic, economic, and other tactics designed to encourage total submission to achieve victory.
- **Gray zone threats, particularly from technology**, are adversarial activities that can affect a wide spectrum of national interest domestically and abroad by operating under the threshold of conflict or by allowing the act to go undetected or unknown long enough to make attribution and/or retaliation difficult. They can include cyberattacks, election meddling, exploiting the lack of established rules to maliciously exploit emerging technology such as space assets or cyber tools, or sowing doubt in international institutions to undermine the international rules-based order.
- **Limited-scale warfare** is a somewhat debated concept. Generally, limited-scale warfare speaks to conflict that falls short of total war, or warfare that leverages a nation's total capacity to fight. For this research, limited-scale warfare includes warfare between states or organized groups where significant, but not total, military mobilization is used. Limited-scale warfare doesn't include competition between states short of armed conflict, sporadic counterterrorism operations, or war between great powers.
- **Defending the rules-based international order** can generally be described as a "shared commitment by countries to conduct their activities in accordance with agreed rules that evolve over time, such as international law, regional security arrangements, trade agreements, immigration protocols, and cultural arrangements." [5] The reason states wish to undermine the rules-based order is often because their political or economic systems conflict with or are not advantaged by the existing rules-based order, and therefore wish to replace it or limit its influence for relative advantage.

The scope and scale of today's leading defense challenges require too much of any single defense organization; there simply isn't enough time, money, or people within a defense department or ministry to effectively address the range of challenges. As a result, many of the strategies that defense departments and ministries are devising to combat today's challenges demand significant coordination with other government agencies, other nations, and even commercial companies.

Take US Cyber Command's new strategy of "defend forward" as just one example. Designed to counter gray zone cyberthreats, this strategy involves the placement of US military cyber experts in foreign countries to disrupt attacks headed for the United States. This strategy demands coordination with host nation governments, their military and security agency cyber forces, and familiarity with regional commercial technology companies.[6]

But most militaries are just not organized to enable the coordination required for today's defense challenges. For example, despite the US Army's commitment to international interoperability and the many interoperability, efforts underway across NATO, ABCANZ Armies, Africa, and Asia, there is only one purpose-built Army unit at the Service Component Command level designed for interoperability—a 30-soldier Digital Liaison Detachment providing digital information-sharing capabilities to allied and multinational forces.[7] When militaries aren't organized for interoperability, they must create it by patching together existing processes and activities not designed for interoperability. The patchwork approach can add costs, create capability dependencies, present capability gaps and seams, and remain inflexible to diverse defense challenges.[8]

Successful strategies against leading defense challenges, then, must include an expanded understanding of interoperability. Exactly what kind of interoperability may vary by the specific threat and country involved, but nearly every strategy for future threats will require defense organizations to work with organizations outside of their comfort zone.

New threats demand renewed focus

FROM GRAY ZONE threats to near-peer conflict, adversary strategies are focused on taking advantage of weaknesses or eliminating the critical nodes that friendly militaries rely on. A single exploitable weakness can mean the difference between an effective defense or not. For example, in peer warfare, militaries are likely to find themselves facing adversaries waging "systems confrontation warfare" designed to cripple the very national and strategic systems a modern military relies on, including communications, logistics, and command and control.[9]

For the United States, a recent Department of Defense wargame showed traditional ways of operating against an enemy targeting critical military systems meant the loss of communications and the battle.[10] The wargame hosted to test the United States' Joint Warfighting Concept designed around interservice interoperability, showed that traditional assumptions—for example, that information will be ubiquitous—led to fatal dependencies easily exploited by the adversary.

A single exploitable weakness can mean the difference between an effective defense or not.

A similar story emerges from other threats such as gray zone influence campaigns. These campaigns, such as that carried out by Russia during the 2017 German election, target democracies' critical node of public perception through a variety of nefarious means.[11]

Interoperability with other government agencies, industry, and allies and partners acts as an important hedge against these adversary strategies by creating affordable redundancies and expanding operational choices. For example, in the case where a peer adversary targets critical communication nodes, interoperability with an allied nation can provide alternative communications pathways that provide redundancies and challenge the adversary by requiring it to attack more targets. For example, the United States has recently recognized that the very expensive but few military satellites it relies on, pose a risk to military operations during conflict because such a small number of critical systems makes for ideal targets.[12] As a result, US Strategic Command is pursuing a new communications architecture prototype that will allow communications to easily transition from military to allied to commercial satellite communications in the event one of the satellites is disrupted.[13]

Similarly, interoperability with commercial technology companies can help provide defense and security agency organizations more avenues to respond when confronting an online mis-/disinformation campaign. Together, these types of interoperability increase operational resilience and options that match the increased scope and scale of today's defense challenges.

Militaries have used interoperability in the past to create exactly this resilience. For example, the proximity fuse, a top-secret radar-based artillery fuse, was originally developed in Britain during the early stages of World War II. But under the strain of the Battle of Britain, the United Kingdom was having trouble operationalizing the technology. By making the research available to the United States, the British were able to tap into not only new sources of supply beyond the reach of German bombers, but also US research capacity, resulting in more and improved proximity fuses reaching British forces. These fuses turned out to be critical in defeating the V-1 flying bomb threat to British cities.[14]

In this way, interoperability doesn't just improve tactical operations; it becomes an important contributor to strategic advantage. In addition to being a technological development accelerator, interoperability can also provide the resilience critical to mitigating the dangers posed by today's myriad of threats. This doesn't require allies and partners to change in the same way, have the same equipment, or even adopt uniform concepts of operation. Instead, it would require leveraging allies and partners, industry, and other government organizations based on their strengths.

Reassessing the value of interoperability

TRADITIONALLY THE VALUE of interoperability was twofold: It could help create coalitions that gave military action greater political legitimacy, and it could improve some operational efficiency. The problem is that interoperability also involves significant costs that can counteract those benefits. It takes money to buy interoperable radios; it takes extra time and effort to coordinate combined operations, and so on.[15] Yet many of the defense challenges of the last 20 years, such as counterinsurgency operations or foreign disaster relief, required relatively limited interoperability. When the cost is high but the strategic and operational return on investment is low—with some exceptions, as is the case for NATO while Russia poses a threat—defense organizations don't have an incentive to increasingly organize around the idea, leaving interoperability efforts to stagnate around select functions or allies and partners. As a result, the benefit of enhancing interoperability to another level or among a wider range of intranational and international partners is rarely seen as justifying the significant costs.

So what is different today? Simply put, interoperability helps provide a strategic advantage in facing today's increasingly complex defense challenges. With new threats targeting the core systems of friendly countries, not just militaries but political systems, infrastructure, and more, the flexibility and resilience that interoperability can provide become a critical element of advantage. But to realize an advantage, defense organizations need to mature beyond traditional forms of interoperability to include other government organizations, private industry, and the various politics, policies, and economics that come with broader coordination. Today's defense challenges may resemble those of the past, but their character is new. To keep pace, interoperability must also take on a new character: one that is more inclusive and sown into the fabric of defense organizations.

So what is different today? Simply put, interoperability helps provide a strategic advantage in facing today's increasingly complex defense challenges.

A modern take for modern challenges

MILITARIES HAVE CULTIVATED interoperability throughout history. The first battle ever recorded in history featured a large coalition force composed of Canaanite vassal states.[16] In the nearly 3,500 years since that battle, interoperability was developed to help preidentified nations work together. NATO represents this line of thinking. Its standards and training have been critical to multinational coalitions from the first Gulf War to Iraq, Afghanistan, and Syria.[17] But NATO is still built on a vision of interoperability among a predefined group of states, and principally along military lines. If a non-NATO member military wishes to take part in NATO training, it must procure the equipment NATO requires to be interoperable, such as radios and the associated communications security software.[18] But procuring specific radios for a training exercise or following strict approval processes to access security software describes a strict form of interoperability where other militaries conform to NATO rather than NATO meeting other militaries where they add value. It connotes an important element of military-to-military tactical interoperability, but it is in and of itself a limited expression of what interoperability could and should be.

In facing peer warfare, gray zone threats, defending the rules-based international order, or limited-scale warfare, the goal is not to develop interoperability as a static model, but to create a defense organization that can adjust its interoperability to missions, allies, and technology.

Today's defense challenges often require a more flexible vision of interoperability. The exact participants of a coalition may not be known ahead of time; key participants and/or partners may not even be militaries but commercial technology companies or NGOs or private logistics providers. Even the challenges themselves are variable. Every defense challenge requires interoperability, but not necessarily the same level of interoperability in every function. Defending a rules-based international order, for example, may demand high levels of workforce interoperability with personnel conversant in the military, commercial, and international resources needed to defend the values and institutions the rules-based international order is built on. Yet, it likely will not require the same close integration of acquisition systems needed in near-peer or limited-scale warfare. This means that rather than nations simply reaching for maximum interoperability in every function for every threat, nations and their defense organizations should tune their interoperability efforts to their specific circumstances.

In facing peer warfare, gray zone threats, defending the rules-based international order, or limited-scale warfare, the goal is not to develop interoperability as a static model, but to create a defense organization that can adjust its interoperability to missions, allies, and technology. To create such an organization requires prioritizing investments in interoperability across four military functions (figure 1). A defense organization should balance how it chooses to develop its interoperability based on the resources at its disposal, its ranking of priorities, and the complementarity of its military, commercial, and government partners, the goal being to achieve enough national interoperability across defense challenges to gain a relative advantage over each priority and situation.

USING THE INTEROPERABILITY INDEX

The interoperability index includes interoperability functions, which cover the spectrum of military activities, and a complementarity progression, which shows how certain tools or processes can progressively create interoperability between actors. These features are assessed against defense challenges noted by color bars at the bottom of relevant boxes within the index.

Interoperability functions

- **Development and acquisition systems**–The full spectrum of activities from basic science research to contracting that turn ideas into material for defense organizations.
- **Resilient operations**–Operational forces employing the full range of their physical digital tools to maneuver, sustain, protect, and apply force.
- **Workforce, skills, and culture**–The composition, recruitment, training, and organization of the workforces that execute defense tasks, regardless of where they work or if in/out of uniform.
- **Decision-making ability**–The collection, processing, analysis, and dissemination of information to support leadership decision-making at every level of a defense operation.

Complementarity progression

- **Baseline**–The minimum level of interoperability needed for any organization to function well and properly.
- **Joint/Service**–The ability of military services/departments to coordinate organizational and operational activities.
- **Intranational**–Closely coordinated relationships between defense organizations, other government agencies, and commercial industry within a nation.
- **Intercountry**–The ability for nations to work together either bilaterally on a series of issues that cut across government/industry, or multilaterally on issues of limited scope.
- **Systemic**–The ability for defense, other government, and commercial industry organizations to work together in real time on complex, evolving issues.

FIGURE 1

The demands of interoperability vary with defense challenge

Assessed level of interoperability needed

⬛ Gray zone threats 🟦 Near-peer/peer warfare 🟩 Defending rules-based international order 🔷 Limited-scale warfare

	Baseline 1	Joint/Service 2	Intranational 3	Intercountry 4	Systemic 5
Development and acquisition	• Repeatable, transparent acquisition processes	• Ability to own and share technical data for select acquisition programs (e.g., via digital or model-based systems engineering) • DevSecOps, Agile, or other iterative models of production used for select software development • Mechanism for joint requirements development/coordination (e.g., JROC in the United States) • Standards for joint interoperability of key systems • Services have access to technical baseline data • Flexible acquisition processes operating at the speed of technology 🟩	• Ability to own and share technical data for all major acquisitions (e.g., via digital or model-based systems engineering) • DevSecOps, Agile, or other iterative models of production used for all software development • Mechanism for efficient and timely intragovernment coordination • Open architectures to ensure better interoperability even of proprietary systems • Services have access to live data from systems • Enhanced and inclusive mechanism for government/industry coordination • Shared curriculum to educate leaders on emerging technology ⬛	• Ability to rapidly share technical details between/among government and industry to allow for distributed production (e.g., using common digital engineering tools) • Open architectures with international standards to ensure better interoperability even of proprietary systems • Mechanism for coordinating international rapid acquisition coordination • Mechanism for international authentication of trusted vendors and sharing of IP • International program for tech education and advancement 🔷	• Ability to share consumption/use data from tactical edge to inform network of international producers (e.g., common digital thread) • Allies iterative development of shareable systems • Mechanism for coordinating defense innovation with allies and partners 🟦
Resilient operations	• National forces can move to a conflict, sustain and protect themselves, and apply force to an adversary	• Common operational standards for common tasks such as air support • Ability to leverage other services'/central military capabilities for transport, fires, or logistics • Joint capabilities to protect integrity of force, including from industrial threats (e.g., suppliers or knowledge of suppliers)	• Shared appreciation of problem sets across government • Understanding the capabilities that industry/government can bring to bear • Process to leverage those capabilities form industry/government 🔷	• Shared understanding of allied forces' incentives, risks, and goals • Common operating picture for allied/partner/commercial military-relevant capabilities • Shared international standards for key components (types of fuel, size of pallets, radio encryption, data formats, permission, etc.) ⬛ 🟩	• Ability to seamlessly drive tactical data between countries, agencies, and even industrial bases to coordinate responses • Integrated information systems that can share data according to need and clearances • Ability to visualize and tap into military, allied, capabilities in real time at the tactical level 🟦
Workforce, skills, and culture	• Defined and accountable organizational culture in defense organizations • Recruitment sufficient to maintain desired end-strength and contemporary skills	• Talent management to account for individual workforce skills and needs • Capacity to quickly organize cross-functional teams • Agile hiring policies to attract and retain top talent in emerging skills • Change in mindset from "know it all" to "learn it all" • Joint standards for use of automation 🔷	• Talent management for interagency assignments • Shared skills and experiences between government and industry via rotation and new talent models • Government, industry, and academic collaboration to shape talent pipeline • Clearly defined inherently government functions and understanding of comparative advantage for all other functions	• Talent management that takes into account allied skills and capabilities • Shared skills and experiences between ally and partner industry, academia, and government • Create cross-functional allied/partner teams and automation 🟦	• Cultivate a culture of shared defense across nations, industry, and militaries • Workforce where military/civilians can leave and return to service • Shared understanding among allies/partner of appropriate use of human vs. automation (e.g., AI ethics principles) ⬛ 🟩
Decision-making	• Secure, reliable information systems • Trustworthy data • Timely data collection and analysis • An understanding of policy and legal boundaries/ permissions	• Coordinated architectures for interservice information management systems • Timely access to mission-relevant joint data • Joint leadership development curriculum tailored to the spectrum of defense priorities • Culture of trust to enable faster decision-making	• Common operating pictures for key issues shared across government agencies • Information management systems capable of bidirectional sharing of data operating in both connected and disconnected modes • Timely access to interagency mission-relevant data • Process for coordinating tasks based on agency legal/policy authorities • Interagency leadership development curriculum tailored to shared-mission areas 🔷	• Information and data management for seamlessly sharing information with allies/partners according to their clearance and immediacy of need without manual processes • Ability to visualize impacts to national interests across social, political, economic, and other dimensions (e.g., via narrow-scope AI tools) • Process for coordinating tasks based on international legal/policy authorities • International leadership development curriculum tailored to specific mission areas 🟦	• Ability to coordinate international response to threat in minutes or hours • Automated information and data management system for combined common operating picture tailored to mission need and permissions (e.g., via general-purpose AI tools) • Shared culture of trust/risk-taking • Adaptable policy and legal permissions for combined operations ⬛ 🟩

Source: Deloitte analysis.

What does this change look like?

WHILE THERE ARE few, if any, examples of militaries placing this broader view of interoperability at the center of their strategies, there are small-scale examples that show how organizational changes such as those highlighted in the index can come together to improve interoperability.

To see how, let's return to the example of UK-French collaboration from the introduction. The pinnacle of UK-French interoperability is the Combined Joint Expeditionary Force (CJEF), which became fully operational in 2020. To overcome the challenges of interoperability highlighted in the introduction—everything from equipment issues to differences in rules of engagement and command philosophy—both nations undertook a series of organizational changes (figure 2). For example, to improve operational resilience, both nations published the *Combined Joint Expeditionary Force Users Guide,* which laid out how forces will use their own national operational concepts as well as a defined political decision-making process for tasking the CJEF (second row in the figure).[19] Similarly, France and the United Kingdom have pursued several joint R&D and acquisition programs, including especially close collaboration in the missile space. The efforts include not only acquisition programs such as the Sea Venom missile, but also the developmental infrastructure that supports further acquisitions such as the creation of shared "Centres of Excellence" for critical enabling technologies (first row in the figure).

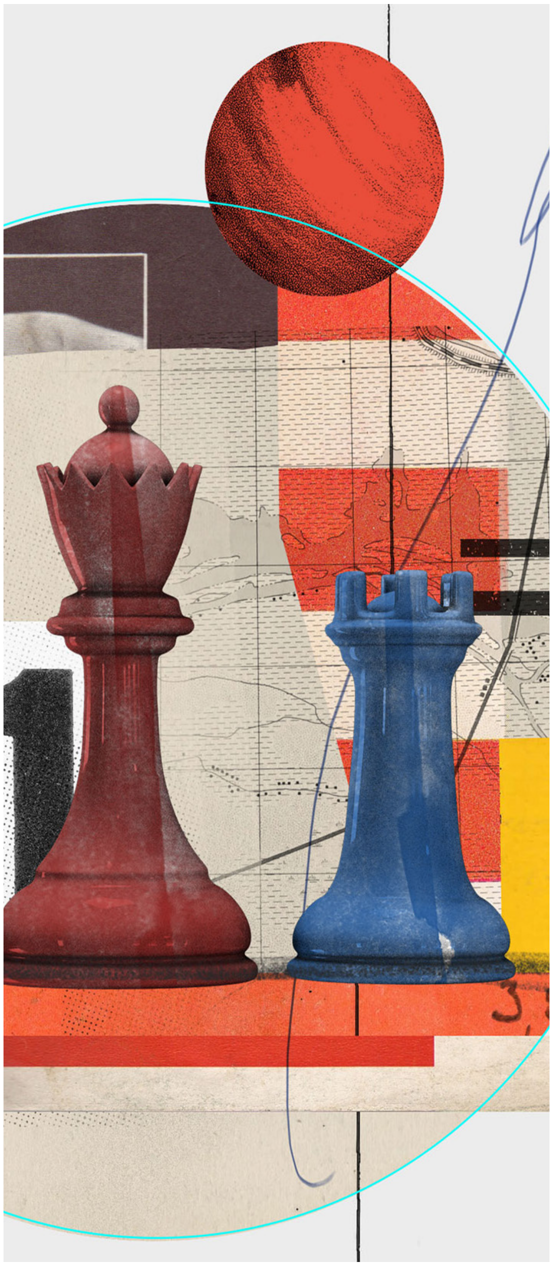
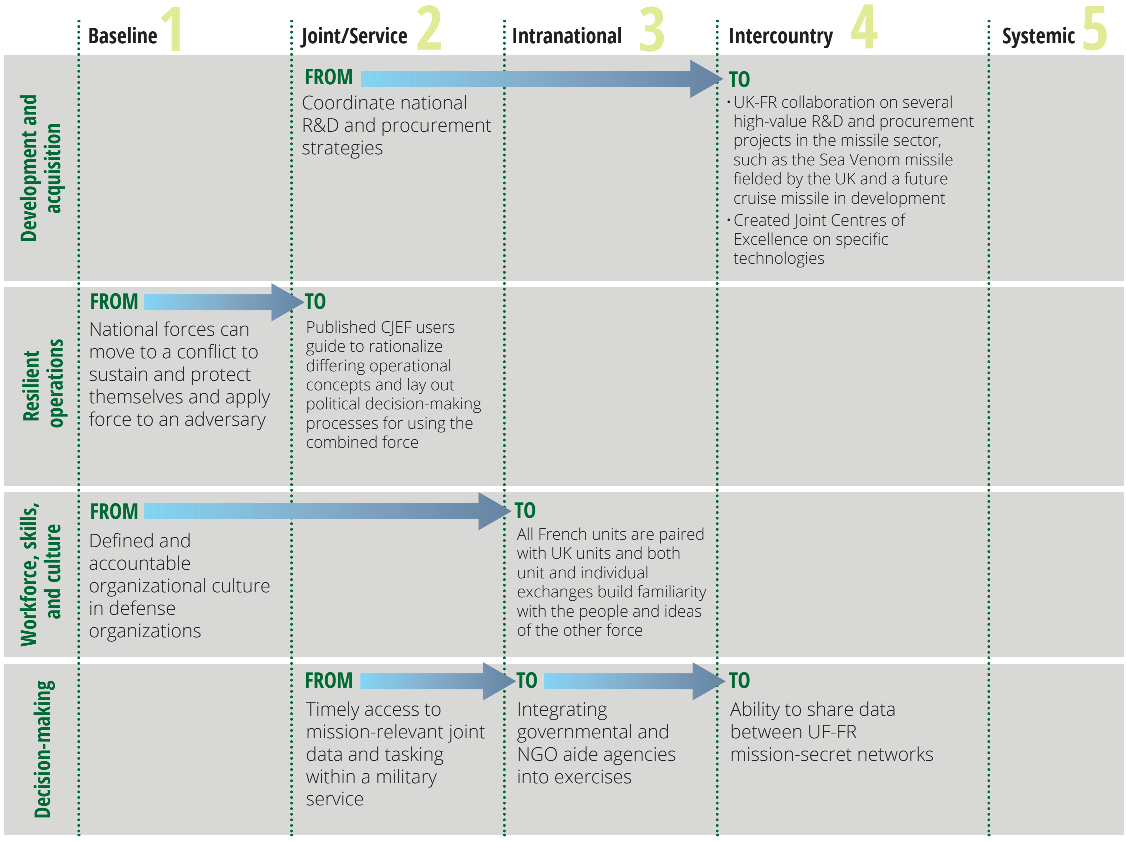


FIGURE 2

UK-French efforts point to how organizational changes can improve interoperability for a mission, but also where the future may require greater focus

Limited-scale warfare



	Baseline 1	Joint/Service 2	Intranational 3	Intercountry 4	Systemic 5
Development and acquisition		FROM Coordinate national R&D and procurement strategies		TO • UK-FR collaboration on several high-value R&D and procurement projects in the missile sector, such as the Sea Venom missile fielded by the UK and a future cruise missile in development • Created Joint Centres of Excellence on specific technologies	
Resilient operations	FROM National forces can move to a conflict to sustain and protect themselves and apply force to an adversary	TO Published CJEF users guide to rationalize differing operational concepts and lay out political decision-making processes for using the combined force			
Workforce, skills, and culture	FROM Defined and accountable organizational culture in defense organizations		TO All French units are paired with UK units and both unit and individual exchanges build familiarity with the people and ideas of the other force		
Decision-making		FROM Timely access to mission-relevant joint data and tasking within a military service	TO Integrating governmental and NGO aide agencies into exercises	TO Ability to share data between UF-FR mission-secret networks	

But even these efforts fall short of what may be required for many of the more complex threats in the future of conflict. For example, while the user's guide lays out some key considerations about operational interoperability, it could not resolve issues around differing rules of engagement or targeting procedures that required lawyers to be present during exercises.[20] Similarly, the impressive international R&D and acquisition remains limited in scope to specific projects or technical areas. The rapid and ad hoc sharing of technologies and data that may be required in high-end fights is still beyond the grasp of even these two closely collaborating allies.

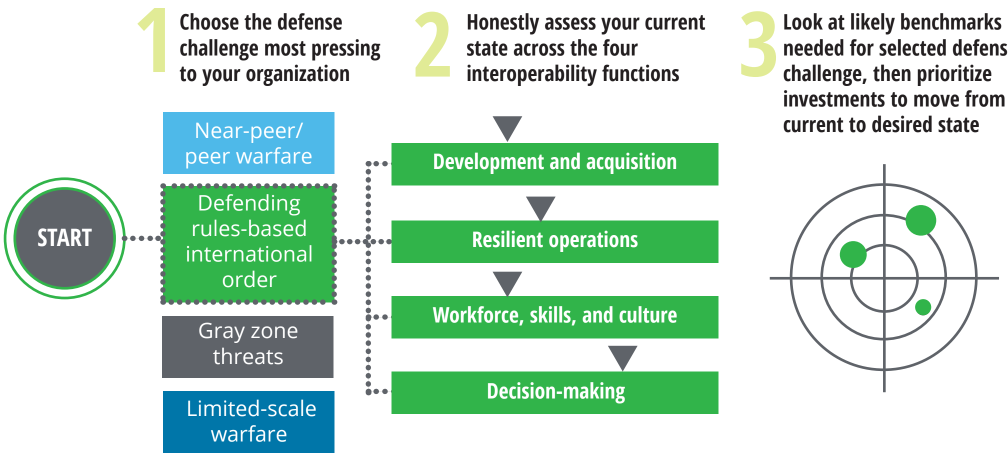
Interoperability is a process, not a destination

THE NATURE OF defense challenges today makes it near impossible for a nation's defense department or ministry to effectively defend against them all. The practical answer is to work together by deliberately and iteratively looking at how militaries, governments, and industry can take on the challenge together through interoperability.

The Deloitte Interoperability Index is designed as a tool to help inform this process. Importantly, it is not intended to provide detailed step-by-step directions toward a particular future. Attempting to provide detailed, one-size-fits-all directions to a dozen or more countries wouldn't likely be effective given the geostrategic differences among them. Rather, the index should be thought of as a map that each ministry and defense organization can use to improve its interoperability based on how it assesses its current defense priorities and interoperability needs (figure 3).

FIGURE 3

The Deloitte Interoperability Index is not a flat document, but a map that can help countries chart their unique course to the future


1
Choose the defense challenge most pressing to your organization
2
Honestly assess your current state across the four interoperability functions
3
Look at likely benchmarks needed for selected defense challenge, then prioritize investments to move from current to desired state
START
Near-peer/ peer warfare
Defending rules-based international order
Gray zone threats
Limited-scale warfare
Development and acquisition
Resilient operations
Workforce, skills, and culture
Decision-making

Charting a course from where you are to where you want to be

BECOMING MORE INTEROPERABLE will be an inherently collaborative exercise where defense leaders iteratively work with other government organizations, allies, partners, and private industry to understand what shape interoperability should take for each defense challenge and what is necessary to realize it. So how can defense organizations get started? A cyclic evaluation process can help:

By cultivating interoperability today, defense organizations can be ready for the future, whatever it may bring.

- **Use national strategy documents, wargames, and other analysis to gain a clearer picture of national defense challenges.** This can help leaders understand the likely interoperability demands of future conflicts.

- **Undertake an honest assessment of the current state.** This should include not just purely military aspects, such as the percentage of aircraft with tactical data links, but also more amorphous cultural aspects such as connections with industry and processes for rapidly sharing information with other parts of government. Part of such an assessment will also require determining what level of interoperability is necessary for a given defense challenge.

- **Prioritize investments and organizational changes.** With a clear picture of the current and desired states of interoperability, defense leaders should prioritize the changes needed to get from where they are to where they need to be.

For specific examples of how militaries should or are adapting to the challenges of the future of conflict, see the Future of Warfighting collection for additional research.

The future of conflict is unknowable. But for each of the major challenges we have identified, interoperability—within militaries, within governments, with industry and other nations—is a key source of strategic advantage. By cultivating interoperability today, defense organizations can be ready for the future, whatever it may bring.

Endnotes

1. Ministry of Defence and Ben Wallace, “UK and France able to deploy a 10,000 strong joint military force in response to shared threats,” Gov.UK, November 2, 2020.
2. Christopher G. Pernin et al., *Targeted interoperability*, RAND Corporation, 2019.
3. The review of publicly available defense strategy documents included Australia, Canada, Germany, Denmark, France, Israel, India, South Korea, the Netherlands, New Zealand, the United Kingdom, and the United States. Other defense priorities were listed in the documents but among the spectrum of challenges listed near-peer/ peer warfare, gray zone threats particularly from technology, limited-scale warfare, and defending the rules-based order were the most consistent and discussed as the most consequential during research workshops with all 12 participating countries.
4. Congressional Research Service, *SolarWinds attack—no easy fix*, January 6, 2021.
5. United Nations Association of Australia, *The United Nations and the rules-based international order*, July 2015.
6. Max Smeets, “U.S. cyber strategy of persistent engagement & defend forward: Implications for the alliance and intelligence collection,” *Intelligence and National Security 35*, no. 3 (2020): 444–53.
7. Department of the Army, *Digital liaison detachment*, December 2017; RAND Corporation, *Chasing multinational interoperability*, 2020.
8. RAND Corporation, *Chasing multinational interoperability*; RAND Corporation, *Targeted interoperability*, 2019.
9. Robert O. Work, *A joint warfighting concept for systems warfare*, Center for a New American Security, December 17, 2020.
10. Theresa Hitchens, “The joint warfighting concept failed, until it focused on space and cyber,” Breaking Defense, July 26, 2021.
11. Constanze Stelzenmüller, “The impact of Russian interference on Germany’s 2017 elections,” Brookings, June 28, 2017.
12. Sandra Erwin, “STRATCOM chief Hyten: ‘I will not support buying big satellites that make juicy targets’,” *SpaceNews*, November 19, 2017.
13. George I. Seffers, “Fight SATCOM concept grows closer to reality,” *Signal*, May 1, 2020.
14. Vannevar Bush, *Pieces of the Action* (Morrow, 1970).
15. RAND Corporation, *Targeted interoperability*.
16. UMass Lowell, *The Battle of Megiddo and its result*, accessed August 12, 2021.
17. Seth Johnston, “NATO’s lessons from Afghanistan,” Belfer Center for Science and International Affairs, Harvard Kennedy School, 2019.
18. RAND Corporation, *Targeted interoperability*.
19. Rachel Ellehuus and Pierre Morcos, “Sticking together or drifting apart: The future of Franco-British Defense Cooperation,” Center for Strategic and International Studies, October 28, 2020.
20. RAND Corporation, *Targeted interoperability*.

Acknowledgments

The authors would like to thank the more than 60 Deloitte experts from around the globe who contributed to this project of which **Kelly Woods** and **Chris Ducas** were particularly instrumental. They'd also like to thank the talented Deloitte Insights staff, and specifically, **Ramani Moses** and **Sayanika Bordoloi**, for their support in producing this research.

About the Deloitte Center for Government Insights

The Deloitte Center for Government Insights shares inspiring stories of government innovation, looking at what's behind the adoption of new technologies and management practices. We produce cutting-edge research that guides public officials without burying them in jargon and minutiae, crystalizing essential insights in an easy-to-absorb format. Through research, forums, and immersive workshops, our goal is to provide public officials, policy professionals, and members of the media with fresh insights that advance an understanding of what is possible in government transformation.

Defense, Security & Justice services

In addition to serving valued clients across the US Departments of Defense and Veterans Affairs, Deloitte is committed to supporting the military family ecosystem by developing capabilities and solutions that enhance quality of life for the military, veterans, their families, caregivers, and survivors, from child development to spouse employment to casualty and memorial affairs. Deloitte acknowledges both the moral imperative and national security value in supporting the military community as well as the sacrifices that come with service. To learn more, visit Deloitte.com.

Contact us

Our insights can help you take advantage of change. If you're looking for fresh ideas to address your challenges, we should talk.

Practice leadership

Roger Hill
Principal | Deloitte Risk and Financial Advisory
+1 571 882 6040 | roghill@deloitte.com

Roger Hill is a principal in Deloitte & Touche LLP's Government & Public Services practice. Hill serves as the Deloitte Risk & Financial Advisory lead for the defense, security and justice (DS&J) sector.

Darren Hawco
Vice admiral (retired) | Executive advisor | Consulting
+1 613 751 5281 | dhawco@deloitte.ca

Darren Hawco is an executive adviser in Deloitte's Consulting practice. He is a retired senior military officer and executive with extensive public, military, and allied services experience.

The Deloitte Center for Government Insights

Adam Routh
DS&J research lead | The Deloitte Center for Government Insights | Deloitte Services LP
+1 202 220 2633 | adrouth@deloitte.com

Adam Routh is a research manager with the Deloitte Center for Government Insights and a PhD candidate in the Defence Studies Department at King's College London. He leads research on defense and security topics.

Joe Mariani
DS&J research lead | The Deloitte Center for Government Insights
+1 312 486 2150 | jmariani@deloitte.com

Joe Mariani is a research senior manager with the Deloitte Center for Government Insights, where his research focuses on innovation and technology adoption by both commercial businesses and national security organizations.

Deloitte.
Insights

Sign up for Deloitte Insights updates at www.deloitte.com/insights.

Follow @DeloitteInsight

Deloitte Insights contributors
Editorial: Ramani Moses, Sayanika Bordoloi, Prodyut Borah, Nairita Gangopadhyay, and Ribhu Ranjan
Creative: Sonya Vasilieff and Rishwa Amarnath
Audience development: Maria Martin Cirujano
Cover artwork: Nazario Graziano

About Deloitte Insights

Deloitte Insights publishes original articles, reports and periodicals that provide insights for businesses, the public sector and NGOs. Our goal is to draw upon research and experience from throughout our professional services organization, and that of coauthors in academia and business, to advance the conversation on a broad spectrum of topics of interest to executives and government leaders.

Deloitte Insights is an imprint of Deloitte Development LLC.

About this publication

This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or its and their affiliates are, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your finances or your business. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

None of Deloitte Touche Tohmatsu Limited, its member firms, or its and their respective affiliates shall be responsible for any loss whatsoever sustained by any person who relies on this publication.

About Deloitte

Deloitte refers to one or more of Deloitte T ouche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.