Is it Human? Our People. Its Purpose

OVERVIEW

This report investigates the use and purpose of Artificial Intelligence (AI) within the US Department of Defence ("Department"). The selection of the Department as a case study is because they have many areas that benefit from its use. Areas highly affected by matters such as regulations, societal impact, ethics and trust, with the overarching requirement to defend the nation through beneficial use of this technology.

The report considers AI in the case study by addressing four questions: (1) its current state in the Department; (2) benefits and drawbacks; (3) outline of risks and challenges with a few simple recommendations, and (4) briefly discusses a suitable framework for the Department to leverage for successful AI development. It then concludes with a summary outlining salient points of research for the case study.

Multiple resources for the research topic were consulted, such as the University of Essex's online library, Google Scholar, Scopus, Microsoft Academic Graph, arXiv, and the Department's websites. Search results were selected primarily from academic journals published between 2017 and 2021, magazines and news articles. Search terms included "DOD", "AI", "Strategy", "People" "Frameworks", "Technology", "AI Threats", "Technology Models", "Implementing AI", "AI Challenges", "Ethics for AI", "AI Benefits" and "Guidelines and Principles for AI".

The author found little existing guidance on Al adoption models, as these frameworks are still in development by organisations and academia; a similar finding echoed by Reim et al. (2020:180) that "Managers are left with little support from academia when aiming to implement Al".

1. AI ACROSS THE DEPARTMENT

The Joint Artificial Intelligence Centre (JAIC), established in 2018, operates as the Department's implementor of AI strategy. As such, they focus on research and

development to identify, plan, and deliver successful, scaled-up AI prototypes and solutions. They also collaborate with academia and commercial partners and are responsible for recruiting and maintaining an AI-capable workforce. The National Defence Authorisation Act (NDAA) Section 238(e) of 2019 commissiopns JAIC to "explore, develop, and field AI capabilities across the force... and to make recommendations for securing and growing the DoD's advantage in AI" (Golden, 2020:78).

Exploring and fielding new AI capabilities in the Department is necessary as they face increased competition from rival states such as China and Russia. For example, China has submitted more peer-reviewed articles (Figure 1 and Figure 2) than the EU and the US.

PEER-REVIEWED AI PUBLICATIONS (% of WORLD TOTAL) by GEOGRAPHIC AREA, 2000-19 Source: Elsevier/Scopus, 2020 | Chart: 2021 Al Index Report

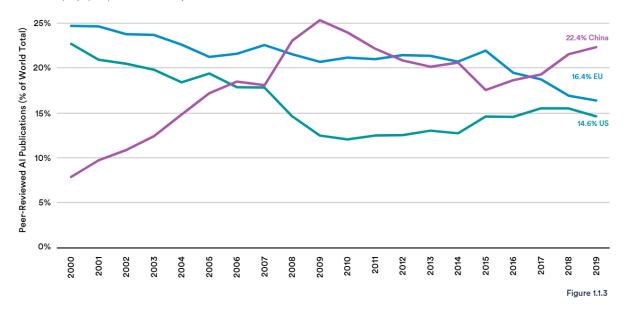


Figure 1 China's total% of peer-reviewed publications (Zhang et al., 2021)

PEER-REVIEWED AI PUBLICATIONS (% of TOTAL) by REGION, 2000-19 Source: Microsoft Academic Graph, 2020 | Chart: 2021 Al Index Report

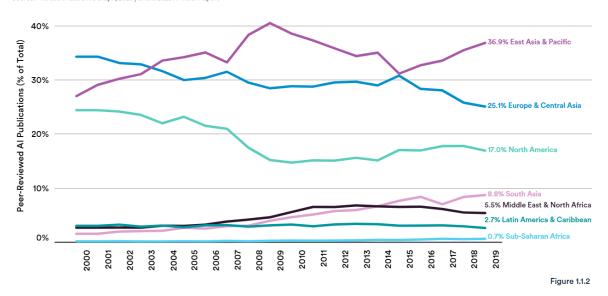


Figure 2 Total % of Peer-reviews by Region (Zhang et al., 2021)

Therefore, the author views JAIC as a necessary response to narrow the investment gap into AI adoption, implementation, and education in the Department. However, despite their current position, they do use AI in a variety of ways:

- Machine-Learning (ML). JAIC used ML to understand critical supply shortages
 in response to the coronavirus pandemic (Project Salus). They also use ML to
 deliver a prototype that reduces a backlog of unmatched financial transactions
 that amount to billions of USD (JAIC_1, 2020).
- Augmented Reality. JAIC recently deployed augmented reality microscopes to aid pathologists in detecting metastatic breast cancer cells using AI models (JAIC_2, 2020).
- Natural Language Processing (NLP). Efforts are underway to embrace NLP to power AI chatbots on government websites and call centres.
- Computer Vision. JAIC used computer vision to track and map wildfires (in collaboration with Microsoft, under the banner of "First Five Consortium") to deliver humanitarian relief and search-and-rescue missions. The Air Force (Project Maven) analysed aerial drone video footage and classified 38 types of objects for human review (Pellerin, 2017).

Predictive Analytics. The Air Force utilises AI for intelligent calculation of repair
and maintenance tasks for several fleets of aircraft types. Moreover, they
recently commissioned research into the use of AI-based performance scoring
for their human resource management processes (Schulker, D. et al., 2021).

2. BENEFITS AND DRAWBACKS

Al brings tremendous benefits to the US DoD; for instance, enhanced situational awareness and decision-making using computer vision to extract useful information from images, video feeds, or raw data. Commanders can then explore options to select alternate actions with the best outcomes that minimise risks to both troops and civilians.

ML can help deliver innovative solutions to assist military healthcare, help reduce warfighter suicide rates, fixing payroll errors, and make better data-informed decisions such as predictive maintenance. When used with computer vision, it enables autonomous vehicles to navigate benign environments and deliver troops' supplies—similar advancements are underway in the private sector for self-driving cars.

The most appealing benefit is reducing costly mistakes and increasing agility, allowing the Department to move staff away from tiresome, repetitive tasks to those requiring higher-level reasoning and judgment.

Finally, using AI drives innovation by creating foundational platforms, reusable tools, frameworks, and standards. These changes promote adaptable problem-solving with AI, encourage experimentation, and improve delivery speed and scaling of AI prototypes.

However, drawbacks exist too; for example, a significant drawback is a change required to current staff acquisition policy and processes. The Department's current recruitment process takes an average of 100 days to recruit staff, where in contrast, the private sector hires in a matter of days (Golden, 2020).

Another drawback is people's distrust of AI systems. Specifically, they push back against the black-box nature of AI systems if they cannot explain decisions or outcomes deemed wrong or contrary to the norm. For example, industry leaders like

Elon Musk, Steve Wozniak, Stephen Hawkins Noam Chomsky have spoken out against the use of black-box automated AI in weapons systems (Autonomous Weapons Systems or AWS). Moreover, Google too has pushed back with their involvement in Project Maven (Brustein & Bergen, 2019).

Furthermore, AI in AWS faces another drawback because the Department abides by the Geneva Conventions regarding armed combat. Arming nonhuman AI agents with the capability to select targets violates the Principles of Distinction and Proportionality (Sharkey, 2013). Moreover, since AI systems do not have context for decisions, they find it difficult to differentiate between civilian or combatant—something humans also struggle with.

Finally, the operational costs associated with gathering, curating and treating AI data can prove exorbitant and impractical. Data is often the costliest and most time-intensive phase of any AI implementation (Coseer, 2017).

3. TECHNOLOGY EVALUATION

Figure 3 shows operational areas used to identify risks and challenges faced by JAIC.

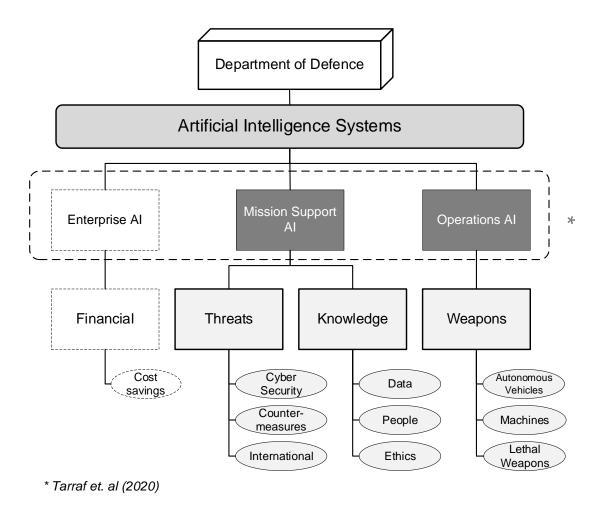


Figure 3 Operational areas of risks and challenges (created by the author with considerations from Tarraf et al., 2020)

Table 1 Al systems areas

Area	Description	Areas of Concern
Threats	Al systems operated by people inside or	Intent and human
Tilleals	outside the Department.	behaviour
Knowledge	Rules, principles, and guidelines governing Al data quality, security, privacy, and use.	Al Ethics and
		Principles
		 Skilled Workforce
		 Regulations
		Governance

Description	Areas of Concern
	■ Trust
	Regulations
	Governance
Al systems used in warfighting scenarios	Safety
or deployed in society.	Autonomy
	■ Human Agency
	Regulations
	Wellbeing
	Al systems used in warfighting scenarios

Figure 4 further classifies the operational areas into a people-centred view to show the connectedness of risks and challenges between People and Purpose through AI.

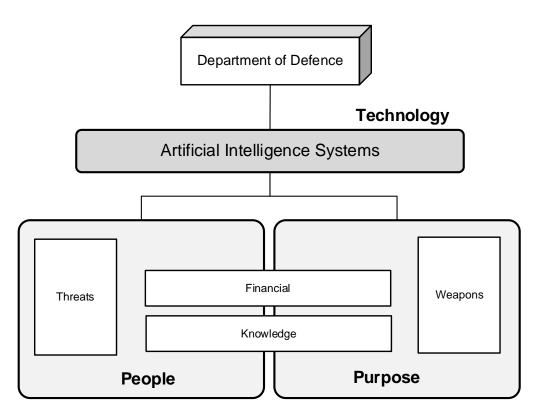


Figure 4 Al for People, Purpose and Technology (created by the author)

Table 2 Al areas for People, Purpose and Technology

Topic	Description	
Technology	Al systems, hardware and platforms they run on.	
People	Users affected by AI systems and included societies' concern, culture, and ethics around AI.	
Purpose	Systems and machines that have a purpose for existence and use across the Department.	

3.1. RISKS TO AI ADOPTION

Zhang et al. (2021) provide a list of risks associated with Al adoption (Figure 5). When considered together with Figure 4, the top four risks are Technology (Cybersecurity), Purpose (Explainability, Regulatory Compliance) and lastly, People (Personal/Individual Privacy). Figure 6 shows this prioritised classification in the context of risks and challenges.

RISKS from ADOPTING AI THAT ORGANIZATIONS CONSIDER RELEVANT, 2020

Source: McKinsey & Company, 2020 | Chart: 2021 Al Index Report Cybersecurity Regulatory Compliance Explainability Personal/Individual Privacy Organizational Reputation Workforce/Labor Displacement **Equity And Fairness Physical Safety** 2019 **National Security** 2020 Political Stability 0% 10% 20% 30% 40% 50% 60% % of Respondents

Figure 3.3.5

Figure 5 Risks associated with Al adoption (Zhang et al., 2021)

In addition to the results from Zhang et al. (2021):

- 1) Technology
- Autonomy. As AI technology advances, concern grows that AI may eventually reach the equivalence of human intelligence and become uncontrollable. A topic referred to as AI anxiety by Johnson & Verdicchio (2017).
- 2) Purpose
- ➤ **Data**. Poorly labelled ML data is a risk that severely affects reputation or leads to unintended actions such as stereotype profiling or acting negatively against individuals based on inaccurate results.
- 3) People
- Collaborations. Collaborating with academia, organisations (which favour intellectual property ownership) and contractors, brings risk because they have access to sensitive or proprietary data that can easily be leaked or manipulated.

3.2. CHALLENGES FOR AI ADOPTION

- 1) Technology
- Cloud Providers. Using cloud platforms allows the Department to reduce unnecessary costs spent maintaining physical hardware and software updates, which can be used instead for the workforce or deployed forces (Department of Defense, 2018).
- 2) Purpose
- Ethics/Principles. The NDAA requires ethics in Al. It is challenging to find guidance on Al in defence scenarios since guidelines and ethics are still in development.
- 3) People

> **Skills.** Rising AI demand from industry is tempting more academics away, and it may prove challenging to attract the right skills without competitive pay incentives. Funding may prove challenging as, according to Golden (2020:80), current US funding levels into AI are inadequate.

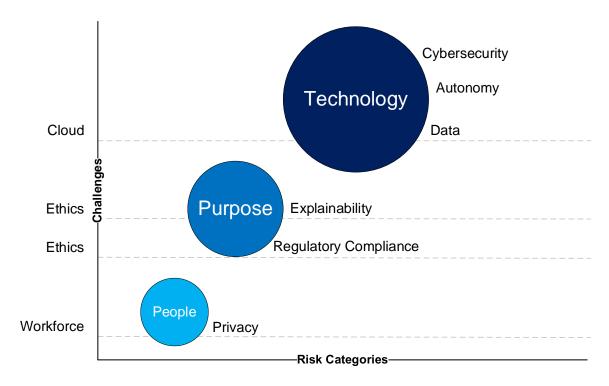


Figure 6 Risk and Challenges according to People, Purpose and Technology (created by the author)

3.3. RECOMMENDATIONS

The primary recommendation is to focus on security and AI process transparency. JAIC will need to maintain an AI-skilled workforce, so training and recruitment are crucial to meet this goal. Also required is the need to implement AI ethics based on guidelines. Using cloud providers is highly recommended for reliable, globally distributed processing capability to handle volumes of data and their support for on-demand scalability.

Tools such as TensorFlow or Microsoft's AI platform are recommended for ML models because these tools are readily available and somewhat easy to use. Lastly, the pace of delivery to facilitate rapid fielding, testing, and deployment of AI systems

must improve. Without an ability to rapidly deliver new AI prototypes, the Department will not benefit from their investment into AI—cost savings, agility, increased productivity.

4. IMPLEMENTATION FRAMEWORK

How can JAIC implement this technology? Table 3 shows frameworks to support the JAIC that are usable by management and engineering teams.

Table 3 Frameworks considered

Framework / Model	Target Use	Audience	AI- centric?	Used by DoD?
RACI Matrix	A roles and responsibilities matrix.	Management	No	
TOGAF	Enterprise Architecture	Architects	No	
DoDAF	Enterprise Architecture	Architects	No	Yes
COBIT v5	IT Governance and Management Practices.	Management	No	
ITIL v4	Delivery of IT services.	Management	No	Yes
EFQM	Quality Management.	Management	No	
еТОМ	Business Process Framework for Service-focused Businesses.	Management	No	Yes
ECCOLA	Al Ethics Systems Design Method.	Engineers	Yes	No
Deloitte Trustworthy AI Framework	Al Ethics Auditing.	Management	Yes	No

Framework / Model	Target Use	Audience	Al- centric?	Used by DoD?
PWC's Responsible Al Toolkit	Set of tools and frameworks to harness AI in Organisations.	Management	Yes	No

To choose an appropriate framework, considered were four points:

- 1. Golden (2020:79) states, "adopting... an ethical framework for all Al... is vital to the DoD's continued compliance...".
- 2. The requirements for JAIC to use AI ethics as required by NDAA Section 238(e).
- According to Dignum (2017), transparency is key to understanding the development of AI systems and forms the main backbone of AI ethics and principles.
- 4. Fjeld et al. (2020) identified eight themes related to AI ethics. The themes address safety and security, fairness, human agency, human values, openness, accountability, responsibility, and privacy.

PWC Responsible Al Toolkit and Deloitte Trustworthy Al Framework are excluded from selection when considering the points above. Their exclusion is because they do not have any associated peer-reviewed articles, and very little research exists on their use. In contrast, the recommendation is to use ECCOLA (Vakkuri et al., 2020) for designing Al systems because it meets point one, two and three above.

ECCOLA is modular, practical and built on ethics research over two years with empirical use data. As Figure 7 shows, it ties nicely with point four above, linking research with an implementation method and provides engineers and data scientists with guidance to turn abstract AI ethics and principles into reality, especially for systems within the Department.

So, from the author's point of view, ECCOLA is an excellent foundation framework for bottom-up implementation.

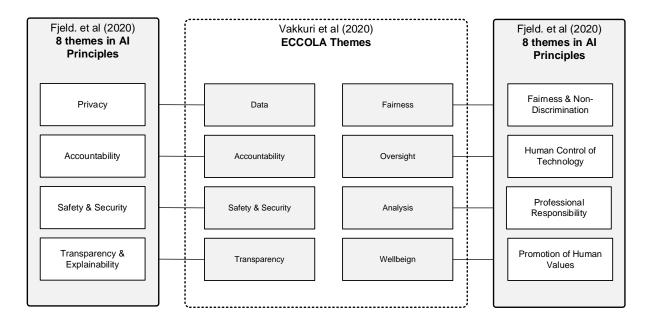


Figure 7 Comparison between ECCOLA and the Principled Artificial Intelligence Whitepaper by Fjeld et al. (2020). (Figure created by the author)

4.1. ECCOLA method overview

The framework comprises several "cards" (Table 4) based on themes found in ethics guidelines (Figure 7). Development cycles consult only those cards applicable during each iteration. Each card has three sections that address the practical aspect of implementing AI ethics (Figure 8).

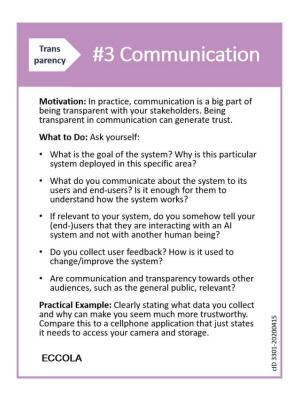


Figure 8 ECCOLA Card Example (Vakkuri et al., 2020)

Motivation discusses the *why* of the principle, What to Do describes research-based *reasoning*, and Examples show *how* implementors can implement the specific guideline.

Table 4 ECCOLA cards

Theme	Card	Addresses
Accountability	Ability to Redress	Compensation in the event of Al failures or catastrophes.
Accountability	Auditability	Ability to audit the AI system and its decisions.
Accountability	Minimising Negative Impacts	Reducing financial impact.
Analysis	Stakeholders	Those affected by the system.
Data	Data Access	How are the data used, and by whom?

Theme	Card	Addresses
Data	Data Quality	Quality and integrity of data that must align with the system's purpose.
Data	Privacy and Data	Regulations and peoples' right to data privacy.
Fairness	Accessibility	Ensures technology is accessible to all.
Fairness	Stakeholder Participation	Involvement of all affected stakeholders.
Oversight	Human Agency	Independent human decisions.
Oversight	Human Oversight	Human decision-making.
Safety & Security	System Safety	Risks and consequences.
Safety & Security	System Security	Attack surface of the system
Transparency	Communication	Being honest and open to foster trust.
Transparency	Documentation Trade-Offs	Documenting selection of alternatives.
Transparency	Explainability	Explain the reasons behind AI decisions.
Transparency	System Reliability	Describe how the system works.
Transparency	Traceability	Supports Explainability.
Transparency	Transparency Requirements	Disclosure of information.
Wellbeing	Environmental Impact	Impact on the environment.
Wellbeing	Society Impact	Impact on society.

4.2. Use in the Department

Considering the twenty-one cards available, it may seem daunting to know where to start; therefore, Figure 9 shows the author's recommendations for the most appropriate themes, considering the risks and challenges identified earlier.

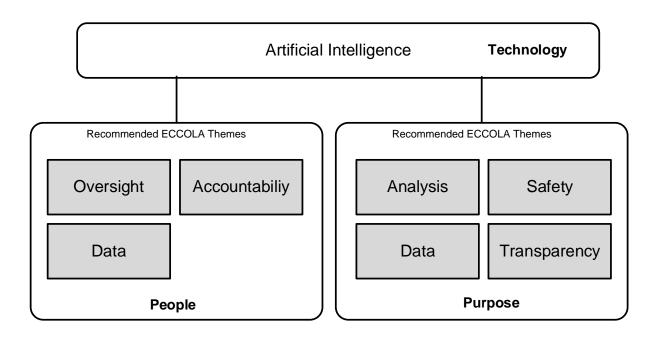


Figure 9 Recommended Cards related to People, Purpose, Technology (created by the author)

Table 5 Recommended cards

Theme	Recommended Card	Reason
Analysis	Stakeholders	 The JAIC must understand the People affected by the AI systems, users, staff, society, or government. The cultural impact of the users' response to the AI systems is vital too.
Transparency	ExplainabilityTransparency RequirementsTraceability	 Al processes must be explainable. Purpose-based Al systems require trust. Regulations may require insight into Al systems.
Accountability Data	AuditabilityPrivacy and DataData Quality	 Protection of data is crucial. Sourcing and manipulation of data must meet high standards.
	Data Access	meet night standards.

Theme	Recommended Card	Reason
Oversight	Human AgencyHuman Oversight	 Humans must always remain in charge of Al systems.
Safety & Security	System SecuritySystem Safety	Purpose-based AI systems can have catastrophic consequences.

CONCLUSION

Today's world is information-based, and AI technology promises to bring positive benefits to organisations and the defence industry. The United States Defence Department has identified global and technological threats they face by AI and taken bold moves to understand and better utilise it. Their collaboration with academia and commercial sectors will foster new AI research, standards, and guidelines that are incredibly positive for establishing globally accepted AI principles in a defence setting.

Much of the research into AI application for the case study identified the concepts of ethics and explainability as primary topics—despite the risks identified by Zhang et al. (2021). Ethics are the intangible principles for data, processes, human involvement, regulations and ultimately, the safety of such systems. These issues fit well with the case study, as addressing each one is not optional: AI affects People and Purpose.

Society is wary of the defence industry's use of AI in weapons systems. The response by the NDAA to mandate using AI ethics to develop Department AI systems shows that government is mindful of AI's perceived threat to society. Not only perceived threats, but researchers, governments and organisations are also working to establish AI guidelines that direct the evolution of AI in all sectors of society (as highlighted by Fjeld et al., 2020). Unfortunately, these guidelines do not consider AI use solely in a defence setting. For this reason, the Department's collaborations will establish new models and targeted guidance for other defence departments globally.

Additionally, even as the Department adopts more AI systems to replace humans in menial tasks requiring full-time engagement, they still need an AI-skilled workforce. So, while academics migrate to the private sector, the Department's need will open

opportunities that allow, as it were, society to be a part of Al system development in the Department.

The Department currently is underutilising their existing data, and they also do not consolidate their data from other divisions. Since every benefit of AI relates to underlying data and models, scanning video, analysing scenarios—investment, society, climate, science, war—, reducing costs, or managing supply chains, the Department requires global infrastructure to provide and sustain their AI systems. Incorporating a cloud-based strategy is transformative and beneficial together with AI technology.

In conclusion, despite words like "learning", "vision", or "intelligence", AI systems are not human but our benefactors. Ethics, guidelines, and regulations are intended not for machines but for people whose purpose requires regulation.

REFERENCES

Brustein, J. & Bergen, M. (25 Nov. 2019) Google's Defense Dilemma. *Bloomberg Businessweek*, 4638: 38–43. Available at: http://o-search.ebscohost.com.serlib0.essex.ac.uk/login.aspx?direct=true&db=bsu&AN=139779246&site=eds-live [Accessed 5 Apr. 2021]

Department of Defense, (2018) DoD Cloud Strategy. Available at:

https://media.defense.gov/2019/Feb/04/2002085866/-1/-1/1/DOD-CLOUD-STRATEGY.PDF [Accessed 18 Apr. 2021]

Dignum, V. (2017) Responsible autonomy. Arxiv: https://arxiv.org/abs/1706.02513 [Accessed 11 Apr. 2021]

Golden, P. E. (2020) DoD's artificial intelligence problem: Where to begin. *Army Lawyer*, 2020(2): 76-85. Available at:

https://heinonline.org/HOL/P?h=hein.journals/armylaw2020&i=190 [Accessed 4 Apr. 2021]

- Fjeld, J., Achten, N., Hilligoss, H., Nagy, A.C, Srikumar, M., Dushkin, R., Tolmatov, A. & Onatsik, K. (2020) Principled artificial intelligence: Mapping consensus in ethical and rights-based approaches to principles for Al. *Berkman Klein Center Research Publication*.
- JAIC_1, (2020) JAIC Partners with DIU on AI/ML Models to Resolve Complex

 Financial Errors. Available at: https://www.ai.mil/blog_10_01_20-jaic_partners_with_diu_on_aiml_models_to_resolve_complex_financial_errors.html

 [Accessed 18 Apr. 2021]
- JAIC_2, (2020) JAIC, in partnership with DIU, Delivering AI-Enabled Cancer
 Diagnostics at the Point of Care. Available at: https://www.ai.mil/blog_10_01_20-jaic_partners_with_diu_on_aiml_models_to_resolve_complex_finanical_errors.ht
 ml [Accessed 18 Apr. 2021]
- Johnson, D., & Verdicchio, M. (2017) Al Anxiety. *Journal of the Association for Information Science and Technology* 68(9): 2267-2270. DOI: https://doi.org/10.1002/asi.23867
- Mishra, S., Clark, J. & Perrault, C.R (2020) Measurement in Al Policy: Opportunities and Challenges. Arxiv: https://arxiv.org/abs/2009.09071v1 [Accessed 16 Apr. 2021]
- Pellerin, C. (2017) Project Maven to Deploy Computer Algorithms to War Zone by Year's End. Available at:

 https://www.defense.gov/Explore/News/Article/Article/1254719/project-maven-to-deploy-computer-%20algorithms-to-war-zone-by-years-end/ [Accessed 3 Apr. 2021]
- Reim, W., Åström, J., Eriksson, O. (2020) Implementation of Artificial Intelligence (AI): A Roadmap for Business Model Innovation. *AI* 1(2): 180-191. DOI: https://doi.org/10.3390/ai1020011
- Schulker, D., Lim, N., Matthews, L.J., Grimm, G.E., Lawrence, A., & Firoz, P.S. (2021) Can Artificial Intelligence Help Improve Air Force Talent Management? An

Exploratory Application. Available at:

https://www.rand.org/content/dam/rand/pubs/research_reports/RRA800/RRA812-1/RAND_RRA812-1.pdf [Accessed 3 Apr. 2021]

- Sharkey, N. (2010) Saying 'No!' to Lethal Autonomous Targeting. *Journal of Military Ethics* 9(4): 369–83. DOI: https://doi.org/10.1080/15027570.2010.537903
- Tarraf, D.C., Shelton, W., Parker, E., Alkire, B., Gehlhaus, D., Grana, J., Levedahl, A., Leveille J., Mondschein, J., Ryseff, J., Wyne, A., Elinoff, D., Geist, E., Harris, B.N., Hui, E., Kenney, C., Newberry, S., Sachs, C., Schirmer, P., Schlang, D., Smith, V.M., Tingstad, A., Vedula, P. & Warren, K. (2021) The Department of Defense's Posture for Artificial Intelligence: Assessment and Recommendations for Improvement. DOI: https://doi.org/10.7249/RB10145
- Vakkuri, V, Kemell, K.-K., & Abrahamsson, P. (2020) 'ECCOLA a Method for Implementing Ethically Aligned AI Systems', 46th Euromicro Conference on Software Engineering and Advanced Applications, SEAA 2020. Portoroz, Slovenia, 26-28 August 2020. 195-204. DOI: https://doi.org/10.1109/SEAA51224.2020.00043
- Zhang, D., Mishra S., Brynjolfsson, E., Etchemendy, J., Ganguli, D., Grosz, B., Lyons, T., Manyika, J., Niebles, J.C., Sellitto, M., Shoham, Y., Clark, J., & Perrault, R., (2021) The AI Index 2021 Annual Report.: AI Index Steering Committee, Human-Centered AI Institute. arXiv: https://arxiv.org/abs/2103.06312 [Accessed 3 Apr. 2021]

BIBLIOGRAPHY

- Corrin, A. (2017) DoD spent \$7.4B on big data, AI on the cloud last year. Is that enough? Available at: https://www.c4isrnet.com/it-networks/2017/12/06/dods-leaning-in-on-artificial-intelligence-will-it-be-enough/ [Accessed 31 Mar. 2021]
- Department of Defence (2018) Summary of the 2018 Department of Defense Artificial Intelligence Strategy: Harnessing AI to Advance our Security and

Prosperity. Available at: https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/-1/SUMMARY-OF-DOD-AI-STRATEGY.PDF [Accessed 31 Mar. 2021]

Department of Defence (2019) Al Principles: Recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense. Available at: https://media.defense.gov/2019/Oct/31/2002204458/-1/-1/0/DIB_AI_PRINCIPLES_PRIMARY_DOCUMENT.PDF [Accessed 3 Apr. 2021]

Department of Defence (2020) Unleashing data to advance the National Defence Strategy: DoD Data Strategy. Available at:

https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF [Accessed: 11 Apr. 2021]

- Dick, S. (2019) Artificial Intelligence. *Harvard Data Science Review, Artificial Intelligence* 1(1). DOI: https://doi.org/10.1162/99608f92.92fe150c
- Hoadley, D.S. & Lucas, N.J. (2018) Artificial Intelligence and National Security.

 Available at: https://a51.nl/sites/default/files/pdf/R45178.pdf [Accessed 16 Mar. 2021]
- Johnson, J. (2019) Artificial intelligence & future warfare: implications for international security. *Defense and Security Analysis*. *35(2)*: 147-169. DOI: https://doi.org/10.1080/14751798.2019.1600800
- Joint Artificial Intelligence Center (2019) Transforming the Department of Defence Through AI. Available at: https://www.ai.mil/index.html [Accessed 31 Mar. 2021]
- NITRD (2019) The Networking & Information Technology Research & Development Program: Supplement to the President's FY2020 Budget. Available at: https://www.nitrd.gov/pubs/FY2020-NITRD-Supplement.pdf [Accessed 3 Apr. 2021]