2022 IEEE/AIAA 41st Digital Avionics Systems Conference (DASC), 18-22 September 2022, Portsmouth, Virginia, USA
DOI:10.1109/DASC55683.2022.9925869

UTM Regulatory Concerns with Machine Learning and Artificial Intelligence

Richard Ryan
Cranfield University
United Kingdom
r.ryan@cranfield.ac.uk

Saba Al-Rubaye
Cranfield University
United Kingdom
s.alrubaye@cranfield.ac.uk

Graham Braithwaite
Cranfield University
United Kingdom
g.r.braithwaite@cranfield.ac.uk

Abstract— **Artificial intelligence (AI) and machine learning will have a significant impact on the application of drones and the integration of universal traffic management (UTM) that relate to unmanned operations in urban environments at very low-level airspace. Artificial intelligence will necessitate high levels of automation and act as an enabler with respect to the integration of unmanned and manned aviation and AI will ultimately enable safe operations with respect to high numbers of drones utilising the same airspace, and more specifically with respect to detect and avoid capability. AI is going to be heavily developed and utilised by organisations that certify as U-space service providers (USSP's) when providing a service to UAS (Unmanned Aerial Systems) Operators. The equipment utilised by UAS Operators will to some extent already benefit from AI, but the level of automation is currently constrained by regulation. A legal framework must exist, as AI will not only have a significant impact upon existing laws but will ensure a framework that facilitates safety and the fundamental rights of citizens and businesses with respect to AI. The EU has published a proposed law, namely the Artificial Intelligence Act as permitted under Article 114 of the Treaty on the Functioning of the European Union (TFEU).**

Keywords— Artificial intelligence, AI, U-space service providers (USSP's), universal traffigfic management (UTM), UAS (Unmanned Aerial Systems), automation, regulation, legal framework, human machine teams, human in the loop, human on the loop, human outside the loop, EU AI Act, machine learning (ML).

I. Introduction

Regulation usually plays catch up with technology as technology evolves, adapts and changes at a very much quicker pace than what can be legislated for. Regulation, therefore, needs to be flexible and/ or proactive [13]. The European Union (EU) have sought to be proactive by laying down harmonised rules on artificial intelligence via their proposal published in 2021 [1], [2]. The EU acknowledged within the explanatory memorandum [2] that *"AI is a fast-evolving family of technologies that can bring a wide array of economic and societal benefits across the entire spectrum of industries and social activities… in light of the speed of technological change and possible challenges, the EU is committed to strive for a balanced approach… that Europeans can benefit from new technologies developed and functioning according to union values, fundamental rights and principles."* Aside from regulating the UTM and UAS Operators, AI regulation is fundamentally required for AI developers, deployers and users with respect to specific uses of AI. In the UTM context, there are many organisations that have teams of software developers that are currently developing AI through their own risk lens. This directly correlates to an assessment of risk made by that organisation, which may lead to an inconsistent approach to the development of AI when employed to support safe operations in a UTM environment. There are many companies operating today that profess to offer a UTM solution and will, if not already, incorporate some form of AI or ML. There would have been no formal scrutiny of the integrity of such a system. The aim for all stakeholders must be to define common obligatory conditions that apply to the shape and development of AI systems before such systems are sold on the market. UTM has many stakeholders that will use or benefit from AI as shown in Fig1.

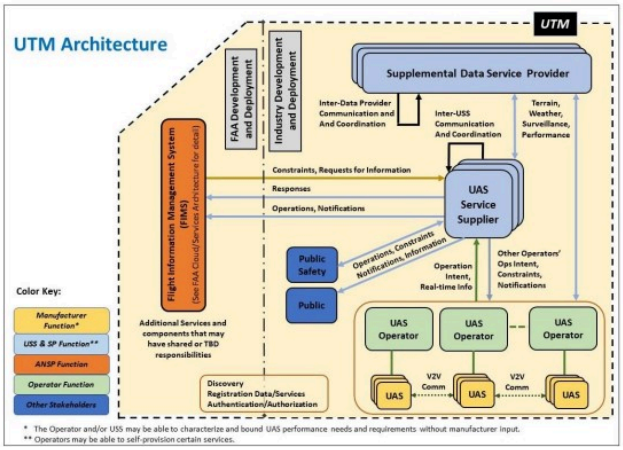

Figure 1 FAA Nominal UTM Architecture [3]

II. EU Artificial Intelligence Act

A. Basis of the EU Act

The European Commission has proposed a legal framework that shall regulate artificial intelligence by virtue of the Artificial Intelligence Act [2]. A legal framework must exist, as AI will not only have a significant impact upon existing laws but will ensure a framework that facilitates safety and the fundamental rights of citizens and businesses with respect to AI. The goal as with any new legislation is to get the balance right between ensuring a user-friendly legal framework is adopted by all stakeholders and the need to build trust, but not stifle innovation and investment.

EASA has not merely acknowledged the implementation, but state that it is part of their AI roadmap [8] for UTM in an urban environment. The EU has developed a risk-based approach to the regulatory framework of AI. This is important so as to establish trust and improve public perception, which has long been an

issue for the business case that relates to the wide adoption of drones in society. The issue is that certain AI systems create risks that must be addressed as it is not always possible to understand why an AI system has made a certain decision and/or prediction. EASA [4],[5] proposes that regulation will:

- address risks specifically created by AI applications;
- propose a list of high-risk applications;
- set clear requirements for AI systems for high risk applications;
- define specific obligations for AI users and providers of high risk applications;
- propose a conformity assessment before the AI system is put into service or placed on the market;
- propose enforcement after such an AI system is placed in the market;
- propose a governance structure at European and national level.

B. *Risk Based Approach*

The proposal seeks to utilise existing regulatory frameworks in a manner that is perceived to be proportionate and necessary by virtue of the adoption of a risk based approach. The EU has defined risks into four categories, namely (i) unacceptable/prohibited risks, (ii) high risks, (iii)limited risks and (iv) minimal risks, as shown in Fig2.

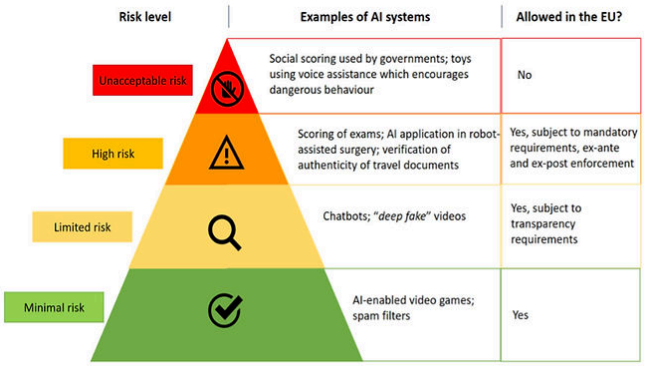

Figure 2 EU Risk Based Approach (source:aipolicyconsulting.com)

III. RISK CATEGORIES

The EU conducted an impact assessment on the proposed legal framework, which attracted a positive opinion on 21 March 2021 [2]. The key aim was to ensure that the EU created the necessary conditions for a trustworthy AI within the EU. Out of four options, the option that ensured a horizontal EU legislative instrument following a proportionate risk-based approach that also included codes of conduct for non-high risk AI systems was preferred. With respect to high-risk systems, the concern was that the legal framework must have requirements that relate specifically to data, documentation and traceability, provision of information and transparency, human oversight and robustness and accuracy. The EU Commission shall establish a system for registering high risk AI applications in a public EU wide database. Such registration will no doubt incur a fee but shall enable multiple stakeholders to verify compliance. Interestingly, AI providers shall be required to provide meaningful information during initial testing and registration, which may be contentious for those with significant intellectual property concerns.

A. *Unacceptable/Prohibited Risks*

The starting point with respect to determining whether or not the AI system is unacceptable is by a comparison with the EU values and fundamental rights. The EU specifically identifies those practices that may have a significant potential to manipulate persons through subliminal techniques beyond their consciousness or exploiting those that are considered vulnerable or cause psychological or physical harm. AI based social scoring is also prohibited, which is a practice that is already in use in China by virtue of utilising facial recognition technology. This technology has already been tested in the UK on a drone in a research environment. The use of such data to identify people in the first instance is subject to data privacy laws, but the further interrogation of data, which is enhanced for facial recognition poses other challenges. Drones can monitor and identify people in crowds, for example, those that are involved in a protest march could then be sanctioned by a public authority. In China, a person that has been found to be jaywalking on a number of occasions is processed by the local authority automatically and is subject to losing social credits. Drones that are used in swarms with such technology could potentially collate substantial data that monitors movement of people and operate with high autonomy. It will be interesting to see how the application of drones using such technology will develop under the banner of law enforcement in order to avoid the unacceptable/prohibited risk tag; more importantly how, if such an exclusion is provided, how a law enforcement decision to use AI in this manner could be subject to judicial review. The AI Act does provide some exclusions for law enforcement on a limited basis.

B. *High Risks*

High risk systems are those that will pose a risk to the health and safety and/or fundamental rights of a natural person(s). In order to be able to operate an AI system in this category, the EU has mandated requirements and a conformity assessment[1] which is aligned to product safety legislation. High risk systems are categorised in two ways:

[1] 'conformity assessment' means the process of verifying whether the requirements set out in Title III, Chapter 2 of this Regulation relating to an AI system have been fulfilled and 'CE marking of conformity' (CE marking) means a marking by which a provider indicates that an AI system is in conformity with the requirements set out in Title III, Chapter 2 of this Regulation and other applicable Union legislation harmonising the conditions for the marketing of products ('Union harmonisation legislation') providing for its affixing;

- AI systems that are intended to be used as a safety component of products that are subject third-party ex-ante conformity assessment.
- Other stand-alone AI systems with mainly fundamental rights implications.

High risk systems include the management and operation of critical infrastructure may include drones although not expressly stated. The requirements for a high-risk system are extensive and contain detail that pertains to requirements for a high-risk AI system that includes a risk management system, data governance, technical documentation, record-keeping, transparency of information for users, human oversight and accuracy, robustness and cybersecurity to name but a few. There are separate obligations for providers of high-risk AI systems that include compliance with the regulation, quality management system, technical documentation, conformity assessments and disclosure to a competent authority. It is therefore a serious consideration for a drone manufacturer or safety component manufacturer that will utilise AI to be aware of both sets of obligations that pertain to the system and the provider. By way of example, a drone manufacturer that has an AI system that has detect and avoid capability and is machine learning (AI Techniques and approaches - (a) Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning; (b) Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems; (c) Statistical approaches, Bayesian estimation, search and optimization methods) could easily fall within the high-risk category due to the safety issues that relate to aviation generally [2],[5]. EASA in their AI Roadmap have scoped the AI taxonomy in Fig 3 that includes ML and AI, but also by extension deep learning.

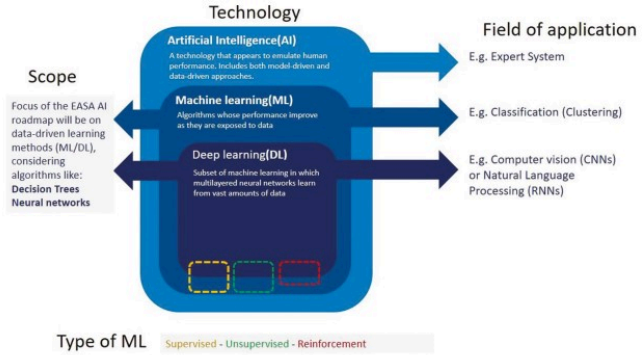

Figure 3 AI Taxonomy EASA AI Roadmap [1]

This aspect of AI will undoubtedly be used with air taxis of the future as each AI system communicates with a UTM system that is also subject to AI and ML utilisation. How will regulation deal with two AI systems that compete on safety where for example there are multiple UTM systems in operation at the same time as EASA intends to make the provision of UTM competitive [6].

The requirement for technical documentation includes a general description of the AI system and a detailed description of the elements of the AI systems and the process of its development. This is referring to unregistered intellectual property such as 'know-how' which is part of an organisations crown jewels that are not easily and/or readily shared with any third party. This includes the system design specifications that refer to the general logic of the AI system and of the algorithms. There is clearly going to be tension with respect to what an organisation is comfortable disclosing to the regulator versus what the regulator requires in order to satisfy conformity assessments. A commercial organisation that fiercely protects their intellectual property will require assurances that their data is safe and secure. Additionally, those companies that provide components or other platforms that contain some form of AI will also be subject to confidentiality provisions within their agreements with customers and would not want to be in breach of contract. The proposed draft legislation is silent on how this can be practically achieved, save for other EU regulations that refer to confidentiality by a member state [7].

C. *Limited Risks*

The EU imposes transparency requirements, much like we see today in relation to providing consent under data protection law when visiting a website. The provider must inform citizens that the citizen is interacting with a machine, e.g., a chatbot. The user should then have the option of not subscribing to use the system.

D. *Minimal Risks*

The EU is under the impression that most AI technology will fall into this bracket of risk and therefore the proposed legislation will not apply as this level of risk will mean that it is negligible or non-existent, such as AI enabled games or spam filters.

IV. USE CASES

Drones are currently using AI in agriculture, construction, mining, forestry and fishing as drones together with robots seek to identify and utilise data to analyse vegetation such as growing of crops, raising and breeding of animals, harvesting timber/minerals and other plants from a farm or their natural habitats. AI is being used in public administration and defence that relate to public order and defence by virtue of the visual data that is used in surveillance, autonomous vehicles and within command, control and communicate domains.

Construction is now also utilising AI in drones on construction sites in order to analyse the construction build programme, civil engineering works and inspections. Quite often the data is collected in real-time and analysed using AI algorithms.

There are many stakeholders that utilise UAS that shall be exposed in some way to AI, as shown in Fig4.

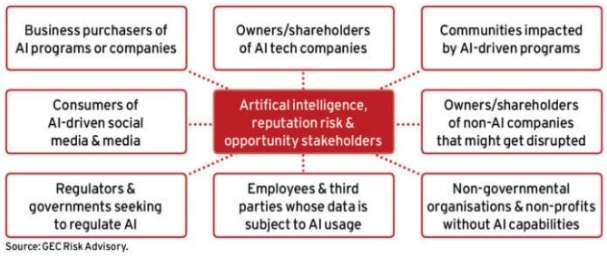

Figure 4 Emerging AI Stakeholders [1]

These use cases shall at some point in the future will have to integrate in a UTM as many platforms will utilise low level airspace and/or transition through it. UTM involves many stakeholders as denoted by the FAA and EASA and will involve some degree of machine learning. It would therefore seem that the integration of many AI technologies would greatly benefit from a sandbox environment whereby AI platforms can be tested in a safe environment before being unleashed onto the wider world. EASA [8] states *"multiple domains of the aviation sector will be impacted by this emerging technology, The air transport system is facing new challenges: increase in air traffic volumes, more stringent environmental standards, growing complexity of systems, greater focus on competitiveness, for which AI could provide opportunities."[8].*

In the USA, the Aviation Rulemaking Committee (ARC) [9] published their final report [9] on 20 March 2022 which makes twenty-three references to autonomy and one reference to artificial intelligence. The case studies referenced included automated flight rules and the application of software. An understanding of the levels of autonomy of the aircraft is required to ensure that the pilot in command can ensure safe operations with other UAS operators in the same airspace. Interestingly, it was outside of the scope of the report to comment upon how autonomous algorithms would be verified and validated, save that this should be proportional to the risk of the operating environment. This poses a number of questions, such as how is the operating environment defined? How does industry ensure that the approach to verification and validation is not fragmented in different local, regional or continental jurisdictions? How is validation of an autonomous algorithm completed and by whom and at what stage?

The EU have stated in their proposed legislation, that should there be a substantial change in the algorithm, then it must be subject to further scrutiny and testing for approval. This is difficult to gauge at the moment as there is no clear path to determine what a variation is to an original algorithm for example. The ultimate aim is to ensure that UAS are safe and that the operations are safer than what is known. The benefits of AI are not fully understood as regulators grapple with adapting existing certification frameworks and basing the development of AI on existing product liability legislation. This may have an impact upon innovation if certainty in legislation cannot be provided as it is difficult to price in risk within a commercial business. Additionally, the regulator is having to deal with operational authorisations in the UK on a case-by-case basis as there is only one pre-defined risk assessment that has been adopted from the EU which is inefficient and slow. The added burden of attempting to assess autonomy within a UAS system adds complexity to what is already an inefficient process. The direct impact on the industry is further delay and expense which stifles innovation as commercial businesses are unable to sustain indefinite operations based upon an uncertain regulatory outcome.

Whilst the regulators, to some extent in some jurisdictions are developing at a more expedient pace than others, such as the EU with the AI Act, the USA with the draft Algorithmic Accountability Act (AAA) [10], other jurisdictions are slow to follow. This could be for many reasons such as a lack of expertise, lack of funding and possibly just waiting for more mature regulators to tackle the issues and adopt their legislation. However, technological development progresses at a quick pace and continue to secure funding for its development, such as Shield AI[11] by building AI pilots for aircraft in the defence sector [11]. AI pilots are seen as a disruptive player in this marketplace with an ambition to develop intelligent swarming. The range of software applications in terms of development opens up many market opportunities and transferable technologies into the commercial sector, as Shield AI state [11] *"Shield AI's Hivemind software is an AI pilot for military and commercial aircraft that enables intelligent teams of aircraft to perform missions ranging from room clearance, to penetrating air defense systems, and dogfighting F-16s. Hivemind employs state-of-the-art algorithms for planning, mapping, and state-estimation to enable aircraft to execute dynamic flight maneuvers and uses reinforcement learning for discovery, learning, and execution of winning tactics and strategies. On aircraft, Hivemind enables full autonomy and is designed to run fully on the edge, disconnected from the cloud, in high threat, GPS and communication-degraded environments."*

In order to form regulation that is comprehensive, it is often useful to promulgate a strategy. The UK MOD published their strategy on 15 June 2022 [12], which acknowledges that the is no single overall owner for AI in the UK Defence space, but that all business units and functions have a part to play in its development. The UK Defence AI and Autonomy Unit (DAU) and the Defence AI Centre (DAIC) will manage the AI strategy jointly. The DAU shall set out the policy frameworks governing development, adoption and use of AI. This means that the DAU will be important in informing regulators as to the shape and function.

In defence, the DAIC and other agencies shall [11] *"establish a comprehensive framework for the testing, assurance, certification and regulation of the AI-enabled systems, both the human and the technical component of human machine teams."* It is also more importantly recognised that through machine learning, the AI system will have to be tested throughout its lifetime. What is fundamental with respect to testing is understanding the frequency of testing that is required in order to make a determination as to whether or not there should be human in the loop, a human on the loop or a human outside of the loop. It is arguable, that some organisations will approach testing in a naïve manner as they will use existing methodologies to begin with, without actually establishing relevant AI specific issues and challenges. In essence, the framework of testing may well be out of date, as shown in Fig 5. The consequence of such lack of information is increased risk that relates to safety critical components and/or systems. The EU has sought to address this issue to some extent by

making such testing mandatory and failure to do so may incur a financial penalty, not unlike what we have seen as a result of data breaches under EU General Data Protection Regulations.

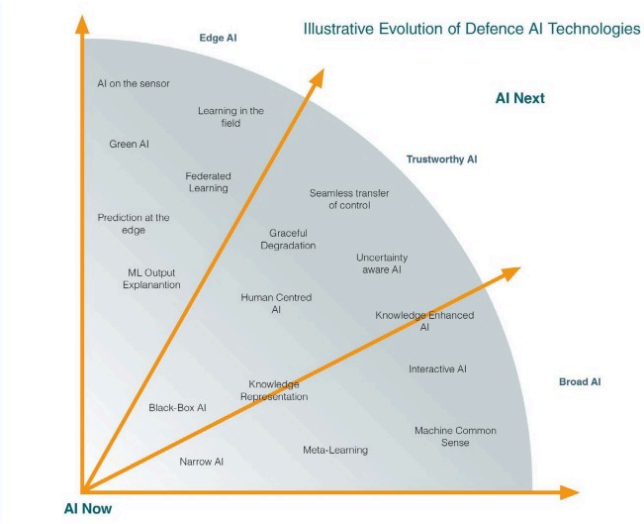

Figure 5 Evolution of Defence AI Technologies

Evolution of AI technologies will be subject to some form of testing and assessment regime. This includes the disclosure of intellectual property, which may prove controversial in some jurisdictions, but not in others. Commercially sensitive information may not be shared with a regulator as there may be a lack of trust with respect to how confidential and proprietary information is handled. The lack of information sharing may well be detrimental to achieving regulation that is well thought through and balanced. The end game is about trust, all stakeholders must have trust in an AI system that is safe, reliable, lawful and ethical. Future scenarios incorporate a trust broker that operates between a new technological application and the end user. The trust broker assists with compliance.[14]

V. CONCLUSION

Those organisations that establish clear principles for risk management and compliance with respect to AI development will become more trusted by the regulator. A clear demonstration of intent together with a practical explanation of the constituent parts of an AI system adopting principles that include intellectual property disclosure that is safe in a high-risk category will garnish some favour with the regulator. Organisations will therefore be able to continue to develop AI once legislation is in the statute books. The EU AI Act is an extensive draft of legislation that will enable stakeholders to become more informed about how to engage and comply with AI, as well as understand the sanctions for non-compliance. This is helpful to business as the risk of non-compliance can be appropriately assessed and mitigated by transparency with the regulator when developing an AI system. UTM is developing at pace with the adoption of autonomy and AI amongst many of the different stakeholders within a UTM system. The layered approach and governance of such a system is high-risk because of the threat to life should a UAS fall out of the sky over an urban environment. It will clearly take some time for legislation to be enacted in different parts of the world, which may inevitably lead to a fragmented approach. This could be difficult if different rules apply as a UAS traverses between two different jurisdictions. A common approach to AI regulation similar to what ICAO has achieved with respect to manned aviation could be a good starting point, but only to the extent that AI and autonomy applies to UAS.

[1]. European Union Aviation Safety Agency (EASA), "USSP's," 22 July 2021. [Online]. Available: https://www.easa.europa.eu/newsroom-and-events/events/what-are-ussps-needs-aircraft-be-electronically-conspicuous-u-space. [Accessed 17 June 2022].

[2]. European Commission, "REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE," 21 April 2021. [Online]. Available: https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF. [Accessed 17 June 2022].

[3]. Federal Aviation Administration (FAA), "Concept of Operations V2.0," 2 March 2020. [Online]. Available: https://www.faa.gov/uas/research_development/traffic_management/media/UTM_ConOps_v2.pdf. [Accessed 17 June 2022].

[4]. European Parliament, "EU Legislation in Progress," January 2022. [Online]. Available:https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf. [Accessed 17 June 2022].

[5]. European Commission, "ANNEXES to the Proposal for a Regulation of the European Parliament and of the Council LAYING DOWN HARMONISEDRULES ON ARTIFICIAL INTELLIGENCE," 21 April 2021. [Online]. Available: file:///C:/Users/User/OneDrive/Documents/PhD/dasc/AI/AI%20proposed%20legislation%20annexes.pdf. [Accessed 17 June 2022].

[6]. European Aviation Safety Agency (EASA) , "EASA U-Space proposals require competitors to exchange tracking data," Unmanned Airspace, 4 July 2019. [Online]. Available: https://www.unmannedairspace.info/uncategorized/easa-u-space-proposals-require-competitors-to-exchange-tracking-data/. [Accessed 17 June 2022].

[7]. Ethical Boardroom, "AI and reputational risk: An ESG perspective," GEC Risk Advisory, Spring 2018. [Online]. Available: https://ethicalboardroom.com/ai-and-reputational-risk-an-esg-perspective/. [Accessed 17 June 2022].

[8]. European Union Aviation Safety Agency, "Artifical Intelligence Roadmap A human-centric approach," EASA, February 2020. [Online]. Available:https://www.easa.europa.eu/downloads/109668/en. [Accessed 17 June 2022].

[9]. Federal Aviation Administration Aviation Rulemaking Committee, “UNMANNED AIRCRAFT SYSTEMS BEYOND VISUAL LINE OF SIGHT AVIATION RULEMAKING COMMITTEE,” 10 March 2022. [Online]. Available: https://www.faa.gov/regulations_policies/rulemaking/committees/documents/media/UAS_BVLOS_ARC_FINAL_REPORT_03102022.pdf. [Accessed 17 June 2022].

[10]. U. S. R. Wyden, “Legislation Requires Assessment of Critical Algorithms and New Public Disclosures; Bill Endorsed by AI Experts and Advocates;BillWill Set the Stage For Future Oversight by Agencies and Lawmakers,” 3 February 2022. [Online]. Available: https://www.wyden.senate.gov/news/press-releases/wyden-booker-and-clarke-introduce-algorithmic-accountability-act-of-2022-to-require-new-transparency-and-accountability-for-automated-decision-systems. [Accessed 17 June 2022].

[11]. SUAS News, “Shield AI Raises $165M Series E to Accelerate Building of the World’s Best AI Pilot,” 10 June 2022. [Online]. Available: https://www.suasnews.com/2022/06/shield-ai-raises-165m-series-e-to-accelerate-building-of-the-worlds-best-ai-pilot/. [Accessed 17 June 2022].

[12]. UK Ministry of Defence, “Defence Artificial Intelligence Strategy,” 15 June 2022. [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1082416/Defence_Artificial_Intelligence_Strategy.pdf. [Accessed 17 June 2022].

[13]. R. Ryan, S. Al-Rubaye, G. Braithwaite and D. Panagiotakopoulos, "The Legal Framework of UTM for UAS," *2020 AIAA/IEEE 39th Digital Avionics Systems Conference (DASC)*, 2020, pp. 1-5, doi: 10.1109/DASC50938.2020.9256577.

[14]. Li, Chen & Guo, Weisi & Sun, Chengyao & Alrubaye, Saba & Tsourdous, Antonios. (2020). Trustworthy Deep Learning in 6G-Enabled Mass Autonomy: From Concept to Quality-of-Trust Key Performance Indicators. IEEE Vehicular Technology Magazine.

UTM regulatory concerns with machine learning and artificial intelligence

Ryan, Richard

2022-10-31

Ryan R, Al-Rubaye S, Braithwaite G. (2022) UTM regulatory concerns with machine learning and artificial intelligence. In: 2022 IEEE/AIAA 41st Digital Avionics Systems Conference (DASC), Portsmouth, 18-22 September 2022, Virginia, USA

https://doi.org/10.1109/DASC55683.2022.9925869