Augmenting Autonomous Agents with Expert-Derived Decision Policies

Tanya Sarah Paul
Thales Digital Solutions Inc.
1405 boulevard du Parc-Technologique, Quebec, Qc G1P 4P5 Canada
CANADA

tanya.paul@thalesgroup.com

Stephanie Allogba
Thales Digital Solutions Inc.
6650 Street Saint-Urbain, office 350, Montreal, Qc H2S 3G9
CANADA

stephanie.allogba@thalesgroup.com

Filipe Carvalhais Sanches
Thales Digital Solutions Inc.
6650 Street Saint-Urbain, office 350, Montreal, Qc H2S 3G9
CANADA

filipe.carvalhaissanches@thalesdigital.io

Jean-Sebastien Thivierge
Thales Digital Solutions Inc.
1405 boulevard du Parc-Technologique, Quebec, Qc G1P 4P5 Canada
CANADA

jean-sebastien.thivierge@thalesgroup.com

Daniel Lafond
Thales Digital Solutions Inc.
1405 boulevard du Parc-Technologique, Quebec, Qc G1P 4P5 Canada
CANADA

daniel.lafond@thalesgroup.com

Antoine Fagette
Thales Digital Solutions Inc.
6650 Street Saint-Urbain, office 350, Montreal, Qc H2S 3G9
CANADA

antoine.fagette@thalesgroup.com

ABSTRACT

The architecture of Unmanned Aerial Vehicles (UAV) is composed of several key components to optimize their efficiency as well as their operability in critical contexts such as in air combat or air surveillance applications. Our research work implements an innovative human expert-derived assessment policy into autonomous collaborative agents for determining the threat level of an UAV. Our objective is therefore to use a cognitive engineering technique called policy capturing to configure an operational threat assessment capability that is aligned with human cognition. This consists of the following two steps. The first step is the integration of a cognitive modelling system into the autonomous agents. This provides recommendations and warnings concerning the threat level assessment based on previous decisions of the experts. It may thus present capabilities of transparency and explainability using real decision-making patterns extracted from human reasoning. In other words, this cognitive modelling system helps make explicit some of the implicit elements in expert decision-making. Additionally, a multi-model approach was adopted and deployed using seven simultaneous supervised machines learning algorithms to predict the threat levels by mimicking expert decisions without being subject to fatigue, stress or distraction. These algorithms are based on enhanced and fine-tuned python scikit-learn modules: Logistic Regression (LR), Decision Tree (DT), K-nearest neighbours (KNN), Multi-layer perceptron neural network (MLPNN), Naive Bayes (NB), Support Vector Classifiers (SVC), as well as Random Forest (RF). The second step consists in transmitting the response provided by the expert policy to the situation awareness module of the autonomous agents. To accomplish it, we perform a fusion of the threat level identified by the expert policy and the initial threat level already identified in the autonomous agent. To achieve this objective, a simulated environment was used to provide a use case of critical asset protection. This use case is composed of four threat levels, ranging from criminal intent to clueless. The solution attempts to maximize the neutralization rate of 'real' threats by managing or prioritizing the number of target drones to be tracked and neutralized according to their threat level. In other words, the defensive swarm of drones prioritizes its response by first addressing the criminal profiles, aiming for neutralization with the highest priority, continuing with careless and then clueless profiles. The defensive swarm adopts a "watchdog" behaviour, adapting to the sudden change in the threat level, for example, when any threat approaches too close to a protected area. It is important to mention that, without the expert policy, all enemy drones are considered equally threatening, and no priority is given, leading to a greater risk of not neutralizing the actual threats. Directions for future work include investigating how to improve human-autonomy teaming through mutual understanding and anticipation capabilities enabled through online learning and explainable AI methods. Furthermore, another potentially disruptive capability enabled by this method could be for a swarm of drones to learn to anticipate online the behaviour patterns of adversary drones to adapt on the fly and achieve cognitive air superiority.

1.0 INTRODUCTION

The development of autonomous system has been perceived as a tool to enhance the efficiency and, performance of human operators, helping reduce the workload, stress and errors made by humans [1]. The rise of autonomous collaborative agents has engendered a major shift within the field of surveillance and reconnaissance [2]. A common mis-conception is that that such collaborative autonomous agents will replace humans or eliminate human error. The automation paradox refers to the notion that in fact it can trigger new types of errors and new types of issues such as the deterioration of human skills and performance due to the abuse of automation [3]. Additionally, being able to trust autonomous systems has often been an issue especially in the field of defence and security, where it is often mandatory to keep humans in the loop. However, this raises issues such as "false-reassurance of human in the loop" where humans are often given the role of supervisors monitoring very complex fully autonomous systems, yet resulting in loss of situational awareness (SA) or even decrease in the overall implication of humans even if they still require to validate or give certain commands to the systems. SA is not only crucial to human performance but as well a challenge in autonomous systems and in cases of human-autonomy teaming.

1.1 Team Situational Awareness (TSA)

TSA is a key component of teaming performance. It can be described as "knowing what is going on around you" and being cognizant of how to understand interpret and extract information about the environment [4]. SA also relates to some of the human biases when it comes to decision-making such as: i) attentional narrowing/tunnelling; ii) memory shortage; iii) workload, fatigue, stress, reaction time; iv) data overload; v) maladaptive mental models (eg., non-logical reasoning or inappropriate behaviour); vi) disuse or abuse of automated systems [5, 6]. Herein, we are particularly interested in the challenge of enabling effective situation assessment by artificial agents controlling unmanned aircraft [5]. In this research we develop a new potential method offering decision support not only to humans but also to autonomous systems, which could help maintain high levels of SA within the application of collaborative autonomous UAV systems.

1.2 Situational Awareness and Human-Automation Teaming of UAV

Human-autonomy teaming (HAT) refers to the ability between human and automated systems to be able to coordinate and collaborate interdependently towards a common task or goal [5]. Lack of SA in both humans and machines could be detrimental to the performance of the team. Studies on military use of unmanned systems found that 33% of mishaps were caused directly by humans, and that 67% were due to issues with the machine [8]. Other statistics from U.S. Department of Defense claim that human error contributes to 20-70% of UAS mishaps in the military [9]. Those metrics vary based on the HAT however common patterns of error in humans: skill-based, procedural, checklist, inadequate operations or the over or under-control over its autonomous systems versus machines tend to fail within the set-up, monitoring, failure of detection and diagnosis [8]. Researchers have demonstrated that mixed initiative target identification where an automated agent provides assistance in locating potential targets in a visual search space actually deteriorated performance consistently over time [10]. They suggest that automated agents who are trained to detect particular stimuli may not perform as well as an alert human [10]. Therefore, it is important when designing HAT frameworks to explore methods of reducing risks, increasing safety and reliability based on each agent's limitations and strengths. Autonomous systems face major trust challenges in terms of explainability as sometimes it is often difficult for such systems to provide reliable, understandable information to assure adequate cooperation and collaboration [11]. Lacking awareness and understanding of the automated agent would only reinforce the out of-the loop phenomenon [12].

1.3 Objectives

We present a prototype solution aimed at allowing artificial agents to learn from human experts how to assess a given type of situation. The use case selected for this study consists in threat assessment in a counter-drone scenario for critical asset protection. This proof-of-concept investigation constitutes a first step in a cognitive systems engineering (CSE) research endeavour aimed at iteratively testing and improving HAT capabilities using human-in-the-loop synthetic testing environment. The CSE approach focuses on enhancing the human ability to understand and control systems and, often plays a key role in developing adaptive/intelligent/learning frameworks [13]. While past work has advanced adjustable autonomy methods for human-UAV collaboration [13, 14, 15, 16, 17], adaptability has been mostly based on the environment, use-case and objectives of the mission (e.g., varying the number of UAVs per operator) [14]. However, no studies have yet demonstrated this adjustability through the use of expert modelling for transferring situation assessment policies to artificial agents to enhance system autonomy and HAT collaboration capacity. In this paper we present the proposed framework in Section 2, our use case application of threat detection in Section 3, the method in Section 4, results in Section 5 and conclusions in Section 6.

2.0 FRAMEWORK AND ARHICTCETURE: EXPERT MODELING & AUTONOMOUS AGENTS

The new solution investigated here combines the use of an AI-based decision-support system called Cognitive Shadow (shadowing of the expert and automatically learning from observed decisions/behaviour patterns; [18, 19]) with Synergetic Partners with AI-Reinforced IQ (SPARQ) a platform for implementation and optimization of collaborative autonomous systems. Both systems are merged into a joint capability resulting in a framework where human operator(s) and autonomous agents can engage in joint learning, coordinate and share information. This HAT enables agents to collaborate towards a joint mission, and reflects complementary adaptive frameworks for mission management with high level of autonomy [17].

2.1 SPARQ

SPARQ is an AI Agent solution capable of working in synergy with human operators and of creating complex multi-function collaborative platforms. SPARQ enables the development, deployment and testing of multi-agent use cases, where other agents can be either artificial or human. It allows humans and AI agents to work together toward a common goal through the use of its associated teaming framework. SPARQ is composed of three major component within its "Digital Twin": i) Awareness capabilities involving the representation and understanding of the AI agent of the current situation and its history, using sensors and simulation models; ii) Anticipation capabilities involving the ability to forecast how the current situation may unfold based on what-if scenarios; iii) Decision capabilities involving the ability to come up with a plan of action based on the inputs from the awareness and anticipation modules. This system has been implemented and tested using real hardware or operating systems such as a UAV fleet, ground control stations and smart sensors. It enables to have organized teams in swarms. These AI-powered systems can carry out complex and diverse missions autonomously, thanks to their ability adapt and reconfigure in real-time.

2.2 Cognitive Shadow

Cognitive Shadow enables the automatic modelling of expert decision and behaviour patterns using a state-of-the-art policy capturing methodology combining multiple supervised machine learning algorithms [20-21]. Such expert-derived cognitive models support a process called judgmental bootstrapping, where models tend to be more reliable than humans because those models are not subject to fatigue, stress, distraction and mental overload [22, 23]. This effect was repeatedly observed using Cognitive Shadow leading to the successful reductions of error rates ranging between 4% and 36% [22-24]. Integrating Cognitive Shadow within SPARQ allows for the personalization of decision-support systems to enable teamed partners (automated agent and human pilot or operator) to get real-time recommendation while optimizing the mission performance. In addition, it allows for the prioritization of information based on the expert-policy and allows extracting contextual information requirements. It keeps humans in the loop of autonomous agent decisions in two ways: i) The use of an AI-algorithm trained on human expert(s), ii) real-time suggestions and interaction [25]. The approach supports explainability and transparency as each decision is based on human expertise and understanding. It offers support not only to humans in challenging error-prone conditions but also to autonomous collaborative agents such as a swarm of drones.

3.0 THREAT CLASSIFICATION

The use-case selected for this investigation focuses on enhancing homeland security using UAV systems by detecting threats surrounding a protected facility. The use of a digital-twin UAV architecture has been a significant step foward for situation monitoring and anomaly detection to enhance security [27].

3.1 Threat Detection Types

Threat assessment is heavily reliant on the context and the situations. In this study we are focusing on UAV-counter measures for the protection of a restricted area. It is important to consider the different types of possible threats within the environment, in order mimic and replicate the reality of their occurrences. The type of threat is often based on the different uses of UAVs such as civilian, terrorist, military or criminal use [26]. Examples of malicious use from a terrorist could be surveillance or suicidal drone, versus a considerate use for civilians could be for disaster response, tourist use and cinematography, aids & supplies, or even commercial ads [26]. However, other research has focused on different types of threats such as Hacking, spoofing, jamming, malware infection hardware attacking [26, 27]. For the present use-case we relied on past work on threat level assessment to determine the threat levels and factors [28].

3.2 Existing Methods of UAV-Threat Assessment

Diverse threat assessment and detection techniques have been researched. One approach focuses on malicious intent of non-cooperative drone surveillance with final destination estimation [29]. Others use rule-based intrusion detection which is developed by defining the types of attacks of concern and implementing them as such “reckless”, “random”, “opportunistic attack”, allowing the minimization of detection error including false positive and false negative rates. However, this method often remains simplistic and is not able to recognize unknown types of attacks [26]. Methods might vary based on the prioritization of certain sensors such as acoustic detection, motion or camera detection, thermal detection and radar detection [8]. Across those methods the threat assessment process remains essentially the same. It is composed of: i) a detection phase involving the ability to identify an entity; ii) discrimination, meaning the ability to accept some input patterns and reject others; iii) a classification step based for example on the types of aircraft (fighters versus bombers), iv) a recognition step about the different types or levels of threats; and v) identification of the types of action required in response.

3.4 Threat Assessment Algorithm & Features

The deployment of intelligence and HAT platforms can improve homeland security and safety of missions where SA is considered a major component of tactical superiority and tactical trajectory planning for multi-aircraft missions [28]. One of the most popular methods to leverage threat assessment with AI has been through Bayesian Network Models. An example in [28] has demonstrated the feasibility of this approach using four event nodes: i) types of recognition (eg., radar imaging, electronic, infrared, or visible light imaging reconnaissance; ii) topographic features (eg., data of the terrain and geomorphic features of the enemy’s weapons location); iii) weather types (eg., visibility of sky); iv) electromagnetic environment (EE), eg., radiation, probability of being detected by the enemy equipment. Such features could help assess the level of threat or probability of detecting malicious UAVs. Similarly, [30] demonstrated the need for dynamic Bayesian network and Markov decision processes for tactical UAV decision-making in HAT scenarios. This work also highlighted how expert commanders conduct assessments such as reasoning and decision-making on how/where/when to deploy available resources in order to increase probability of survivability and accomplishment of the given mission [30]. This was combined with features such as target type, weapon type, affiliation (friend, enemy, neural or unknown), distance to the entity of interest, detection radius, weapon range, speed, direction, and type of terrain. They have encoded such features in into rule-based models to assess the classification. Other work in [31] demonstrated the use of a support-decision-making support system for UAV threats. It uses fused knowledge-based and sensor-based classification performance in order to classify threat levels. They tested three strategies i) Velocity-based rules using purely the change of acceleration spread through four classes, where acceleration is an indicator of risk; ii) Distance from the protected facility; and iii) velocity and velocity-change pattern categorised within 5 levels. [32] used dynamic Bayesian Network model, using similar features. However based on domain expert knowledge, they added vehicles types and characteristics: bombardment aircraft need to dive to medium height to make pinpoint bombing, electronic jammers and early warning aircraft are often at high altitudes

[32]. Lastly, [33] used Bayesian Network used the types of EE (military, civilian, no emission), radar type (civilian, military), jammer (on vs off), as well as mission type (reconnaissance, commercial light, illegal flight, other) and, speed (subsonic, transonic, supersonic, hypersonic).

4.0 METHODS

4.1 Experts

The first step of the pipeline was generating interviews on four experts. We interviewed three experts in the field of Aerospace and Navigation from Thales Land and Air Systems, as well as Thales Canada Defense & Security, Royal Canadian Mounted Police experts in counter UAV. A fourth expert was a fighter jet pilot. The experts helped provide feedback on the scenario and helped validate inputs for expert policy modelling. In addition to expert feedback, we drew from the previous research listed above in order to ensure that the proof-of-concept study was based on realistic assumptions.

4.2 Simulation and UAV

This study involved using AI agents and simulated enemy UAV which needed to be neutralized based on the defined use-case and experts feedback. Each simulated UAV represented a quadrotor drone provided and developed by Autonomous Robotic Aviation (ARA). In order to train our HAT we used SE-STAR simulator [34] which enables us to develop counter-UAV simulation scenarios. This allowed simulating the different threat levels using a customizable terrain with specific dimensions of the land and zone to protect. The simulation involves blue agents (the defence team), red drones (threats to assess), the ground control station and radars. By connecting SPARQ to the drone simulator we can simulate interaction between the drone and the environment (i.e., simulated sensing and physics). The setup provides a testbed for our HAT teaming framework with expert policy model. Through this implementation, it enables us to have a dynamic environment and the possibility of human-in-the-loop interaction. It also allows generating training and testing data, situational awareness metrics and teaming performance. Such simulated tests can help find potential gaps, dysfunctions and fallacies within our framework and policy, which need to be addressed prior to subsequent field testing stages.

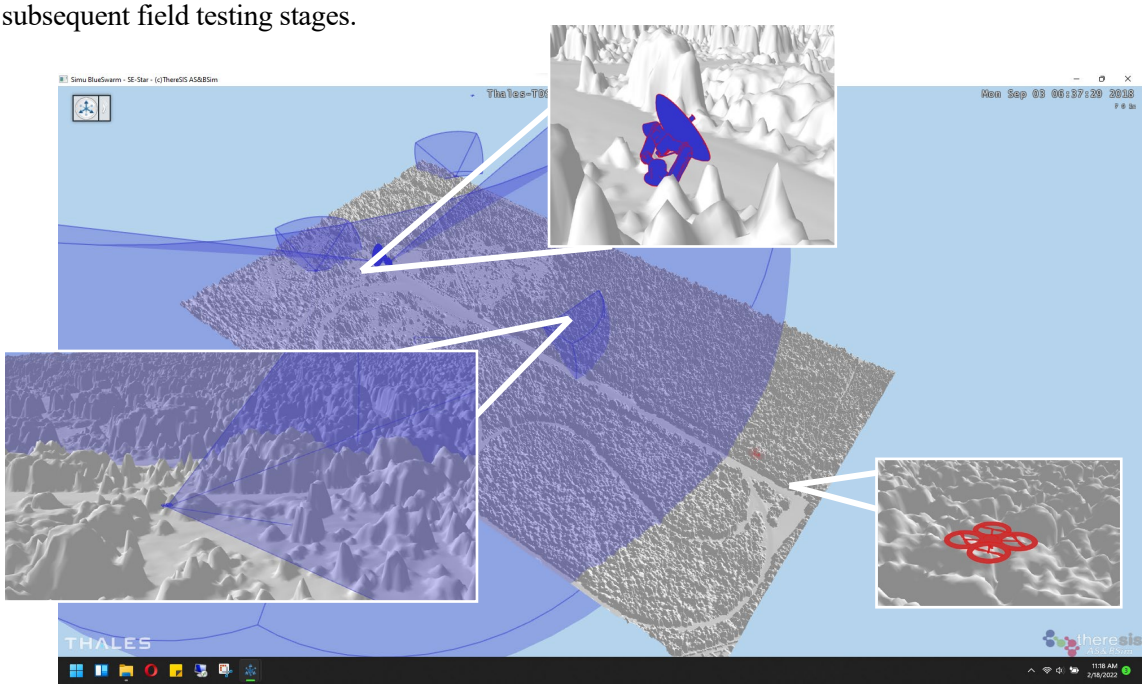

Figure 1: SE-STAR Simulation demonstrating the red and blue force, and ground control station.

4.1.1 Use-Cases

Following the interviews and feedback with experts, we extracted four different types of behavioural threat levels. They correspond to four UAV user profiles often found within the context of restricted zone protection. The four levels are labelled as Clueless, Careless, Criminal No Harm and Criminal with Harm. Each of these categories is described within Table 1.

Table 1: Threat Levels Classification

Threat Levels	Definition
Clueless	A UAV is a Beyond Visual Line of Sight (BVLOS) hobbyist testing their drone without any knowledge about airspace.
Careless	A UAV considered a supply delivery drone whose flight plan has been defined without consideration of the restricted airspace.
Criminal No Harm	A UAV navigated by a curious photographer getting closer to the restricted area to take pictures.
Criminal with Harm	Is a UAV terrorist-operated drone with an explosive payload. UAV reduces its altitude while approaching its final target.

The four behaviours are then analysed with respect to a division of the terrain of three zones: Restricted Zone, Buffer Zone and the Detection Zone as illustrated in Figure 2. Using this simplified representation of the surrounding terrain we were able to conceptualize and generate different types of profiling behavioural patterns mapped to each of our Threat Levels. The important part of this method is that the dimensions of each of the zones are mapped onto our simulated environment SE-STAR to ensure the continuity and application of the parameters and configuration as a realistic environment.

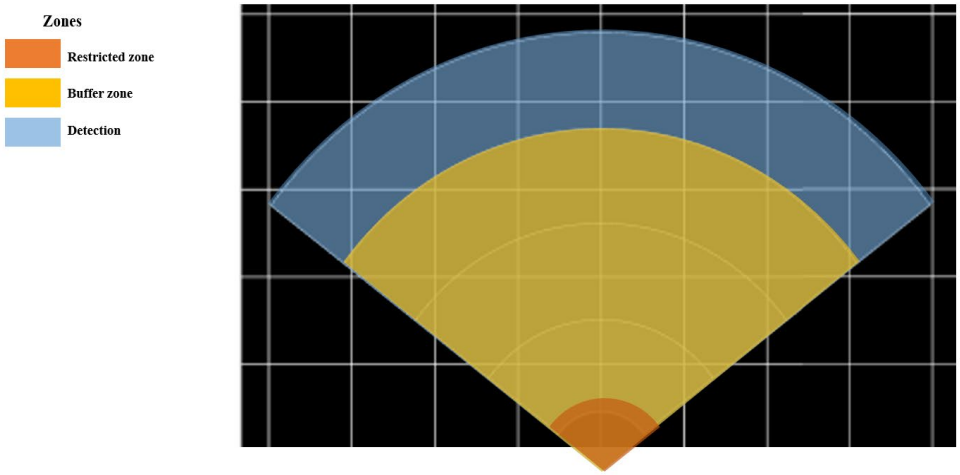

Figure 2: Zone delimitations (Detection, Buffer, Restricted zone).

4.2 Model Pipeline

The general pipeline of this threat detection algorithm can be broken down into several steps. The first step was the computational representation of the threat identification process such as recognition, classification based on literature review and expert interviews and feedback. That step allowed formalizing the features

used during the threat assessment of experts, and enabled modelling the environment and real-time computation of those features. Once the features and variables were selected, we then proceeded with extracting the relevant features from the Digital Twin component in SPARQ. The digital twin then engenders a process called State Mapping which is part of the Situational Awareness module of SPARQ. It enables pre-processing and feature engineering from raw to interpretable data. This allows the feature values to be transmitted to Cognitive Shadow for expert-model for training and testing.

4.2.1 Digital Twin and State Mapper

Digital Twin's component enables information collection from its SA module through sensors. It is composed of over twenty elements such as the timestamp of each first and last observation, the name of the entity, the types of alliance, altitude, position, heading, velocity, uncertainty, sensors available, as well as the zone within which the entity is located. In order to select the most relevant feature needed for the application of the situation assessment policy, we have certain requirements and restrictions. The primary feature, which enables filtering the data input to the threat assessment policy, is based on the type of detection "EntityType" (drone, bird, unknown). Secondly, the feature selection requirement is based on allegiance: friend, enemy, neutral or unknown. The feature transformation process is known as the State Mapper which collects the relevant information and transforms it into interpretable features. The State Mapper enables the drone to track information about the environment, which is then used to understand, decide and act. Table 2 summaries the list of features used in this study.

Table 2: Digital State Mapper Features.

Features	Definition	Feature Engineering	Encoded
Speed	The velocity of the drone measured in m/s.	[Low, Medium, High]	[0,1,2]
Altitude	Position of the UAV with respect to the ground.	[Low, Medium, High]	[0,1,2]
Direction Azimuth	Angular position with respect to the restricted area.	[Right, Left, Front, Rear]	[0,1,2]
Zone	The zone within which the UAV is currently positioned.	[World, Buffer, Restriction]	[0,1,2,3]
Direction Elevation	Angular position with respect to restricted area	[Up, Level, Down]	[0,1,2]
Acceleration	The acceleration of the UAV	[High, Medium, Low Deceleration, None, High, Medium, Low Acceleration]	[-3,-2,-1,0,1,2,3]
Distance	The distance of the red UAV from the restricted zone.	[Very Far, Far, Close, Very Close]	[0,1,2,3]
Past Threat Levels	The previous classification based on the expert policy.	[Clueless, Careless, Criminal No Harm, Criminal with Harm]	[0,1,2,3]

Each of these features is also associated to time –n which means that the SA enables keeping a memory of previous instances mapped to previous classifications.

4.3.1 Training and Modelling

The first step once we have the features selected and expert policy defined is to be able to prepare the dataset for training and testing. We used stratified sampling to identify the right criteria for online training, model optimization and cross-validation will be based on. Cognitive Shadow simultaneously trained multiple supervised machine learning algorithms and selected the best model in terms of proportion of correct classifications on the 10 held-out data samples in a standard 10-fold cross validation procedure.

4.3.1.1 Supervised Learning Algorithms

Cognitive Shadow enables the training and testing of seven different algorithms: Naïve Bayes, Decision Tree, K-nearest neighbors, Support vector machine, Logistic Regression, Feedforward Neural network, Random Forest. During the training process, Cognitive Shadow also performs hyper-parameter tuning using a randomized search called RandomizedSearchCV (using Scikit-Learn library). Parameters are sampled through a list of values as it reduces cost of computationally heavy process compared to traditional exhaustive grid search method. A 10-fold cross-validation splitting strategy is performed in the evaluation process of the different hyper-parameter settings. The training data is split into ten groups as for the hyper-parameter selection and model evaluation. This then leads to the section of the best estimator. In order to prevent overfitting, we implemented a second 10-fold cross-validation loop with fixed hyper-parameters. At each of the 10 iterations, the confusion matrices is computed for the validation (test) subset. Then the precision, recall and F1-score are calculated from the validation (test) confusion matrices.

5.0 RESULTS AND DISCUSSION

5.1 Model Performance

In order to analyse the results, it is ideal to ensure we have balanced classes (types of threats). Our synthetic training data was composed of 22% of Clueless, 22% of Careless while having 28% CriminalNoHarm, and 28% of CriminalWithHarm (totalling 716 instances post-label distribution). For the seven supervised machine-learning models, results in terms of predictive accuracy from best to worst are: decision-tree model (100%), support vector machine (99.72%), neural network (98.32%), random forest (98.04%), K-Nearest Neighbours (97.91%), logistic regression (89.38%), and Naïve Bayes (65.78%).

Training time was also tracked which informs that the worst model required the shortest time of (4.52 seconds) compared to the support vector machine which required the most time (over 2 minutes). Figure 3 shows the results for each of model in terms of accuracy based on the 10-fold cross-validation, training time, total sample count, and prediction accuracy per class.

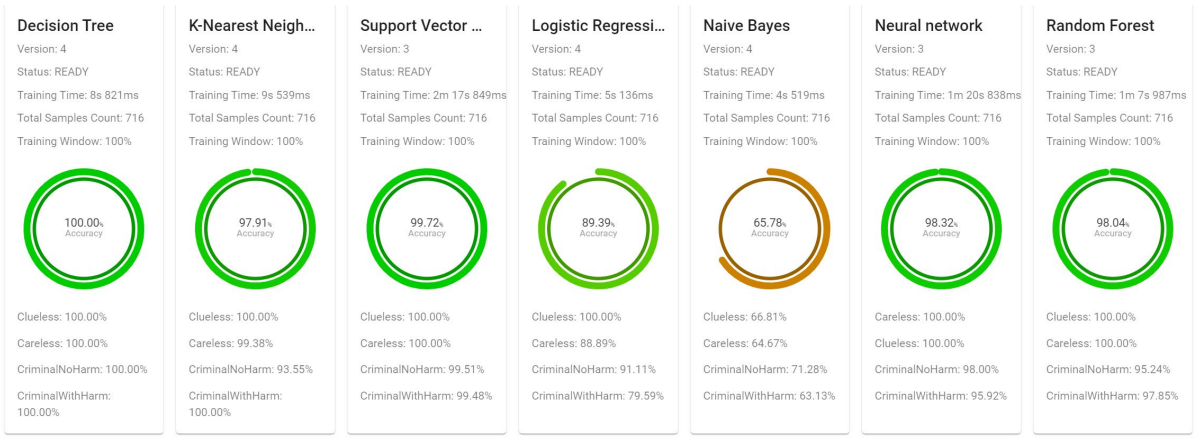

Figure 3: Results of Cognitive Shadow Model on Threat Detection on the four possible classes.

Based on the analysis of model performance per class we note that the class which was the hardest to predict is CriminalNoHarm. This can be explained as it is the critical line between not harmful and very dangerous behaviour which might entail neutralization. This is often one of the biggest challenges for the operator to know when to pull the trigger. Additionally, it is difficult as some harmful behaviour might mask their harmful intention until the last minute, which is hard to detect in advance.

We have also assessed the precision, recall and F-1 score for each category to ensure the model kept high accuracy across all types of classification. Through this analysis, we notice an overall higher accuracy for Threat Level 1 and Threat Level 2 (the lower threat levels). However, the decision-tree model is the only one which remained consistent across all classes with a predictive accuracy of 100%.

5.1.1 Application Real-Time Implementation CS and SPARQ

Once the full machine-learning pipeline was developed from State Mapper to Cognitive Shadow, we were able to test scenarios in real time. In order to do this we replicated and simulated enemy drones behaving in similar ways within SE-STAR. This enabled us to mimic our behaviour of interest to test our machine learning model. The trials demonstrated the feasibility of our real-time processing pipeline from SPARQ to Cognitive Shadow, and vice-versa, verifying that the expert-policy was properly executed. The output of this model enabled augmenting the autonomous systems with human-derived comprehension and the potential for extending this capapility to the projection module. This enabled the UAVs to make appropriate decisions about how to behave according to threat level: watch-dog, stand-by or neutralization actions.

5.2 Limitations

There are several limitations to this first proof-of concept HAT framework. One limitation is the incapability of recognizing other types of behavioural patterns outside of the knowledge of the expert. This means our model will not be able to recognize other types of attacks or profiling types, if they do not match one of the four current classes. Thus, if confronted with a new scenario or unseen or unrecognizable scenario by the expert, the model is at risk of misclassification or may even dismiss certain types of disguised behaviour, thus requiring humans-in-the-loop to better handle novelty. Additionally, based on our pipeline we rely on a chain of action and information processing where if one information is misclassified it could delay or even falsify the algorithm results. For example, if the computer vision classifies an observed entity as a bird incorrectly, it will result in a miss and the information will be wrongly filtered out without being considered by the threat detection algorithm. Similar challenges of video or camera-based detection have been raised previously [16]. Certain methods of disguise have already been implemented such as dove drones or bird look-a likes [24]. Additionally, similar consequences will arise if the drone is misclassified as a friend. In this work we developed a simplified threat assessment model for initial testing and HAT implementation through expert modelling. However, more complex behaviour patterns and features could be considered such as aircraft types, and being able to recognize payload types (eg., explosives) or being able to track trajectory patterns overtime (zigzag, linear, etc.). The simplified ground truth generation rules and feature set used herein could have made it easier to achieve the high levels of accuracy observed in this study. Lastly, cognitive modelling remains a major challenge as different experts might have different knowledge and judgment strategies.

5.1.1 Future Improvements

Future work will focus on the implementation of additional environmental features to represent the dynamically changing features, which will be fed into the UAV sensors such as light variation, time of the day, or weather modification that might affect the possibility to detect and perceive accurately. Another next step is to capture a larger range of profiling behaviours and integrate them within the existing four levels of threats. This might include taking into consideration different types of malicious UAV but also harmless behaviors such as search and rescue. Ultimately, this prototype solution will be deployed and tested in real-

life using physical blue and red forces drones. This is an important step toward implementing an adjustable human autonomy collaboration capability which are capable of high task accuracy even in complex open environments. Furthermore, another potentially disruptive capability enabled by this method could be for a swarm of drones to learn to anticipate online the behaviour patterns of adversary drones to adapt on the fly and achieve cognitive air superiority.

6.0 CONCLUSION

This research investigated the feasibility of integrating an automatic policy capturing capability into an AI agent framework. An expert-policy for threat assessment in a counter-drone scenario was derived and tested both offline and online. This combined capability is seen as a first step towards enabling a human-AI co-learning process for HAT in the context of UAV missions and beyond. This framework could enhance trustworthiness by enabling faster and more robust situation assessments, with experts in the loop providing feedback to their AI counterparts (and vice-versa). This is a step toward achieving human-AI co-learning capabilities where both the automated agents as well as human experts are able to learn together and get to familiarize with the behaviour and capabilities of their teammates to better adjust to new challenges and enhance teaming performance during pre-operation, in-operation and post-operation phases. Capturing human cognitive and behaviour patterns in this way may also help improve HAT by allowing AI agents to anticipate human actions and therefore better know when and what to communicate and to coordinate explicitly or even implicitly like highly trained human teams typically do thanks to their accurate team mental models [36].

7.0 REFERENCES

[1] CCDC Army Research Laboratory, "Multimodal Physiological and Behavioral Measures to Estimate Human States and Decisions for Improved Human Autonomy Teaming," *apps.dtic.mil*, Oct. 02, 2020. https://apps.dtic.mil/sti/citations/AD1111968#:~:text=This%20provides%20a%20foundation%20to%20employ%20a%20priori (accessed Sep. 05, 2023).

[2] C. Wang, Y. Su, J. Wang, T. Wang, and Q. Gao, "UAVSwarm Dataset: An Unmanned Aerial Vehicle Swarm Dataset for Multiple Object Tracking," *Remote Sensing*, vol. 14, no. 11, p. 2601, May 2022, doi: https://doi.org/10.3390/rs14112601

[3] Australian Goverment, "Safety behaviours: human factors for pilots," *Civil Aviation Safety Authority*, Jun. 14, 2021. https://www.casa.gov.au/sites/default/files/2021-06/safety-behaviours-human-factor-for-pilots-10-design-automation.pdf

[4] M. R. Endsley and D. J. Garland, *Situation Awareness Analysis and Measurement*. Informa, 2000. doi: https://doi.org/10.1201/b12461

[5] M. R. Endsley and E. S. Connors, "Situation awareness: State of the art," *2008 IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century*, Jul. 2008, doi: https://doi.org/10.1109/pes.2008.4596937

[6] A. Munir, A. Aved, and E. Blasch, "Situational Awareness: Techniques, Challenges, and Prospects," *AI*, vol. 3, no. 1, pp. 55–77, Mar. 2022, doi: https://doi.org/10.3390/ai3010005

[7] T. Elmokadem and A. V. Savkin, "Towards Fully Autonomous UAVs: A Survey," *Sensors*, vol. 21, no. 18, p. 6223, Jan. 2021, doi: https://doi.org/10.3390/s21186223

[8] S. Giese, D. Carr, and J. Chahl, "Implications for unmanned systems research of military UAV mishap statistics," *IEEE Xplore*, Jun. 01, 2013. https://ieeexplore.ieee.org/abstract/document/6629628 (accessed Sep. 05, 2023).

[9] A. P. Tvaryanas, W. T. Thompson, and S. H. Constable, "Human factors in remotely piloted aircraft operations: HFACS analysis of 221 mishaps over 10 years," *Aviation, Space, and Environmental Medicine*, vol. 77, no. 7, pp. 724–732, Jul. 2006, Accessed: Sep. 05, 2023. [Online]. Available: https://pubmed.ncbi.nlm.nih.gov/16856358/

[10] M. Demir, A. D. Likens, N. J. Cooke, P. G. Amazeen, and N. J. McNeese, "Team Coordination and Effectiveness in Human-Autonomy Teaming," *IEEE Transactions on Human-Machine Systems*, vol. 49, no. 2, pp. 150–159, Apr. 2019, doi: https://doi.org/10.1109/thms.2018.2877482

[11] G. Soudain, "EASA Artificial Intelligence concept paper (proposed Issue 2) open for consultation," *EASA*, Feb. 24, 2023. https://www.easa.europa.eu/en/newsroom-and-events/news/easa-artificial-intelligence-concept-paper-proposed-issue-2-open

[12] J. Mccarley and C. Wickens, "Human Factors of UAVs 1 Human Factors Implications of UAVs in the National Airspace," 2005. Accessed: Sep. 05, 2023. [Online]. Available: https://www.tc.faa.gov/logistics/Grants/pdf/2004/04-G-032.pdf

[13] J. Lundberg, M. Arvola, and K. L. Palmerius, "Human Autonomy in Future Drone Traffic: Joint Human–AI Control in Temporal Cognitive Work," *Frontiers in Artificial Intelligence*, vol. 4, Jul. 2021, doi: https://doi.org/10.3389/frai.2021.704082

[14] Z. Zhao, C. Wang, Y. Niu, L. Shen, Z. Ma, and L. Wu, "Adjustable Autonomy for Human-UAVs Collaborative Searching Using Fuzzy Cognitive Maps," *IEEE Xplore*, Sep. 01, 2019. https://ieeexplore.ieee.org/abstract/document/8901937/ (accessed Aug. 29, 2022).

[15] L. Huang *et al.*, "Human-Autonomy Teaming: Interaction Metrics and Models for Next Generation Combat Vehicle Concepts," *apps.dtic.mil*, Aug. 2020, Accessed: Sep. 05, 2023. [Online]. Available: https://apps.dtic.mil/sti/citations/trecms/AD1109144

[16] M. Johnson, J. M. Bradshaw, P. J. Feltovich, C. M. Jonker, M. B. Van Riemsdijk, and M. Sierhuis, "Coactive Design: Designing Support for Interdependence in Joint Activity," *Journal of Human-Robot Interaction*, vol. 3, no. 1, p. 43, Mar. 2014, doi: https://doi.org/10.5898/jhri.3.1.johnson

[17] S. Schwerd and A. Schulte, "Operator State Estimation to Enable Adaptive Assistance in Manned-Unmanned-Teaming," *Cognitive Systems Research*, Jan. 2021, doi: https://doi.org/10.1016/j.cogsys.2021.01.002.

[18] D. Lafond, K. Labonté, A. Hunter, H. F. Neyedli, and S. Tremblay, "Judgment Analysis for Real-Time Decision Support Using the Cognitive Shadow Policy-Capturing System," *Advances in Intelligent Systems and Computing*, pp. 78–83, Jul. 2019, doi: https://doi.org/10.1007/978-3-030-25629-6_13

[19] T. Ahram, R. Taiar, S. Colson, and A. Choplin, Eds., *Human Interaction and Emerging Technologies*. Cham: Springer International Publishing, 2020. doi: https://doi.org/10.1007/978-3-030-25629-6

[20] K. Nokes and G. P. Hodgkinson, "Policy-capturing: An ingenious technique for exploring the cognitive bases of work-related decisions," *research.manchester.ac.uk*, 2018. https://research.manchester.ac.uk/en/publications/policy-capturing-an-ingenious-technique-for-exploring-the-cogniti (accessed Sep. 09, 2023).

[21] A. Marois, D. Lafond, A. Audouy, H. Boronat, and P. Mazoyer, "Policy Capturing to Support Pilot Decision-Making," *Aviation Psychology and Applied Human Factors*, Feb. 2023, doi: https://doi.org/10.1027/2192-0923/a000237

[22] J. S. Armstrong, "Judgmental Bootstrapping: Inferring Experts' Rules for Forecasting," *International Series in Operations Research & Management Science*, pp. 171–192, 2001, doi: https://doi.org/10.1007/978-0-306-47630-3_9

[23] L. Salvan, A. Marois, B. Chatelais, D. Lafond, and A. Audouy, "Pilots' decision-making during unstabilized approaches: Group-level policy capturing for cognitive assistance," 2022. Accessed: Sep. 09, 2023. [Online]. Available: https://events.isae-supaero.fr/event/14/contributions/388/attachments/53/91/ICCAS2022_Salvan_et_al_extended_abstract.pdf

[24] K. Labonté, D. Lafond, A. Hunter, H. F. Neyedli, and S. Tremblay, "Comparing Two Decision Support Modes Using the Cognitive Shadow Online Policy-Capturing System," *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, vol. 64, no. 1, pp. 1125–1129, Dec. 2020, doi: https://doi.org/10.1177/1071181320641270

[25] A. Marois, K. Labonté, D. Lafond, H. F. Neyedli, and S. Tremblay, "Cognitive and Behavioral Impacts of Two Decision-Support Modes for Judgmental Bootstrapping," *Journal of Cognitive Engineering and Decision Making*, p. 155534342311533, Feb. 2023, doi: https://doi.org/10.1177/15553434231153311

[26] J.-P. Yaacoub and O. Salman, "Security Analysis of Drones Systems: Attacks, Limitations, and Recommendations," *Internet of Things*, vol. 11, no. 100218, p. 100218, May 2020, doi: https://doi.org/10.1016/j.iot.2020.100218

[27] B. Fraser, S. Al-Rubaye, S. Aslam, and A. Tsourdos, "Enhancing the Security of Unmanned Aerial Systems using Digital-Twin Technology and Intrusion Detection," *IEEE Xplore*, Oct. 01, 2021. https://ieeexplore.ieee.org/document/9594321 (accessed Sep. 05, 2023).

[28] X. Wang *et al.*, "Research on Artificial Potential Field Route Planning Method Based on Threat Level Assessment," *IEEE Xplore*, May 01, 2021. https://ieeexplore.ieee.org/document/9601634 (accessed Sep. 05, 2023).

[29] J. Liang, B. I. Ahmad, M. Jahangir, and S. Godsill, "Detection of Malicious Intent in Non-cooperative Drone Surveillance," *IEEE Xplore*, Sep. 01, 2021. https://ieeexplore.ieee.org/document/9541485 (accessed Sep. 05, 2023).

[30] M. Frey, J. Attmanspacher, and A. Schulte, "A Dynamic Bayesian Network and Markov Decision Process for Tactical UAV Decision Making in MUM-T Scenarios," *IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA)*, Jun. 2022, doi: https://doi.org/10.1109/cogsima54611.2022.9830690

[31] Y. Ko, K. E. Ho, M. Lee, and E. T. Matson, "UAV Threat Level Assessment based on the Velocity and Distance from Collision," *IEEE Xplore*, Nov. 01, 2020. https://ieeexplore.ieee.org/document/9287915 (accessed Sep. 05, 2023).

[32] Y. Wang, Y. Sun, J.-Y. Li, and S.-T. Xia, "Air defense threat assessment based on dynamic Bayesian network," *IEEE Xplore*, May 01, 2012. https://ieeexplore.ieee.org/document/6223112 (accessed Sep. 05, 2023).

[33] J. F. Basso Brancalion and K. H. Kienitz, "Threat Evaluation of Aerial Targets in an Air Defense System Using Bayesian Networks," *IEEE Xplore*, Nov. 01, 2017. https://ieeexplore.ieee.org/document/8328495 (accessed Sep. 05, 2023).

[34] L. Navarro, F. Flacher, and C. Meyer, "SE-Star: A Large-Scale Human Behavior Simulation for Planning, Decision-Making and Training," *Semantic Scholar*, May 04, 2015. https://www.semanticscholar.org/paper/SE-Star:-A-Large-Scale-Human-Behavior-Simulation-Navarro-Flacher/7b0f1f6a47e5e6c7f3305aee45dc66c4fa6de866 (accessed Sep. 09, 2023).

[35] W. Yang, L. Wang, and B. Song, "Dove: A biomimetic flapping-wing micro air vehicle," *International Journal of Micro Air Vehicles*, vol. 10, no. 1, pp. 70–84, Oct. 2017, doi: https://doi.org/10.1177/1756829317734837

[36] K. Stowers, L. L. Brady, C. MacLellan, R. Wohleber, and E. Salas, "Improving Teamwork Competencies in Human-Machine Teams: Perspectives From Team Science," *Frontiers in Psychology*, vol. 12, May 2021, doi: https://doi.org/10.3389/fpsyg.2021.590290