2023

Ethical Concerns in the Technical Acquisition of Predictive Maintenance Technology within the Department of Defense

MAYA DAVIS

ESI 6891 – IEMS RESEARCH METHODS

INDUSTRIAL ENGINEERING

OCT 22, 2023

The integration of software into military applications gives rise to profound ethical concerns. Regarding data privacy and transparency, it is important that the data is protected, and the end users are informed on how the data will be utilized. Predictive maintenance systems are reliant on vast data sets, thus present risks of misuse and privacy violations. Furthermore, cybersecurity is a paramount worry due to the vulnerability of predictive maintenance systems to cyber-attacks, jeopardizing data integrity. The complexity of predictive maintenance algorithms makes the challenge more complicated, hindering transparency and accountability in decision-making processes. Accountability is further complicated considering who will take the responsibility when errors occur, potentially resulting in significant consequences. Moreover, ethical debates concerning artificial intelligence (AI) focus on job displacement, raising concerns about unemployment and societal repercussions. Lastly, the environmental impact of technology components, from production to disposal, presents ethical concerns. Mismanagement of these impacts raises questions about the environmental footprint of predictive maintenance technology. In this report, I will delve into the ethical dilemmas associated with the government's ongoing procurement of predictive maintenance software. The aim is to unravel the intricate intersection of technology, ethics, and military operations. Additionally, this report provides a unique perspective drawn from my personal experience as a defense contractor actively engaged with predictive maintenance technology. Leveraging my firsthand encounters, I will offer nuanced insights, supported by relevant research, to underpin the arguments presented.

Numerous instances illustrate how ethical considerations can influence research practices related to the technical acquisitions of predictive maintenance technologies within the Department of Defense (DoD). Predictive maintenance, employing artificial intelligence (AI) and machine learning, guides end users on the timing of specific actions. Predictive maintenance technology encompasses proactive tools that offer guidance to end users regarding the precise timing of necessary actions. The advent of AI streamlines tasks such as anomaly detection and identifies part failure at the end of its

lifespan. Ensuring military preparedness is crucial, and predictive maintenance technology plays a pivotal role in supporting these processes for the military. As the DoD strives to maintain military preparedness, the integration of predictive maintenance technology emerges as an imperative. By efficiently predicting and preventing potential equipment failures, the military can ensure the reliability and functionality of its resources and safeguard national security interest.

Addressing ethical concerns in research cannot be left solely to individual researchers, a practice reminiscent of the pre-World War II era, illustrated by events like the Nuremberg trials under the Nazi regime in Germany (White, T. L. and D. H. McBurney [1]). These historical incidents served as a stark reminder of the ethical implications in psychological research, emphasizing the need to learn from past errors. Understanding the cause-and-effect dynamics in psychological research over time became crucial. The report underscored the challenge of predicting acceptable practices a decade or two into the future (White, T. L. and D. H. McBurney [1]). In the military context, learning from previous mistakes is not always possible due to the unpredictable nature of the world today. Predictive maintenance technology, especially in defense contracts like the F-35 platform, allows minimal room for error given the rapid pace of technological advancement. Employees at defense contractors like Lockheed Martin must collaborate with various companies, and when issues arise, accountability complexities surface. A recent report by the Government Accountability Office (GAO) highlighted the need for better accountability for global spare parts, citing significant losses and delays in disposition instructions for over 19,000 spare parts in the F-35 program (Kociolek, K [5]). The GAO proposed four solutions to address this issue, but the concern remains about algorithm-driven decisions declaring parts end-of-life; who should be held accountable for faulty predictions could pose a more significant problem (Kociolek, K [5]). Often defense contractors collaborate across various companies for a single contract. Sometimes it is unpredictable when things go wrong. When things go wrong ethically these companies must be held

accountable. Accountability is an ethical concern because it is important to hold entities accountable when ethical issues arise.

In the Ethics in Research report, the American Psychological Association (APA) ethics code was outlined, emphasizing the importance of a systematic approach to research (White, T. L. and D. H. McBurney [1]). Acknowledging the insufficiency of relying solely on individual researchers for ethical oversight, the APA established internal review boards (IRBs). These IRBs, obligatory for institutions receiving government funding, consist of diverse panels including scientists, non-scientists, and individuals affiliated with the conducting institution (White, T. L. and D. H. McBurney [1]). The diversity within these IRBs serves an important purpose. Similarly, institutions such as the Defense Advanced Research Projects Agency (DARPA [2]) adhere to similar principles, employing diverse committees to assess research projects, ensuring a multifaceted perspective on ethical considerations, and enhancing the integrity of scientific inquiry (DARPA [2]). In 2016, DARPA sought research on interpretable artificial intelligence (XAI) in direct response to concerns about transparency in algorithms (Arrieta et al [3]). The rapid progress in machine learning and artificial intelligence has led to the emergence of highly capable autonomous systems. However, these systems face challenges in articulating their decisions and actions to human users. This lack of clarity is a significant concern for the Department of Defense (DoD) as it endeavors to develop more intelligent and autonomous systems. Initially, AI systems achieved clarity through logical and symbolic reasoning methods, generating explanations based on human-readable symbols. With AI's evolution, newer, more effective machine learning techniques emerged, albeit resulting in less clear models. DARPA aims to confront this challenge by developing interpretable machine learning methods, combining them with explanatory techniques to facilitate users' comprehension, trust, and management of the evolving generation of AI systems (Arrieta et al [3]). The transparency of these systems is an important ethical concern. It is important that the end user is aware of how the algorithm is functioning. This will help overcome blindly trusting the technology.

Condition-based maintenance, a proactive method aimed at detecting potential failures before they occur, is commonly employed by various sectors of the military. Typically overseen by the DoD contractors, this approach involves continuous inspections by personnel to identify and report structural anomalies necessitating repair or replacement. Although diagnostics, often performed by contractors or the military, offer valuable pre-failure information, accurately predicting remaining life estimates presents challenges. In an article, Application of physical failure models to enable usage and load based maintenance, the authors claim that it is unnecessary to monitor equipment in the matter of conditional-based maintenance, but only equipment usage (J. Dalzochio et al. [4], Tinga et al [7]). In this context, it's essential to consider the broader impact of AI technologies. AI and automation threaten to replace jobs across various sectors, making it imperative for industries to adapt and evolve. The invention of AI-powered predictive maintenance algorithms, although promising in their efficiency, raises concerns about potential job displacement. Industries face significant transformations due to AI. Automation and predictive algorithms, while enhancing efficiency, also pose challenges to the workforce. Striking a balance between technological advancement and preserving employment opportunities remains a critical consideration as AI continues to revolutionize diverse sectors. Therefore, the need for a holistic approach to integrating AI in maintenance practices becomes not only a technical challenge but also a socio-economic imperative.

In the pursuit of developing advanced predictive maintenance techniques, one encounters the immense challenge of accumulating an extensive and diverse dataset. In the article Predictive Maintenance in the Military Domain, the authors mention that one of the challenges is data security, bandwidth, and latency (J. Dalzochio et al. [4]). This collection of data forms the foundation upon which these techniques are built. To ensure the accuracy of predictions, intricate models must be meticulously trained, necessitating access to a wide array of data sources. However, the ethical landscape surrounding this becomes complex when considering data privacy and cybersecurity. Safeguarding the

privacy of the data being utilized is of paramount importance. The article also briefly mentions the importance of data encryption as a technique to minimize security problems when transmitting sensitive information (J. Dalzochio et al. [4]). In the realm of predictive maintenance, where the evaluation of data related to military professionals is imperative for precise predictions, ethical concerns regarding privacy infringement arise. The intrusion into personal or professional data for the sake of accurate predictions raises ethical dilemmas, especially in sensitive contexts such as military operations. Striking a balance between accessing valuable data for predictive insights and respecting individuals' privacy rights is crucial. Moreover, the security of this data cannot be overstated. Protecting this information from unauthorized access and potential misuse is equally vital. Predictive maintenance algorithms rely on the estimation of useful life and the analysis of conditional events to predict failure accurately. If this data were to fall into the wrong hands, it could be exploited for nefarious purposes, posing significant risks. In summary, the development of predictive maintenance techniques is not only a scientific and technical challenge but also an ethical one. Balancing the need for comprehensive data access with respecting individual privacy and ensuring robust cybersecurity measures is essential to the responsible advancement of these predictive technologies.

As we delve deeper into the realm of predictive maintenance techniques, it becomes increasingly evident that these advancements in technology can potentially ripple across various sectors, including the environment. One significant environmental implication arises from the reduced frequency of parts cannibalization facilitated by these predictive methods. While there might be valid reasons for disposing of specific parts and materials, the disposal process itself can trigger environmental impacts. Predictive maintenance, by prolonging the life of components, might inadvertently impede certain recycling processes. In the article, Simultaneous predictive maintenance, and inventory policy in a continuously monitoring system using simulation optimization, the authors discuss the development of a maintenance model that simultaneously considers the predictive maintenance and inventory policies

of spare parts (Y. Y Liu et al [6]). The proposed model aims to find the optimal component inventory policy and degradation level thresholds of each component (Y. Y Liu et al [6]). The findings suggest that the increase in purchasing cost would barely affect the optimal inventory policy, and higher purchasing costs would result in a higher difference between the repair and replacement policies (Y. Y Liu et al [6]). This unintended consequence could lead to a stagnation in the recycling chain, hindering the sustainable management of materials and resources. Additionally, the algorithms driving predictive maintenance might predict shorter lifespans for certain parts, triggering premature replacements. Such alterations in the replacement cycle could strain the supply chain, accelerating the consumption of resources and exacerbating environmental stress. Therefore, it is imperative to broaden our perspective when developing these algorithms. Alongside the technical precision and accuracy, due consideration must be given to the intricate interplay between predictive maintenance, the supply chain, and the environment. These considerations become paramount ethical concerns, as they underline the responsibility inherent in technological advancements. Balancing the need for efficient maintenance with the preservation of environmental integrity is not just a moral obligation but also an ethical imperative that guides the development of predictive maintenance techniques. Only by addressing these concerns can we ensure that our technological strides do not come at the cost of environmental degradation.

In conclusion, the integration of predictive maintenance technology within the Department of Defense raises several ethical concerns. Data privacy and transparency are major issues due to the vast data sets required for predictive maintenance algorithms. The complexity of these algorithms also hinders accountability in decision-making processes, which can have significant consequences. The potential for job displacement and societal repercussions is another concern, as is the vulnerability of predictive maintenance systems to cyber-attacks. Finally, the environmental impact of technology components used in predictive maintenance systems raises questions about their sustainability.

Addressing these ethical concerns is crucial to ensure that the integration of predictive maintenance technology within the Department of Defense is done in a responsible and sustainable manner.

References

[1] White, T. L. and D. H. McBurney (2012). Research methods, Cengage Learning.

[2] Agency, D. A. R. P. A from https://www.darpa.mil/about-us/about-darpa.

[3] Arrieta, A. B., et al. (2020). "Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI." Information fusion 58: 82-115.

[4] Dalzochio, J., et al. (2023). "Predictive maintenance in the military domain: a systematic review of the literature." ACM Computing Surveys 55(13s): 1-30.

[5] Kociolek, K. (2023). F-35 Program: DOD Needs Better Accountability for Global Spare Parts and Reporting of Losses Worth Millions. G. A. Office.

[6] Liu, Y.-Y., et al. (2023). "Simultaneous predictive maintenance and inventory policy in a continuously monitoring system using simulation optimization." Computers & Operations Research 153: 106146.

[7] Tinga, T. (2010). "Application of physical failure models to enable usage and load based maintenance." Reliability engineering & system safety 95(10): 1061-1075.