Deloitte.

# The Age of With™

The AI advantage in defence and security

# Introduction

A businessperson today can hardly open a magazine or sift through a Twitter feed without seeing the words: data, artificial intelligence, automation, IoT, bots, machines, and transformation. These words are connected to opportunity and the time to grasp it is now—we are at the turning point when everything changes. Forever.

To navigate the continually changing landscape of data, artificial intelligence (AI) becomes our roadmap. And how we start is by each of us initiating our own journey into the advancing world of technological growth.

This story can be summed up in a single word—"*with*."

What's happening around us—shared data, social engagement, digital assistants, cloud platforms, connected devices—is not about people versus machines. It's about human collaboration made greater with the machines we invent. It's a new age.

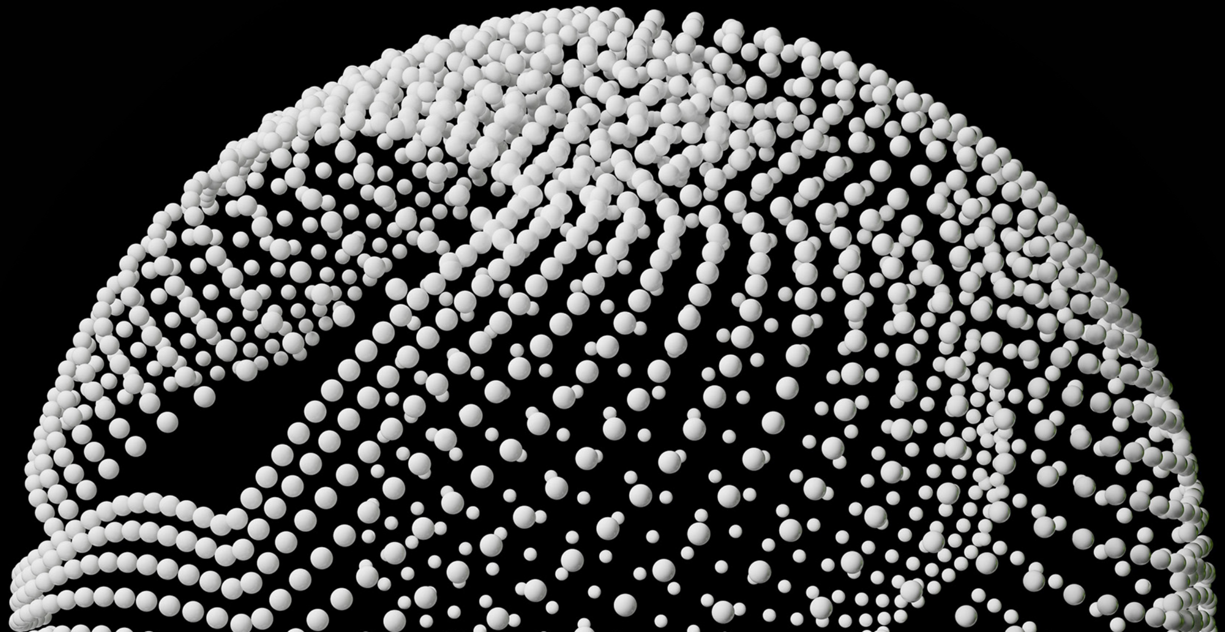
If we hope to perform, compete, and break through, we need to create a cognitive advantage by tapping the power of well-structured data with design thinking *with* analytics *with* machines.

While that feels a bit uncharted, it isn't. *With* has long been the great human advantage. We've sought it out. Benefitted from it. Built business models around it. In fact, *with* is at the core of many great inventions, from the municipality to the assembly line to the internet.

To succeed in the future, build your human intelligence where it is aided, enhanced, and augmented with AI. The potential is limitless.

# Disruption in the defence and security sector

The introduction of AI can bring profound changes to governments, including improving citizen experiences, driving economic prosperity, and enhancing public safety and security. Consequently, countries and governments around the world are embracing AI at a rapid pace.



## Trends affecting governments

From the rise of Siri and Alexa to personalized recommendations on Amazon and Netflix, and even instant orders for taxi and grocery services, we're all noticing how technology is changing our everyday lives in major ways. Citizens are becoming both more knowledgeable and more dependent on technology—as have their governments. Government leaders have noticed the benefits of adopting a digital-first mentality, as well as the imperative to do so. Both they and private-sector organizations are seeing opportunities to make optimal use of the mountains of digital information being generated by our increasing digital lives.

To respond to these trends in digital awareness, governments are more frequently engaging with the private sector to solve complex, digital-age problems. Partnerships are forming to further cutting-edge research and to provide the right solutions for unique problems.

To gain access to the right technology for these solutions, governments need to navigate a complicated procurement process. They're beginning to look at other types of budget models and agile procurement solutions that can accommodate pilot projects, are more transparent in the bidding process, and have a variety of service vendors.

These trends are also having a profound impact in defence and security, one of the government sectors that is most affected by digital disruption.

## Doing more with less

The defence and security industry is at the forefront of innovation and technology. Security organizations are one of the largest consumer-producers of data; they already own disproportionately more data than others due to the nature of the work. This industry faces a myriad of unique challenges in procuring, preparing, implementing, and scaling solutions. Given the amount of assets involved—including people, vehicles, equipment, and technology—an endeavour to build successful solutions can be an overwhelming task. Furthermore, governmental departments are being asked to do more with less as budgets come under intense scrutiny. To respond to growing global pressure to build more capabilities, government defence and security departments need to be more effective and efficient with existing programs and resources.

## The time for AI is now

AI has the potential to see beyond the horizon in ways that haven't been done before. Between the exponential growth in data and technical capabilities, the advancement of technology and processing power, and the investments being made by governments in AI research and development, the public sector is ready to implement new tools that will help make the decision-making cycle faster. Whether it be in the military, policing, or border security, these defence and security organizations need to be prepared on multiple fronts: to operationalize their data, to streamline existing functions, to implement new technology, to respond to ethical concerns, and to procure the necessary tools to accomplish their goals.

It's a double-edged sword: disruptive technology and digital capabilities present a multitude of opportunities to improve defence and security functions. It also presents a multitude of new ways for criminals and terrorists to advance their methods of operation. The capability of local and national security is shrinking against demand. The sophistication of threat actors in the world today is growing exponentially as information is traded on the dark web, crimes become harder to

### Opportunity spaces for AI in defence and security

Key areas where AI-enabled technology can be used to maximize assets, augment resources, and provide the most value in defence and security.

| | Detection | Planning | Field operations | Support functions |
|---|---|---|---|---|
| **Military** | Use AI-supported systems to collect and analyze surveillance data feeds. Use smart sensors to track and detect objects or personnel. | Use available data and machine-learning algorithms to better anticipate resourcing requirements and associated costs for missions and training exercises. | Provide real-time information and quick assessments to improve mission outcomes. Protect people, assets, and information. | Expedite procurement processes and manage vendor contracts. Provide intelligent budgeting solutions. Support HR functions for smarter recruiting, automated services, and payroll requests. |
| **Police** | Use AI algorithms and smart sensors to identify people objects in digital data and active policing to provide a more holistic understanding of crisis scenarios. | Use available data and machine-learning algorithms to better anticipate potential threats and deploy resources. | Use reason-based analysis and neural networks to manage the collection and interpretation of data related to ongoing investigations. | Expedite procurement processes and manage vendor contracts. Provide intelligent budgeting solutions. Support HR functions for smarter recruiting, automated services, and payroll requests. |
| **Border security** | Use AI algorithms and smart sensors to detect potentially dangerous people and objects at border crossings, customs checkpoints, and other ports of travel. | Use available data and machine-learning algorithms to better anticipate travel activity and potential threats, and deploy resources at security checkpoints. | Use AI-supported systems to analyze trends and patterns of behaviour in traveller data to better identify suspicious activity. | Expedite procurement processes and manage vendor contracts. Provide intelligent budgeting solutions. Support HR functions for smarter recruiting, automated services, and payroll requests. |

investigate, cyber creates new points of attack, and information is easily falsified and disseminated.

The world today is more complex than it's ever been. AI and information-processing tools will play an instrumental role in helping governments make the right decisions.

### Opportunities for AI in defence and security

The spectrum of AI opportunities available in the defence and security industry is massive. The proliferation of data being produced and collected provides a more holistic view into the current and future state of operations. Using AI to support the collection and collation of data enables organizations to sift through mountains of information, tease apart complex interactions, and capitalize on the results in analyses and predictive scenario-planning.[1] Machine-learning algorithms and complex neural networks provide real-time assessments to support critical field operations. Autonomous vehicles using AI not only provide life-saving activities, but can further protect human lives through remote operations. Intelligent automation can reduce the administrative burden present in many roles, particularly in back office operations where processes can be time-consuming. Most importantly, the collaboration of AI with humans provides the opportunity to remove extraneous, low-value-added activities that ultimately distract from the core mission, no matter what kind of operation—planning and preparing, serving in field operations, or supporting complex resourcing logistics.

This report explores the opportunities and potential of AI in defence and security, focusing on the fields of military, police, and border security operations, highlighting the key considerations for the use of AI and the infrastructure required to scale applications.

# New solutions *with* new approaches

# Military

From mission planning to sensor technology, drone surveillance to autonomous vehicles, military departments are looking for opportunities where AI can provide a critical advantage in operations and support functions.

## The opportunity

A massive amount of surveillance data is being captured. While only a small amount is pertinent to operations, one estimate found that the amount of data gathered by military drones and other types of surveillance technology alone rose by 1,600 percent between 2001 and 2011.[2] The question is, how do you sift through all this information to find what is actually usable? Integrating AI into the way satellite and drone surveillance feeds, collects, and interprets that data can provide a clearer understanding of a conflict or crisis dynamic,[3] using AI models and pattern analysis to determine activity that may not be perceived as a threat by a human observer. These datasets could encompass historical mission data, mapping and environmental factors, and on-the-ground human intelligence gathered by intelligence officers.

The use of this holistic dataset is critical in multiple applications in both the intelligence theatre of operations and military scenario-planning at all levels of command. In the intelligence theatre, for example, this holistic dataset can be used to help gather and analyze local community sentiment about military presence, such as by social-media scraping, and to develop strategies to combat misinformation campaigns and misconceptions. And AI can be used in military scenario-planning at all levels of command, from task-force commanders down to individual company and platoon levels, to determine the requirements for a mission. Enhancing the planning of battle procedure with AI ensures the most advantageous use of resources during a mission.

The collection and operationalization of data for military operations extends beyond core mission activity. The support services that the human resource function provides are unique to military organizations. HR is a rich landscape of opportunity to transform the soldier experience. Military recruiters need better strategies for hiring the right candidates. Statistics on how existing top performers were recruited, why they resigned after reaching certain milestones, and why the military retains certain roles are valuable are valuable datasets that can be used to determine strategies for targeting applicants who will be dedicated in the long term. Once in the military, HR supports soldiers' health and well-being. Analyzing data on common injuries and ailments, time spent on sick leave, the cost of care, statistics on mental health issues and more could provide valuable insight into developing a more human- centric approach to the care of personnel and their dependents.

## Unique challenges

Applying AI within the military comes with a unique set of challenges. Collecting mass amounts of data also means considering the quality of the data, where it is being stored, who has access, how it is classified, and simply getting it into one place so it can be used. Existing systems and technologies have inherent compatibility issues with the way data is captured and processed. As a result, AI implementation becomes difficult due to these technical infrastructure limitations.[4]

Furthermore, the military operates in a closed network that makes accessing information through new technologies more complicated. Potential AI vendors need to consider how to integrate with the existing network infrastructure in order to provide relevant information in real time.

The procurement process can also be a speed bump in securing new solutions in the military. The public sector typically relies on clearly defined requirements and scope, whereas AI solutions and new capabilities can be hard to define. Reviewing possible vendors can take a significant amount of time, often several months, and any change in leadership could potentially mean restarting the entire process altogether. To solve this, military are looking to create more agile procurement vehicles that secure a partner for multiple years to help develop pilot projects and use cases that create incremental value along their AI journey.

These types of solutions become even more important when looking to implement AI in military support functions, such as in finance or HR operations, where chatbots can provide quicker access to medical and benefits information, or intelligent automation could process payroll paperwork with greater speed and efficiency, ultimately working *with* government employees to refocus their attention on more high-value tasks. With the right processes in place, AI has the potential to transform both tactical military operations and the teams of people who work behind the scenes to support them.

# AI opportunities in military operations

### Intelligence *with* data

Integrate AI into the collection and interpretation of satellite and drone surveillance data feeds to provide a clearer picture of a conflict or crisis dynamic, considering historical mission data, environmental factors, and more. Use autonomous vehicles, such as submarines and land machines, enhanced with reinforcement learning algorithms to perform reconnaissance and discover targets.[5]

### Logistics and mission planning *with* purpose

Combine environmental, asset, and historical mission data to better predict mission scenarios to ensure resources are allocated advantageously, coordinating between multiple missions, operations, or task forces. Identify optimal areas for camps, and evacuation supply routes for both military and humanitarian efforts.

### Predictive asset maintenance *with* confidence

Use sensor technology and computer vision to detect flaws and system failures in equipment before they occur. Use deep learning and planning algorithms to determine maintenance schedules based on operating standards for various components, reducing accidents and unplanned delays. Consolidate and analyze real estate assets to create improved management and maintenance strategies.

### Enhanced operations *with* precision

Use sensor technology to track company movements and quickly identify unknown objects in the field, thereby better informing command decisions. Deploy autonomous vehicles to provide life-saving duties for wounded soldiers in the field.

## Electromagnetic spectrum operators *with* accuracy

Spectrum warfare is the military use of the electromagnetic spectrum (EMS) to locate parties, disrupt enemy communications, and blind their radars.[6] Operators of the EMS receive a multitude of signals on their dashboard, most of which are non-critical. It's their job to decipher the signals and determine what to act on. In the evolution of electronic warfare technology, AI can provide faster analysis of incoming data from sensors, identifying correlations between data points in real time. Working *with* AI to filter the noise coming in reduces the cognitive burden of the operators, allowing them to focus on the signals that matter.[7]

# Police

The public is distinctly aware of the behaviours and activities of police officers. Between bystander live streaming, heightened media attention, and constant interaction with citizens, police officers are some of the most highly scrutinized public servants.

## The opportunity

With all of the digital technology available in the palm of one's hand and the data it generates, there are some interesting opportunities to engage the public in positive ways and using this information to increase public safety. Police organizations are showing more interest in creating service portals that could serve a variety of purposes. They could, for example, provide a platform for the next generation of 911 correspondence, augmenting the role of 911 and police dispatchers, and allowing citizens to supply real-time updates in the form of texts, photos, and video, which could provide a huge amount of information on a public safety incident. Integrating AI into the platform would operationalize this data, sifting through what has been collected to paint a more accurate picture of the crisis. Providing 911 responders and dispatchers with the use of AI enables them to prioritize police activity more effectively by consolidating multiple sources of information about a single incident, providing relevant updates to constables in motion, and even coordinating with other emergency services or other agencies. Crowdsourcing exercises would be possible to support events, such as amber alerts, informing the population and engaging their support.

Changes are also happening in the ways in which police organizations collect, manage, and share their data. Police services are looking at using open data portals to push out previously restricted or controlled data into the public to consume and use in a variety of ways, providing the private sector with the opportunity to find insights and use cases for data operationalization and AI applications. Body-worn camera providers are moving toward capitalizing on this proliferation of data in the industry, changing their business models to offer data collection and management capabilities, a procurement option that appeals to organizations that have difficulty sourcing multiple vendors for data management.

## Unique challenges

With the increase in data opportunities available, there is also an increased amount of concern with how and when this information is being used. There's competing pressure to both use AI tools and technology for public safety and better outcomes, and to address potential bias and transparency in solutions, ensuring privacy and security measures are inherently built in. As they increase their use of technology, police officers and services are facing human rights violations and class action lawsuits that have led to stopping the use of software and tools. Concerns also arise in data privacy—lawsuits can and have been made against organizations that have collected a person's image for one investigation, and then used it again in another investigation. In this case, the personal data (image) was not being used for the original purpose for which it was collected. This calls into question body-worn camera footage, where an officer is walking through various environments collecting massive amounts of information, and what can actually be used due to personal data privacy considerations. There is an increased thirst for AI, but ethical concerns remain at the forefront of the conversation.

To combat these concerns, security elements must be built into AI solutions from the beginning; they cannot be a second thought. The focus should be on understanding the factors that led to a security event. Police organizations are ready to work *with* AI, but there is a natural tension between adopting this technology while ensuring the right governance and framework exist to avoid unintended outcomes. To support this, the European Union's General Data Protection Regulation includes a recital that indicates a person should have the right to not be subjected to a decision with legal implications based solely on automated processing.[8] This is why it is so important that AI and humans work together to achieve the best possible outcomes, ensuring there is no "black box" AI that cannot be explained. This human-*with*-machine partnership has a bright future, as substantial turnover at the leadership level in policing is bringing in individuals who are more tech-savvy and are familiar with technology as a disruptor.

Even so, establishing the right AI ethics framework that accounts for how the AI is being used, what it is used for, and how to address issues of inherent bias and transparency in algorithms is critical in the adoption of AI in policing.

# AI opportunities in policing

### Investigations *with* evidence

Use reason-based analysis and neural networks to better manage the collection and interpretation of data related to investigations, including the digitization of paper-based data, to find connections between pieces of evidence, processing media, and identifying criminal activity. Combine datasets from multiple emergency services to better inform investigations and police activity.

### Administration *with* understanding

Reduce the administrative burden on police officers by automating various elements of paperwork and legislative compliance. Enable smart search capabilities to quickly return search results and relevant corresponding files during the course of a charge on an individual. Support recruiting functions to target the right quality, diversity, and capabilities of talent, particularly in populations that historically distrust police services.

### Resource allocation *with* data

Use available data to better anticipate threats and scenarios to better deploy police resources in order to ensure community safety and supporting staff are utilized effectively.

### Policing *with* acumen

Use drone technology and image-recognition capabilities to locate missing persons, manage crime scenes, and support forensic investigations. Use smart sensors to listen for gunshots, identify flagged licence plates, and log locations while officers are on the road.[9] Crowdsource evidence-gathering for emergency events and analyze in real time, triaging relevant information accordingly.

## Police investigators *with* confidence

With the increase in use of video in various capacities, from CCTV footage to dash cams and body-worn cameras, constables and investigators are required to review what could be hours upon hours of video footage, looking for a relevant piece of information. Research shows, however, that after watching a video monitor for more than 20 minutes, people lose 95 percent of their ability to detect events.[9] Through the use of reason-based analysis and neural networks, AI can work *with* an investigator to:

- Designate a specific zone in a video feed to detect changes, such as the removal of items from a retail store
- Identify abnormal items or behaviour, such as a speeding car that drives onto a sidewalk or unaccompanied baggage in an airport
- Search for particular pieces of information, such as a specific make and model of a vehicle or a missing person's outfit

# Border security

In the United States, border security guards quit at double the rate of other types of law enforcement positions, with low morale and work conditions being cited as part of the problem.[10, 11] By augmenting the jobs of agents with AI, border security agencies could both increase the effectiveness and increase retention of valuable personnel.

## The opportunity

Integrating AI into the jobs of officers could provide much-needed support in the early detection of dangerous people, goods, and activity. Security staffing has a significant impact on the resources required to physically patrol border crossing areas. By employing the use of smart sensors coupled with integrated datasets on migration patterns, crossing activity, demographics, environmental data and more, AI could work with security agents to re-allocate or deploy personnel directly to areas of the border where they would be most effective.[12]

AI can also be used to enhance existing systems, such as x-ray scanners for luggage/package/parcel review. Using computer vision and machine learning algorithms, dangerous goods can be more accurately and consistently identified, reducing the amount of manual labour and possible human error involved in having border agents examine the scans.

There is so much data being tracked every day, but often its value cannot be unlocked simply because it doesn't sit in the same place. Integrating previously siloed datasets can reveal connections that a human would not be able to piece together–but AI could. AI-supported systems could collect traveller data associated with a particular person–identified biometrically to ensure their identity–who has been entering and exiting the country frequently, each time with a child that has a different name. This might not be flagged immediately to a border agent, but by tracking and analyzing data in near-real time, an AI-enabled system would flag this individual for further investigation by the border security guard as a risk for human trafficking.[10] AI-powered machine vision could also support this in-depth investigation by using infrared cameras and blood flow pattern recognition systems to recognize deception in an individual. Studies suggest humans are able to spot a lie about 54 percent of the time, whereas AI has an accuracy rate of over 80 percent.[10] Through machine learning and the integration of more and more data, these methods are continuing to be refined. Though research looks promising, the debate on the validity of lie detectors remains at the forefront of conversation around implementing this type of technology. Whether or not this will play a role in border security has yet to be determined, and as with other aspects of law enforcement, it includes a unique set of challenges to consider.

## Unique challenges

Using biometric technology and facial recognition software can provide many benefits, including improving passenger flows in airports and re-focusing security personnel to address only certain individuals.[13] What needs to be considered, however, is the inherent bias present in the algorithms used to train the models for this type of detection software. This is why it is so important to ensure that new data is consistently being used to train the models, improving the accuracy and reliability of the results. It is equally important to perform algorithmic risk assessments to ensure the recommendations being made do not reflect bias. Integrating AI into border security services has great potential for a higher level of consistency that would not be possible with human operators alone. The focus needs to be on ensuring the human operator remains the key decision-maker, contextualizing analyses and information in emotionally intelligent ways that a machine cannot.

> The focus needs to be on ensuring the human operator remains the key decision-maker, contextualizing analyses and information in emotionally intelligent ways that a machine cannot.

# AI opportunities in border security agencies

### Traveller identification *with* accuracy

Use AI to recognize patterns of behaviour in individual traveller data that could indicate suspicious activity and flag for officer review. Use biometric technology to accurately match travellers to their travel documents to improve flow of traffic at security checkpoints, flagging only certain individuals who present irregularities.[13]

### Surveillance *with* integrity

Combine migration pattern, demographics, environmental data, and border activity data to provide increased situational awareness along border crossings and effectively prepare and deploy security agents. Use smart sensors and image recognition to improve surveillance activities and object detection across large areas of border crossings to refocus security agents' efforts on responding to unauthorized crossings and other security breaches instead of conducting ad hoc patrols.[14]

### Data *with* purpose

Analyze trends in large-scale travel data to better allocate security resources.[15] Model the effects of legislation updates, such as immigration policy changes. Use AI-enabled systems to process immigration applications online to reduce manual workloads.

### Customs *with* confidence

Use computer vision technology to more effectively screen X-ray images of cargo and baggage to identify dangerous goods. Analyze metadata from shipments to track and identify smuggling scenarios and other illicit items.

## Customs agents *with* speed

Inspection checkpoints at border crossings can be tedious experiences for both customs agents and freight truck operators. Individual screening and manual inspections are time-consuming. Using facial and image recognition technology, truck operators and their vehicle licence plates could be scanned and pre-screened prior to entering the customs station to expedite this process and single out only operators that need further questioning by a customs agent. AI-enhanced X-ray scanning technology can provide safe and accurate identification of possible dangerous goods or abnormal loads that could be instances of smuggling. Finally, AI-enabled systems can quickly analyze cargo metadata to identify suspicious shipments that require detailed inspection. By enhancing the role of the customs agent *with* AI, agents are empowered with accurate information in a more timely manner.

# Scaling AI to achieve long-term success in defence and security

The more integrated human *with* machine teams are, the more capable the team is.

Integration of AI technology into an organization is not just about ensuring the technology is trusted and secure. It's about the strategy to ensure AI is adopted broadly, the processes that are in place to procure and govern solutions, the data that is unbiased, and the people who are ready to nurture and develop AI capabilities. Governments may be trending toward a more digital-first mindset, but to ensure this change provides the kinds of results leaders are looking for, a cultural change needs to happen in implementing the digital workforce. With the right change in management strategy, organizations across government bodies, including the military, police services, and border security agencies, can institutionalize AI solutions that are governed with the highest degree of accountability, explicability, and success. Being agile in the procurement process allows teams to start with small pilot projects that test solutions and provide the appropriate opportunities for onboarding and training–key elements in developing the synergies between humans and AI. By demonstrating measurable success with these pilot projects, the solutions can then be applied outside the original use cases, broadening the scope of the solution to impact other areas of the organization. Throughout this process, nothing remains more critical than the human operator in all stages of implementation.

### Scaling for long-term success

The adoption of AI in an organization requires a North Star vision for the implementation and use of AI. Ensuring that the solutions put in place provide tangible, continuous results requires a broader vision for what AI will be able to accomplish. By setting a precedent for the role of AI, the organization can then move forward with solutions that work toward achieving the vision, reusing tried and tested models for various applications across multiple departments where it makes sense.

**Strategy**
Develop a strategy to ensure AI is adopted broadly and provides measurable success to the organization.

**Process**
Ensure processes are in place to procure solutions and govern the ethical use of AI.

**Technology**
Procure technology solutions that are trusted and secure.

**Data**
Use data that is unbiased and can be used to inform algorithms.

**People**
Enable a workforce that can nurture and develop AI capabilities.

# Tomorrow: Ensuring humans are in the loop

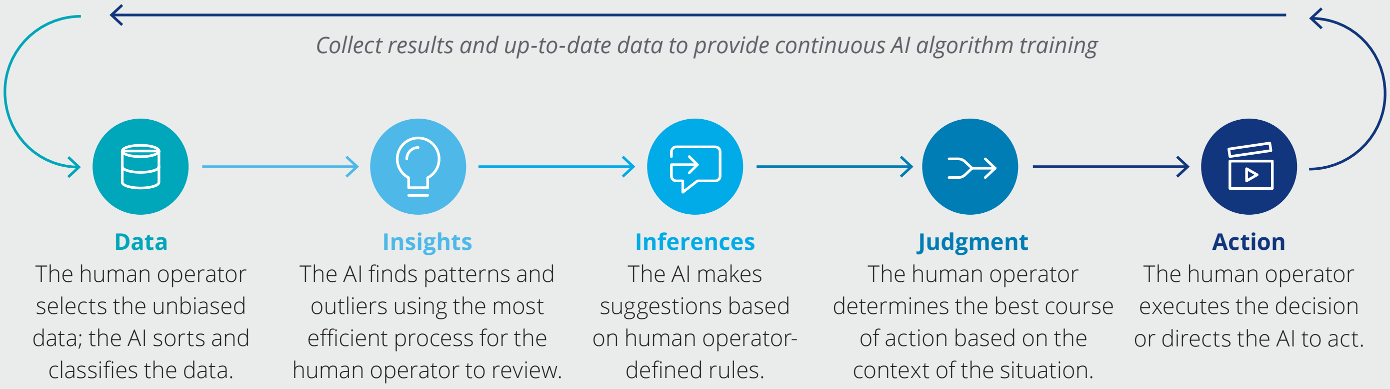
AI provides an incredible opportunity to enhance and augment the way we work.

Although the concept of intelligent automation has created concerns around job security for many people, the reality is that technology won't replace humans outright, as it historically hasn't. AI technology will substitute for specific assignments, allowing workers to refocus their time and energy on more complex reasoning tasks that require something AI doesn't have—emotional intelligence.[16] One of the biggest advantages of AI is to complete complex pattern analyses that humans cannot do due to the volumes of data involved. In defence and security, this means providing those who are in charge of protecting our countries and communities with critical information that helps them do their jobs more effectively.

Human operation and interference is of paramount concern in defence and security, where there is more at risk. The use of AI requires a much higher level of accountability and reliability than in other sectors given lives, expensive equipment, and the security of citizens are at stake. Operators must be able to explain why and how a model or algorithm arrived at a particular result, and must be the ultimate decision-makers. AI should not replace a human decision, but should re-direct resources to more value-add activities. Designing with humans at the centre and privacy from the beginning will safeguard AI solutions against more serious consequences.

Governments are poised to take immediate action on AI implementations that could drastically transform workflows and results. AI-enabled technology can be used to maximize and protect assets, augment resources, enhance data collection and interpretation, and reduce costs, fundamentally changing the industry. The time for AI truly is now.

**Humans in the loop**



*Collect results and up-to-date data to provide continuous AI algorithm training*

**Data**
The human operator selects the unbiased data; the AI sorts and classifies the data.

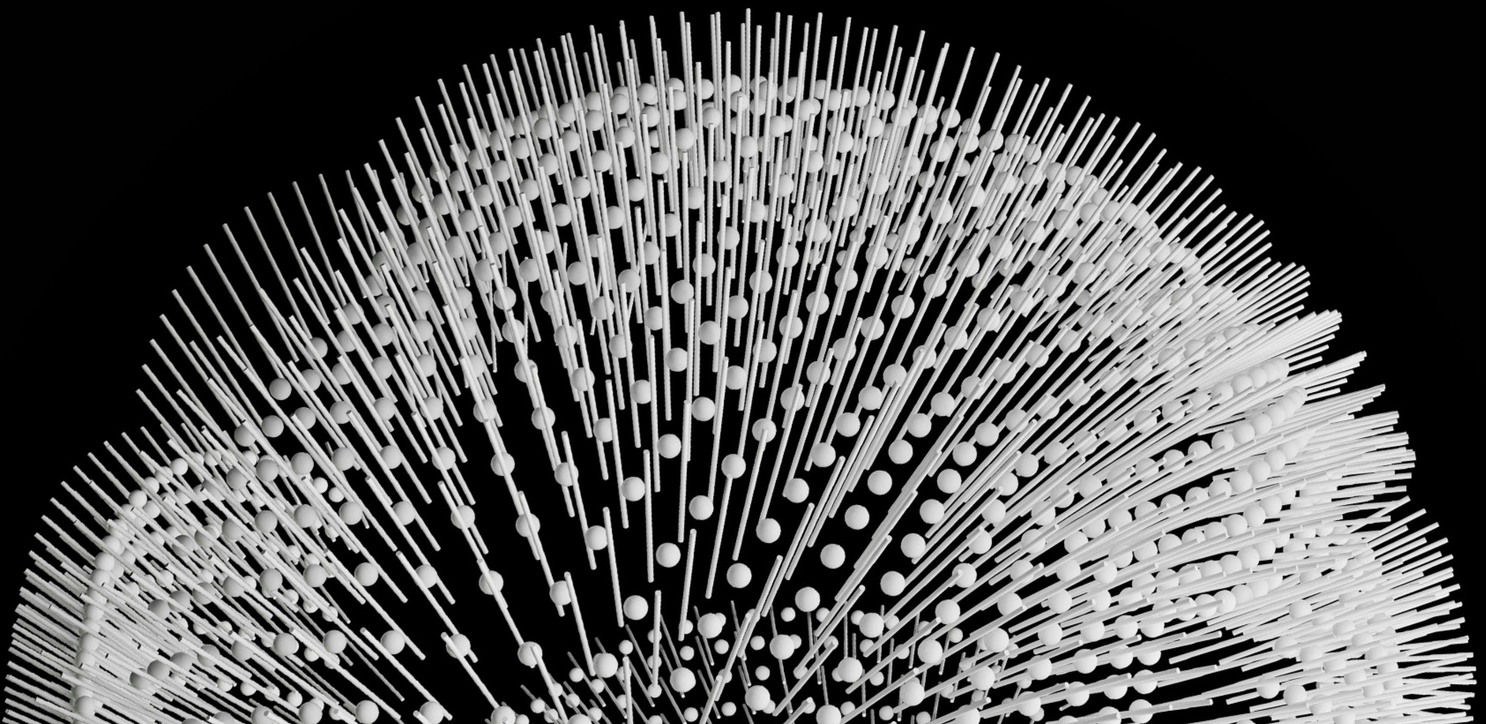
**Insights**
The AI finds patterns and outliers using the most efficient process for the human operator to review.

**Inferences**
The AI makes suggestions based on human operator-defined rules.

**Judgment**
The human operator determines the best course of action based on the context of the situation.

**Action**
The human operator executes the decision or directs the AI to act.

# Going deep *with* an AI lens



# Using computer vision to improve border security

## Increase accuracy and effectiveness of X-ray scanning

Reading images on a screen can be very labour-intensive. Border security workers are required to spend long hours reviewing X-ray scans of packages and cargo, looking for images of dangerous goods. After a time, it's easy to see how items can be missed or hard to interpret. With AI, this could change.

Using leading-edge image recognition technology, AI can provide security agents with the ability to more accurately detect dangerous goods. Using both open source libraries and cloud infrastructure, computer vision algorithms can be trained to detect specific objects, such as firearms or explosives, against background images to increase the accuracy of detection with minimal false alarm rates.

These models include:

### YOLO: You Only Look Once

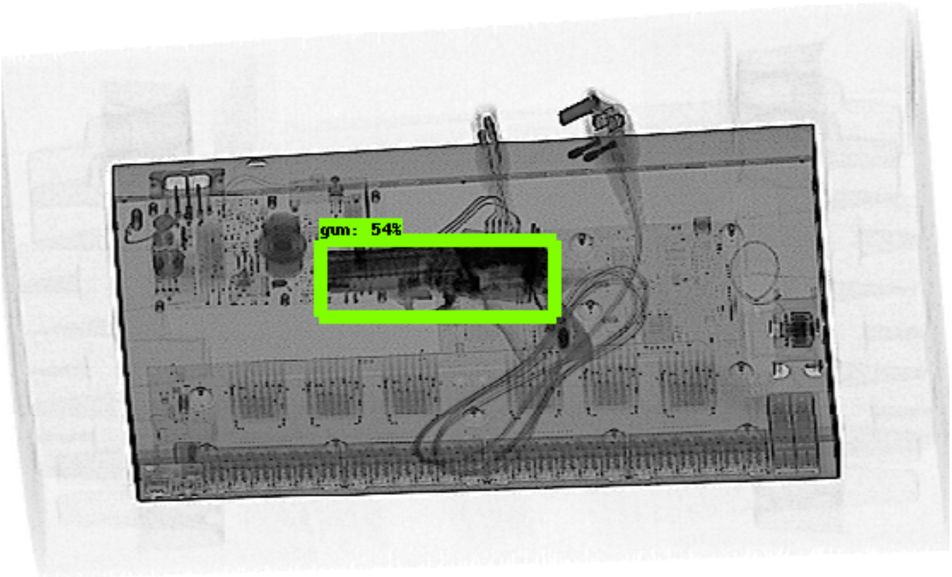
- Apply a single neural network to the full image, which divides the image into regions.
- Predict bounding boxes and probabilities for each region, weight bounding boxes by predicted probabilities, then threshold the detections by some value to only see high-scoring detections.

### SSD: Single Shot Detector

- A single deep neural network that combines regional proposals and feature extraction.
- Different bounding box predictions are achieved by each of the last few layers of the network responsible for predictions for progressively smaller bounding boxes and the final prediction is the union of all these predictions.

### RetinaNet

- A one-stage detector (e.g., YOLO, SSD) that has the performance of a two-stage detector (e.g., Faster-RCNN)
- An FPN (Feature Pyramid Network) with the cross-entropy loss replaced by Focal Loss



# Cybersecurity across the organization

### Using AI to protect against cybersecurity threats

IT and security professionals across government departments are required to protect their assets, ensuring that sensitive data is secure and the organization is not compromised. Security operations managers, for example, require on-demand reporting to assist in the management of security operations. IT administrators need to understand what assets are at the highest risk and what areas need to be patched first. Security analysts would be better supported with what-if analyses to predict and prevent future cyberattacks and activate security control functions.

A holistic, integrated platform enables various roles within the IT department to maintain better insight into cybersecurity health and can provide recommendations for remediation, preventing attacks before they occur.

By analyzing current asset connectivity, vulnerability, and risks to critical assets, AI can illustrate the current state of cybersecurity and demonstrate the path of least resistance an outside threat may take to gain access. Data inputs include the network and security architecture, configuration management base, endpoint and access logs, SIEM logs, and risk assessment results.

Data analytics, powered by advanced machine learning algorithms, can map threat scenarios, attack signatures, and vulnerabilities to drive a recommendation engine that provides multiple options for remediation, ensuring that emerging threats are flagged in near-real time.

Flag threats in near-real time by mapping threat scenarios, attack signatures, and vulnerabilities.

# Enabling support functions

### Procurement and vendor management

Across government organizations that span multiple departments and complexities, it can be extremely challenging to manage contracts, particularly as regulatory changes, rapid technological advances, and increased financial pressures force departments to do more with less. For defence and security, contracts are long-term, highly secure and confidential, and very complex.

By using an AI-enabled contract management solution, procurement and purchasing officers can maintain better visibility into contract populations, vendors, and procurement cycles. Using optical character recognition (OCR), paper contracts can be ingested digitally and reviewed, or the solution could support the request of a standard first draft of a document. Negotiations could take place all in the same system, using AI to flag any changes to the contract that fall outside the organization's risk appetite. Once executed, the purchasing officer then has a holistic view of all the vendor contracts in one place, enabling the officer to perform analytics on the data collected. This would provide insight into vendor management, showing which vendors negotiate the longest, what clauses are consistently reviewed (potentially flagging a requirement to update the standard first draft agreement), and how long various types of procurement contracts take to execute from start to finish, thereby providing officers with the ability to more efficiently plan in advance.

### Intelligent chatbots and automation

Support functions include employees who work in finance and human resources to carry out administrative activities. These areas are rich with opportunities to incorporate AI in ways that reduce non-core or time-consuming activities, allowing employees to spend more time on higher-value tasks that involve human judgment and reasoning.

One of the easiest solutions to implement is an intelligent chatbot. With the support of an automated service, a natural language processing-trained chatbot could respond to the hundreds of requests that an HR department would receive on a daily basis. A chatbot could be implemented from the beginning of the recruitment cycle with potential candidates to answer questions about the organization or role and collect feedback from candidates who drop out. For new and existing hires, an intelligent chatbot could answer frequently asked questions about onboarding, training, payroll, and even questions about healthcare benefits, coverage, and other departmental policies.

A Deloitte analysis found that at least 21 percent of US federal employee time was spent on non-core work, tasks that workers deemed unimportant to their job function. This type of work can include documentation and accessing information. While an intelligent chatbot can assist with information requests, intelligent automation can expedite manual data entry, filing paperwork, tracking information, scheduling, and reducing the backlog of tasks.

# Predictive asset maintenance

**Predicting failures before they happen**

Asset maintenance can be costly and can have a severe impact on missions and daily operations when unexpected failures happen. The integration of AI could provide critical predictive information that would help avoid operational disruptions and unnecessary downtime for machinery and other types of assets.

By combining existing sensors on assets like vehicles with AI software, the system can identify parts that require maintenance before they fail. Physical information from the asset is translated into a digital format that a machine can then analyze. This technology employs machine learning to analyze large amounts of data available in real time and provide key insights into the likelihood of part failure and longevity. Through the collection of more data over time, more valuable insights can be generated to identify correlations between events that could lead to breakdowns, ensuring that other similar assets are improved prior to critical failure and outdated equipment is replaced with more effective tools. Further, creating a connected network of machinery parts or asset components provides a greater scale of data that enables more accurate analyses. This comprehensive view of components yields a greater transparency for strategic decision-making and performance optimization.

Incorporating AI into the maintenance of assets and machinery provides valuable information that drives more effective maintenance strategies, maximizing resources and reducing overall spend on reactive activities.

Analyze large amounts of asset data and generate insights to create more effective and efficient asset maintenance strategies.

Photo: US Army, Spc. Dustin Biven

HUMAN
HUMAN
HUMAN
HUMAN
HUMAN
HUMAN
HUMAN
HUMAN
HUMAN
HUMAN

# Endnotes

1. “Military readiness through AI”, Deloitte Insights, accessed on May 9, 2019, https://www2.deloitte.com/insights/us/en/industry/public-sector/ai-military-readiness.html.
2. “In New Military, Data Overload Can Be Deadly”, The New York Times, accessed on May 9, 2019, https://www.nytimes.com/2011/01/17/technology/17brain.html.
3. “Artificial intelligence – what implications for EU security and defence?”, European Union Institute for Security Studies, accessed on May 31, 2019, https://www.iss.europa.eu/content/artificial-intelligence-%E2%80%93-what-implications-eu-security-and-defence.
4. Lindsey R. Sheppard. “Artificial Intelligence and National Security; The Importance of the AI Ecosystem.” Center for Strategic and International Studies: 21. Web. May 31, 2019.
5. “8 Key Military Applications for Artificial Intelligence in 2018”, Market Research.com, accessed on May 31, 2019, https://blog.marketresearch.com/8-key-military-applications-for-artificial-intelligence-in-2018.
6. “Today's battle for the electromagnetic spectrum”, Military and Aerospace Electronics, accessed on May 31, 2019, https://www.militaryaerospace.com/communications/article/16709112/todays-battle-for-the-electromagnetic-spectrum.
7. “AI Puts Army’s Electronic Warfare Missions in Focus”, MeriTalk, accessed on May 31, 2019, https://www.meritalk.com/articles/ai-puts-armys-electronic-warfare-missions-in-focus/.
8. “Recital 71 EU GDPR”, EU General Data Protection Regulation (EU-GDPR), accessed on May 31, 2019, http://www.privacy-regulation.eu/en/recital-71-GDPR.htm.
9. “How AI will transform digital evidence management”, PoliceOne.com, accessed on May 31, 2019, https://www.policeone.com/police-products/body-cameras/articles/476484006-How-AI-will-transform-digital-evidence-management/.
10. “The border guards you can’t win over with a smile”, BBC, accessed on May 31, 2019, http://www.bbc.com/future/story/20190416-the-ai-border-guards-you-cant-reason-with.
11. “Why More Border Patrol Agents Quit”, AFGE, accessed on May 31, 2019, https://www.afge.org/article/why-more-border-patrol-agents-quit/.
12. “Artificial Intelligence Helps Keep Borders Safe”, iHLS, accessed on May 31, 2019, https://i-hls.com/archives/88465.
13. “Artificial Intelligence serving border security”, IDEMIA, accessed on May 31, 2019, https://www.idemia.com/news/artificial-intelligence-serving-border-security-2018-11-16.
14. “Artificial Intelligence Helps Keep Borders Safe”, iHLS.
15. “The border guards you can’t win over with a smile”, BBC.
16. Lindsey R. Sheppard. “Artificial Intelligence and National Security; The Importance of the AI Ecosystem.” Center for Strategic and International Studies: 11. Web. May 31, 2019.

# Contacts

### Industry & Sector Leaders

**Beth McGrath**
Defence, Security & Justice Leader
Deloitte Global
bmcgrath@deloitte.com

**Ed Delaney**
HC Specialist Leader
Deloitte United States
edelaney@deloitte.com

**Scott Savage**
Public Sector Transformation Leader
Deloitte Canada
scsavage@deloitte.ca

### Global AI Leaders

**Jas Jaaj**
Partner, Omnia AI
Deloitte Canada
jjaaj@deloitte.ca

**Shelby Austin**
Managing Partner, Omnia AI
Deloitte Canada
shaustin@deloitte.ca

**Costi Perricos**
Global Analytics & Cognitive Leader
Deloitte United Kingdom
cperricos@deloitte.co.uk

**Nitin Mittal**
Principal, Analytics
Deloitte United States
nmittal@deloitte.com

### Contributors

**Nihar Dalmia**
Government & Public Services Omnia AI
Leader Deloitte Canada
nidalmia@deloitte.ca

**Andrew McHardy**
Senior Manager, Omnia AI
Deloitte Canada
amchardy@deloitte.ca

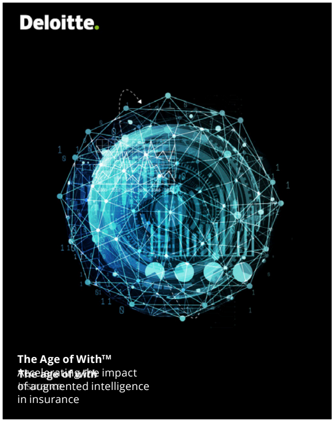
**Bilal Jaffery**
Senior Manager, Omnia AI
Deloitte Canada
bjaffery@deloitte.ca

**Jana Betik**
Senior Consultant, Omnia AI
Deloitte Canada
janabetik@deloitte.ca

## The Age of With™

Explore the series

**The Age of With™**
Leveraging AI to connect the retail enterprise of the future



**The Age of With™**
Accelerating the impact of augmented intelligence in insurance

**The Age of With™**
The future of energy, resources and industry with AI

Deloitte.