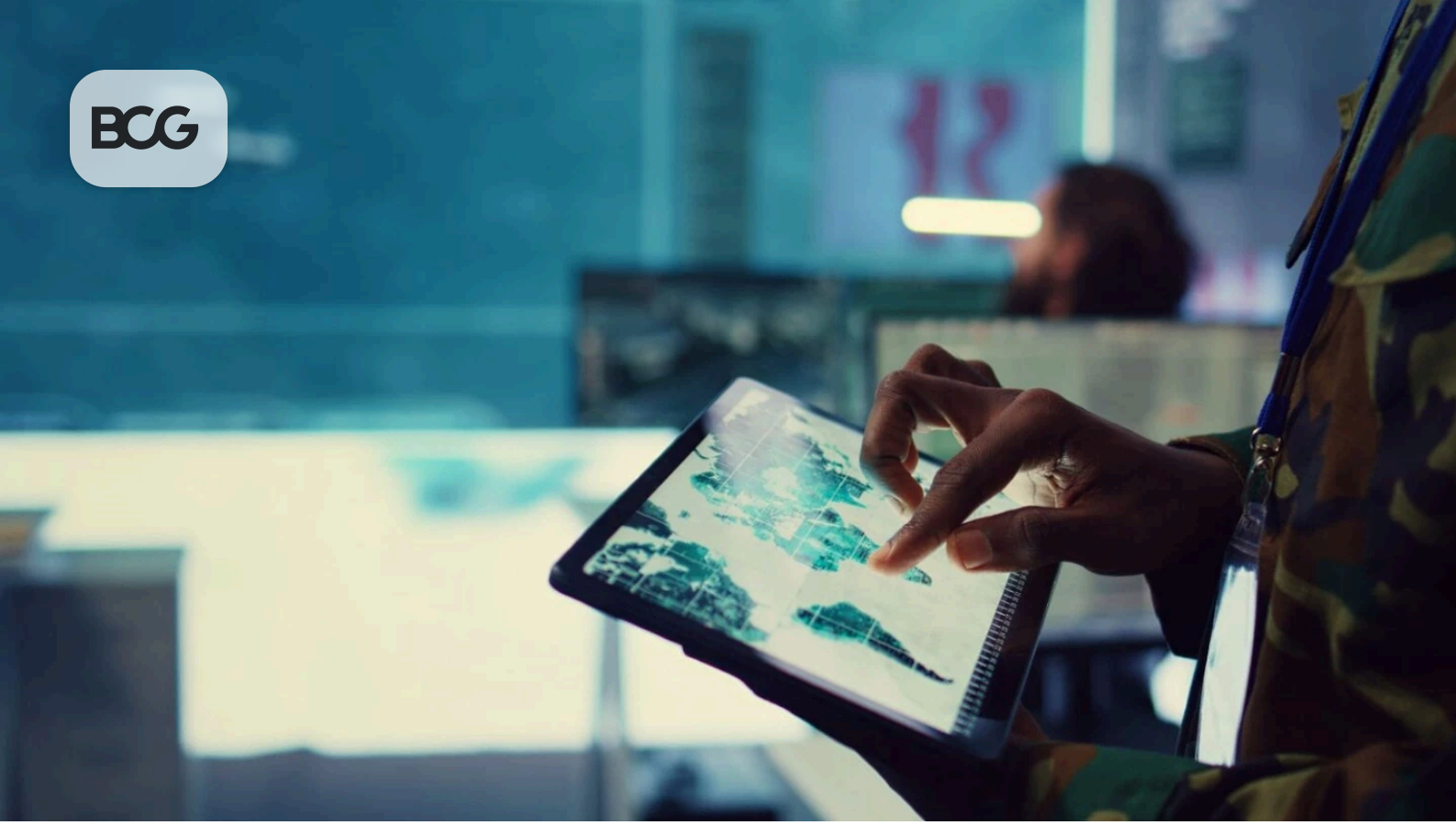

PUBLIC SECTOR

How Defense Organizations Can Build Digital and AI Skills at Scale

By Patrick Erker, Kathryn Finnis, Ben Shuttleworth, Louis Watt, and Nadjia Yousif

ARTICLE OCTOBER 21, 2025 8 MIN READ

Defense organizations are making massive investments in digital technology and AI; at the same time, making a similar investment in building skills among their armed forces and civil servants to use these technologies could be a wise move.

In the past, defense organizations dominated through strength, with large forces, advanced platforms, and expansive infrastructure. Today, the competitive edge in national security comes from digital technology and AI. Capabilities—including autonomy, automation, and secure connectivity—determine how fast a force can act, how well it can coordinate, and how successfully it can outmaneuver an adversary in complex, digitally contested environments.

But digital tools are only as effective as the people using them. To capitalize on their investments, defense organizations can train their teams in the digital and AI skills they need to succeed.

The Skills Gap in Defense Is Growing

Many public- and private-sector organizations are well aware of the skills gap. In fact, 90% of government agencies already identify AI and data analytics skills as high-priority skills. By 2030, across industries, ensuring that talent has these skills is expected to become the most rapidly rising priority.

But the skills gap is growing faster than are most organizations' capabilities to keep up. Globally, nearly 40% of today's core skills are anticipated to become obsolete within five years. In many tech roles, the half-life of a skill has already shrunk to less than two-and-a half years.

> Nearly 40% of today's core skills are anticipated to become obsolete within five years.

These issues are compounded at defense ministries, where advances in automation and AI are reshaping how missions are planned, executed, and adapted in real time. Secure digital connectivity has become the backbone of coordination—within forces, across agencies, and among allies—and data is as important as platforms. Capabilities, including data analytics, automation, and connectivity, are no longer support functions—they are frontline skills. The armed forces have a clear need to get these elements right, and they face a clear risk in implementing them incorrectly without the right skills in place.

Digital as a Force Multiplier

In many cases, defense organizations can generate significant productivity gains from baseline digital skills that are widely used in the private sector. (See the sidebar “Three Digital Productivity Skills from the Business World That Forces Can Apply.”) Yet the real advances come from defense-specific digital applications, including the increased use of AI. Consider the following roles and how their typical job skills are likely to change from 2020 to 2030.

— Three Digital Productivity Skills from the Business World That Forces Can Apply

Digital applications for defense are advancing rapidly, but organizations can apply commercial off-the-shelf productivity tools as well, leading to improved productivity.

- Some organizations still share documents by attaching files to emails or attaching notes to documents. Upgrading to cloud-based file sharing allows easier collaboration on live documents, reduces the load on servers, eliminates version-control issues, and saves hours of administrative time for teams.
- At some defense ministries, time-pressed service members and support staff haven’t received training on common programs like Microsoft Outlook. A lack of understanding about how to use the calendar and manage their inbox has led to missed tasks and project delays. Relatively straightforward training can help people use smarter functions, including through AI copilots, often reducing by half the amount of time spent on email in a typical day.
- Dedicated cyber training can help individuals identify vulnerabilities to external threats, including in their personal life, and give them practical guidance on avoiding security breaches and responding quickly when incidents do occur.

Intelligence Officer. In 2020, intelligence officers still consolidated and analyzed data manually using spreadsheets, and they spent much of their time developing briefing documents using programs like Microsoft Word and PowerPoint. By 2030, we expect that these officers will use AI-enabled solutions to model and identify emerging threats. They are likely to capitalize on full-spectrum, open-source intelligence and integrate intelligence, surveillance, and reconnaissance information from operational forces in real time. GenAI is expected to automatically generate briefing documents for people to review and validate the findings.

Logistics Officer. Five years ago, a logistics officer's responsibilities typically involved manually tracking shipments with barcode scanners, maintaining paper-based logs, and relying on experience to make judgment calls about routing decisions for materiel, fuel, and other resources needed in the field. Five years from now, we expect logistics officers will be able to use predictive, AI-based supply chain analytics and automated convoy-routing tools. They are likely to run simulations to model the impact of changing ground conditions on supply levels and generate updated recommendations in seconds. Life cycle tracking solutions are expected to give them the current status of every asset in the force, including projected service life and the next maintenance activity.

Communications Officer. In 2020, these officers configured satellite communications systems, oversaw radio networks, and addressed problems by troubleshooting hardware. By 2030, cross-domain data integration is expected to be the norm, primarily through AI-enabled solutions. Communications leaders are likely to implement zero-trust architectures to improve cyber defenses and run network diagnostics that not only can spot issues but also can anticipate them.

Six Steps for Upskilling in Defense

Building digital literacy at scale doesn't require a wholesale reinvention but rather focused, deliberate action that aligns people, technology, and mission outcomes in a coherent way. By grounding their efforts in a structured and strategic approach, defense organizations can begin to close the capabilities gap and continue to position their people for mission success.

> Closing the capabilities gap requires deliberate action that aligns people, technology, and mission outcomes.

Our experience points to six interconnected steps that help build digital and AI literacy at scale. Notably, these are not one-and-done measures; rather, they are part of an iterative loop that can help organizations when applied repeatedly, and rapidly, to keep pace with changing digital technology.

Assess the current skills baseline. The first step is to establish a clear picture of current digital and AI skills—across roles, functions, and units—with a primary focus on identifying critical gaps. Each organization is at a different starting point and requires a clear understanding of its unique situation and context in order to design an effective solution.

Set clear, mission-aligned objectives. Whether the focus is improved decision speed, stronger coordination across forces, or enhanced resilience, being clear about the problem that needs solving is important. Digital and AI training efforts become meaningful when they're linked directly to operational, mission-relevant objectives and tracked using quantifiable metrics.

Define digital and AI competencies. Digital competency means different things in different contexts. The digital requirements of, say, a logistics officer will differ significantly from those of an intelligence analyst, and effective programs are designed to accommodate that variety without becoming fragmented. Organizations can define the digital competencies they need—ranging from basic fluency to advanced AI—by role.

Segment training approaches by role and need. Treating the workforce as a single audience limits both relevance and scalability. Segmenting personnel into profiles—or personas—enables tailored learning journeys that can be deployed at scale, while still reflecting the specific operational realities of each group.

Design practical, targeted learning journeys. Learning is most effective when it reflects how work is actually done. A blend of personalized delivery methods—self-guided, immersive, and applied—allows people to integrate training into existing workflows. This approach transforms learning from an occasional intervention into a continuous process of professional development and adaptation.

Moreover, different modalities are more relevant for people at different seniority levels. For example, a junior intelligence analyst may start with a high baseline of digital skills from her personal life, and she may prefer online, gamification-oriented training offered through asynchronous modules. Conversely, senior leaders will likely require more live sessions, with highly targeted scope to fit in among their other priorities.

Monitor progress and continuously adapt. Digital and AI capabilities will continue to change in line with evolving technology, threat environments, and mission requirements. Leading organizations embed mechanisms for measurement, feedback, evaluation, and iteration, so that learning systems can adapt and stay relevant.

Digital and AI mastery is no longer a peripheral advantage—it is a defining factor in operational success and strategic resilience. Defense ministries have invested in digital tools and AI, but without the right investment in skills training, the gap between potential and performance will only grow wider—placing missions, alliances, and national security at risk.

The challenge is significant, but so is the opportunity. With a focused, structured, and mission-aligned approach, defense organizations can close the gap in digital and AI skills and build a workforce that is adaptive, interoperable, and digitally fluent by design.

Authors

Patrick Erker

Associate Director, Upskilling
Los Angeles

Kathryn Finnis

Partner
London

Ben Shuttleworth

Managing Director & Partner
London

Louis Watt

Managing Director & Partner
London

Nadjia Yousif

Managing Director & Partner, Chief Diversity Officer
London

ABOUT BOSTON CONSULTING GROUP

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

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