



The next major Defense challenge

Recruiting intelligent automation talent



To win the data war, defense forces look to leverage specialized skills in digital automation and artificial intelligence.

Organizations of all kinds are examining ways to use digital automation, under names including artificial intelligence, machine learning or bots. But defense agencies have among the strongest motivations to adopt this group of technologies, known collectively as intelligent automation, given the ever-increasing volumes of data they need to analyze accurately, safely and quickly, in the interests of national security.

"Intelligent automation is absolutely essential for the military," says Ian McDonald, Director of Technology Enablement in Defense and National Security, KPMG in Australia. "They cannot operate the capabilities they currently have to their full potential without it."

Take ballistic missile defense, a vital part of many countries' military activity. As many as a dozen satellite and sensor systems may be used in detecting hostile missile launches, with a further dozen systems involved in destroying such missiles. A defense agency could have just 8–10 minutes to decide whether a launch represents a threat, share findings with allies and decide what to do. The use of countermeasures has to happen quickly, given that missiles could impact 16 minutes after launch.

"At the moment, there are humans in the loop between those systems," says McDonald. "You cannot respond within 16 minutes, unless you are already in a state of high alert." Intelligent automation can rapidly integrate all the data from satellites and sensors and present findings, allowing personnel to decide what action to take.

Finding the right level of automation

Intelligent automation, which David Kirk, Managing Director of Advisory for KPMG in the US, defines as "the automation of mission delivery and business processes by leveraging digital technologies to support tasks undertaken by knowledge workers,"¹ can be split into three levels of sophistication. The first level, robotic process automation, can make routine tasks more efficient in areas including finance, accounting, human resources and compliance. KPMG firms have worked with defense clients to automate payments between agencies, including securely accessing systems and obtaining and processing the data required.

The second level of intelligent automation, learning cognitive automation, often involves the use of natural language processing and chat-bots. Kirke Everson, Managing Director of the Intelligent Automation Group at KPMG in the US, says this has potential to automate routine communication such as helpdesk ticketing and directory inquiries. "Chatbots can understand sentiment and intent, they take care of multi-thread questions depending on the datasets plugged into them and they tend to learn over time based on interactions with humans," he says.

'Virtual agents' that use multiple channels including mobile and desktop computers, telephone and voice-activated speakers, are already used by some companies and civilian government organizations. They could allow military personnel to get answers to straightforward questions on travel or housing, pulling together data from

¹ KPMG LLP, "Demystifying Intelligent Automation: The layman's guide to the spectrum of robotics and automation in government" (June 2016).




different agencies, leaving humans in call centers to handle more complex queries. “It’s moving from a user interface to a conversational interface,” says Payam Mousavi, Director of Public Sector Advisory Services for KPMG in the US. “It makes accessing that information a lot easier and faster.”

The third and highest level of intelligent automation, reasoning cognitive automation, is able to derive insights from large amounts of data, including unstructured material such as written text, audio and video. In administrative work this has potential in recruitment and training, where existing staff records could be used to propose which specialisms a new recruit could be trained in.

But there is stronger potential for reasoning cognitive automation in improving battlefield decision-making. Currently, when a scout tank at the front of a group crossing hostile territory is running low on shells or fuel, it requires radio communication with the group commander to order another tank to take over the lead role. However, this process could be automated by analyzing data generated by the tanks. “What you can do is speed everything up on the battlefield,” says Ian McDonald.

Integrating all the data from an area into a battle management system can improve safety, by accurately keeping track of allied forces and friendly non-military personnel such as aid workers. “Bringing all that data together is where intelligent automation comes in,” McDonald says, given the large quantities that need to be integrated quickly. This is particularly important for the most advanced drones, which can collect terabytes of data — including visual, radio and radar — in missions lasting more than 24 hours. Intelligent automation can allow this data to be analyzed in near real-time, highlighting what looks important within minutes rather than days later.

Levels of intelligent automation

1		Robotic process automation E.g.: Automating routine payments between defense agencies
2		Learning cognitive automation E.g.: Answering straightforward queries from personnel on travel or housing
3		Reasoning cognitive automation E.g.: Analyzing intelligence data from drones in real-time or near real-time

“It’s important you have someone with a data science background as well as people with on-the-ground expertise.”

Military training for systems

With higher levels of intelligent automation, systems need to be trained with data that includes inputs and the conclusions drawn, allowing them to model which inputs should lead to which conclusions. This requires reliable sets of training data, some of which can be gathered from the routine use of military aircraft, ships and land vehicles. It can also be generated by digital simulations, war-gaming and physical military exercises, including how personnel behave in them.

Data used to train an intelligent automation system has to be accurate and unbiased for its conclusions to be useful, and ensuring this is the case requires the right skills. “It’s important you have someone with a data science background,” says Kirke Everson, as well as involving people with on-the-ground expertise: “Someone who understands the use-cases and objectives of what you are trying to do.”

Payam Mousavi adds that a range of expertise helps to minimize bias: “There is some governance, some control and an approval process for what learning goes into the system — and multiple experts training the machine, rather than one person.”

Many defense agencies lack these at present, as militaries have tended to attract people who are good at operating machines and vehicles rather than computers, while defense-minded people with IT skills are often sucked into cybersecurity work. “There’s a global shortage,” says Ian McDonald.

Kirke Everson adds that it is vital for intelligent automation projects to use people with a strong understanding of the technology: “That’s where we’re helping clients the most, to say you need a business architect, a robot process automation developer and three domain experts to implement this solution, and we can help you do that.” KPMG in the US recruits graduates of university courses that include machine learning and artificial intelligence, to strengthen its technical resources.

Intelligent automation projects also need strong cybersecurity, and defense agencies set high requirements, including controls on authentication and segmenting of duties. Intelligent automation techniques can themselves be used in building stronger cybersecurity, by analyzing data on previous attacks for patterns.



Rise of the humans

As the need for skilled humans in its development suggests, intelligent automation is less about raising a robot army and more about making defense personnel more effective. For an officer in the field this can mean less time spent on routine administration and more on mission-critical work. “It can provide a force multiplier,” says Everson.

Ian McDonald says the number of unmanned vehicles is expected to increase, including driverless tanks and fighter aircraft, as this will speed decision-making, reduce costs and remove personnel from harm’s way. But he adds: “You won’t ever remove all the humans — you can’t.” Indeed, defense agencies are likely to create new roles for people who can monitor and understand automated systems, to determine they run smoothly and safely.

“Agencies feel much more comfortable in having a human in the loop,” adds Kirke Everson. “You still have a human saying I agree with this, or I don’t agree with this.”

Intelligent automation will involve significant changes in the way defense agencies work, and it can make sense to start with pilot projects. Everson recommends building a business case for such change through small proof of concepts that can show a good return on investment. In the US, the flexible and quick Other Transaction Authority (OTA) process designed for prototyping can be appropriate for these. It can make sense to start with projects that are trained on structured data, such as that held within databases or spreadsheets, as they are easier to evaluate.

Simulations, war-gaming and physical military exercises provide a good place to trial intelligent automation, as well as gathering data for it: “Build tomorrow’s battlefields, tactics and strategies, and prove it that way,” McDonald says. If an intelligent automation system can save the price — both financial and human — of a single aircraft or ship, it will easily justify its cost.

Further reading

David Kirk, *Demystifying intelligent automation: the layman's guide to the spectrum of robotics and automation in government*, May 2017. Available from <https://www.kpmg-institutes.com/content/dam/kpmg/governmentinstitute/pdf/2017/demystify-intelligent-automation.pdf>

Martin Sokalski and Kelly Combs, *Intelligent automation takes flight: risk and governance will help you safely land your automation goal*, November 2017. Available from <https://advisory.kpmg.us/content/dam/kpmg-advisory/risk-consulting/pdfs/2017/11/intelligent-automation-takes-flight.pdf>

Rise of the humans: the integration of digital and human labor, November 2016. Available from <https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2016/11/rise-of-the-humans.pdf>

About the contributors



Kirke Everson

KPMG in the US

T: +1 703 286 8106

E: keverson@kpmg.com

Kirke Everson is a managing director in KPMG's Federal Advisory practice based in McLean, VA, whose consulting experience focuses on technology enablement, program management, process improvement, cyber security, risk management, and financial management. He currently serves as the Government lead for Intelligent Automation for KPMG in the US. Kirke has extensive experience in leading large programs supporting technology enablement, information systems security, information technology risk management, business process reengineering and financial management in the Federal government.

Kirke is a Certified Information Systems Security Professional, Certified Information Systems Auditor, Certified in Risk and Information Systems Controls, Certified in the Governance of Enterprise IT, a Project Management Professional and a Certified Government Financial Manager. Kirke is a member of the Intelligence and National Security Alliance, Information Systems Audit and Control Association, the International Information Systems Security Certification Consortium, Project Management Institute and the Association of Government Accountants. Kirke was also awarded the National Intelligence Meritorious Unit Citation in support of efforts to streamline and improve the management of the National Intelligence Program.



Ian McDonald

KPMG in Australia

T: +61 2 6248 1351

E: imcdonald@kpmg.com.au

Ian McDonald is an Aerospace and Defense military logistics and IT system specialist with over 43 years' experience in the global military logistics and IT sector. Ian has operational experience on Mirage, F/A18 and F111 weapons systems with Engineering and Master's Degrees in design and systems engineering at senior design approval authority level. His experience covers the aviation spectrum of operations, engineering, maintenance, logistics and IT programs including PD and strategic consultant roles for several of the largest global military organizations.

Ian currently provides strategic IT and systems consulting services at CIO/J4/J6 level for requirements and system capability outcome determination, implementation requirements, cyber security requirements and change management. He currently consults for a number of large militaries and Defense Industry vendors on enterprise IT systems and Cyber Security requirements as a global systems design and implementation specialist with over 4 decades experience in end user requirement, systems requirement and design, implementation and change management.



Payam Mousavi

KPMG in the US

T: +1 213 955 8714

E: pmousavi@kpmg.com

Payam Mousavi is a PMP Certified Director in KPMG's Public Sector Advisory Services practice with experience covering all phases of initiation, planning, design, development, and deployment of solutions to leading global companies. Additionally, Payam is a leader in KPMG's Intelligent Automation practice helping federal, state and local governments implement a number of different automation and cognitive solutions.

Payam is skilled in providing leadership, vision, and management to project teams in helping them tackle complex challenges and has considerable experience implementing large-scale IT systems as a Project Manager and/or Solution Architect. He possesses many years of Public Sector consulting experience with the state & local government agencies in both the US and Canada. He has also worked in private sector consulting completing projects in insurance, high technology, financial services, telecommunications, and sales in North America, Europe and Asia.

[kpmg.com](https://www.kpmg.com)

[kpmg.com/socialmedia](https://www.kpmg.com/socialmedia)



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

© 2018 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with 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. All rights reserved.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.

Designed by Evalueserve.

Publication name: The next major Defense challenge: Recruiting intelligent automation talent.

Publication number: 135343-G. Publication date: April 2018