

MANNED-UNMANNED TEAMING (MUM-T): HOW FAR CAN I TRUST MY TEAM MEMBER AND ON WHAT IS THIS TRUST BASED?

Laura Samsó Pericón*

We are living a thriving moment in history, not only because everything is going exponential in terms of human development and technology, but because it could and will change how cross-domain/sector systems inter operate, communicate, how missions are ran and how decisions are taken and executed to achieve tactical superiority in the defense domain or, better performance, in commercial applications.

Autonomy propels interconnected systems, but the AI frontier introduces also a symbiotic blend of human and machine capabilities. This manifests as AI-driven Manned-Unmanned Teaming (MUM-T), leveraging Human-Machine Teaming and neuro interfaces. The core is the collaboration of human operators and autonomous drones, forging tactical supremacy. Fusing human intuition with AI precision enhances target identification and engagement. The core is the collaboration of human operators and autonomous drones, forging tactical supremacy. Fusing human intuition with AI precision enhances target identification and engagement.

In this evolving landscape, the integration of MUM-T systems has emerged as a pivotal paradigm. The paper delves into the dynamic realm of AI and Human-Machine Teaming enabled MUM-T uncrewed systems, encompassing innovative tactics, cutting-edge stealth technologies, wearable innovations, novel materials, advancement in sensor fusion, swarming intelligence and the transformative influence of exponential technologies such as Brain-Computer Interfaces (BCI) – neuro-interfaces, augmented reality and quantum technologies to name a few.

MUM-T systems have ushered a new era of commercial and defense capabilities, but they also bring forth a host of challenges and vulnerabilities that demand careful consideration. Those range from interoperability complexity, cybersecurity and vulnerability, Electronic Warfare (EW) threats, quantum technologies, ethical and legal concerns, operational concepts, Human-Machine Interfaces (HMI), training and skills, situational complexity, public perception and acceptance, reliability and redundancy.

This paper will show the state of art of MUM-T and it will also elucidate, through a use case, the pivotal role of a holistic approach in orchestrating the coordination between these elements, the challenges and vulnerabilities of integrating an HMI and AI enabled MUM-T capabilities in joint multi domain operation.

* R&D Cyberdrones, laurasamso.com

INTRODUCTION

“Can you really trust Artificial Intelligence (AI)?”, this is one of the topics the experts discussed about during one of the sessions in the Annual World Economic Forum (WEF) meeting back in January 2024. If we go further into the details: How far can I trust my Team member and on what is this trust based?

A new geopolitical balance is undergoing across the world, testing the strengths and weaknesses of our societies and, at the same time, it offers a battleground for new technologies.

We are in the path of a major transformation in many ways, leveraged by the rise of new developments and its acceptance by the society, from workforce to logistic chains, economic challenges to how wars are fought.

The recent conflicts around the globe have seen an increasing military expenditure by countries worldwide, with rising needs for intelligence, surveillance, and reconnaissance (ISR) operations, analysis and autonomy; integrating manned and unmanned systems into all aspects of warfare and using AI as the glue for all those operations. But not only this, we are in the brink of a major leap, the symbiosis of human-machine in the realm of warfare.

Back to the initial question, when it comes to trust. On what is this trust based when human and machine team to enhance battlefield performance? How to ensure officers trust AI decisions and how to ensure the decision taken by the Human-Machine Teaming (HMT) is not the result of a hacking event? Both questions are slightly different but come to a convergence in the sense that both questions require analyzing human-human teaming into the realms of sociology and psychology (cognitive realm).

To really understand what an autonomous system, HMT in this case, is doing, it is not enough just to observe what the platforms are doing, but to really understand and have a view of the different transparent stages of the decision-making process. It is also key to know which are the components of a MUM-T ecosystem, so to be aware of the weak points that could be used to gain advantage of whole system. With that, an “AI behavior issue” could be isolated and contained, at best.

Uncertainty in contested environments adds another layer of complexity that only transparency between autonomous system and humans can ensure an effective way to exchange between them.

When it comes to MUM-T systems, there are few definitions, such as those real-world applications that involve one or more human and machine elements in which each is capable of some degree of autonomous actions, but their overall goal is shared and thus, some degree of cooperation is also assumed (Reference 1).

But how is it possible for this type of systems to work?

Autonomy and AI propel Human-Machine Teaming (HMT) and MUM-T operations, together with other secondary components or technologies such as stealth, wearables, communications to name a few.

The paper uses the definition provided by NATO where it defines it as a system that decides and acts to accomplish desired goals, within defined parameters, based on acquired knowledge and evolving situational awareness, following an optimal but potentially unpredictable course of action.

The system’s operator defines its parameters and objectives, but the system directs itself via artificial intelligence (AI). In the case of uncrewed aerial systems, an autonomous drone can

communicate, reroute, and make decisions based on the data it gathers about its environment, eliminating the need for continual human operation. Applying autonomy to a network of drones also enables drone swarming, allowing for the drone network to execute missions as a single, focused entity.

As it is mentioned in the Blueprint for Autonomy publication, the autonomous future is composed by five foundational building blocks: motivation, technology, airworthiness, operations, and integration.

In these type of MUM-T systems and scenarios, where the blend with human and machine offer so much performance operations enhancement, but also weak points, could your team member betray you? And would you have the means to spot it and up to what point?

The following sections will give the reader an overview about MUM-T ecosystem, its advantages and threats and how trust between MUM-T arena could be build.

MUM-T: THE NEW BATTELFIELD ARENA

MUM-T can be described as a cross dimensional arena, expanding current capabilities, providing a new combat strategy, planning and a collaborative environment. The United States Army Aviation Centre (USAACE) defines MUM-T as “*The synchronized employment of soldier, manned and unmanned air and ground vehicles robotics, and sensors to achieve situational understanding, greater lethality, and improved survivability*” (Reference 2).

Other bodies such the IEEE defined MUM-T as the “*coordinated use of manned and unmanned systems to achieve a common goal*”. (Reference 3).

A high level MUM-T architecture is composed by different dimensions such as air, ground, sea and space in the future.

Given several facts such as the increase of different types of unmanned systems being used in different domains and that every nation design and procures UAS (Unmanned Aircraft Systems) themselves, interoperability needs to be ensured between the different NATO community platforms and systems.

This may enhance decision-making and mission effectiveness, offering new different tactical chances which could make a difference in the development of future strategies.

Table 1. Levels of Interoperability (NATO’s STANAG 4586).

Level 1 Indirect receipt of UA-related data
Level 2 Direct receipt of ISR/other data where ‘direct’ covers reception of the UA data by the UCS when it has direct communication with the UA
Level 3 Control and monitoring of the UA payload in addition to direct receipt of ISR/other data
Level 4 Control and Monitoring of the UA, less launch and recovery.
Level 5 Control and Monitoring of the UA (Level 4), plus launch and recovery functions.

MUM-T configurations will offer different scenarios with advantages and capabilities and will also have an impact in the level of trust assumed. In this basic scenarios different usages could be envisaged such a small platform can be utilized to send sensor data to the manned aircraft or to some other node of the ecosystem, to deliver weaponry, when in coupling mode with a manned aircraft it could be used as a decoy. At the same time, the different nodes can launch attacks through different means overwhelming or confusing the defense opponent systems.

Apart of all the technological constraints, human factors and risks posed by MUM-T applications will become prominent when designing and developing the future aircrafts, manned or unmanned. The pilots/crew workload will be under stress in those type of scenarios and it is important to design not to exceed the human limits but also thinking in how AI can leverage that and which information in an HMI operations will be shared between human-machine and how decisions will be taken according to that.

OPERATION ENABLERS: TECHNOLOGY ADVANCEMENTS

We are currently at the brink of another exponential technology leap, where several advances are already converging into a major step, where reality and augmentation barriers become blurry.

AI and autonomy will revolutionize how wars are fought, symbiosis between humans and machines will become common, new sensors, novel materials and developments in stealth technologies will improve the survivability and operability rates; and quantum communications and processing will achieve the next leap.(Reference 10), (Reference 11).

But as advances are positive to grow as a society they normally come with drawbacks. In that case, all these enablers will be and are prone to be influenced, posing a risk/threat not only to the sole MUM-T operation but also to the civilians.

In addition, pilot (human) decisions whether to trust the AI companion or not, could also become influenced by parameters such the type of operation, the possible damage that would cause. But then, as a second derivative, are they able to detect and assess a misbehavior from the AI if it would be hacked/influenced?

Cognitive neuroscience of human decision making takes special relevance and AI will ensure speed in decision making as it analyzes all the information going through, but then the trust dilemma will appear.

Find below different of those operation enablers.

Stealth Technology

The beginning of stealth technology can be traced back to the Cold War era, when the US military recognized the need of this capability in order to penetrate enemy defenses undetected.

Petr Ufimtsev, a Soviet physicist, is considered the father behind the stealth technology. In 1962 he published the paper Method of Edge Waves in the Physical Theory of Diffraction, where he described the mathematical rationale for the development of those technologies. In the 1970s, his work was translated and reused in the US to produce the first operations stealth combat aircrafts, the Lockheed F-117 fighter and the Northrop B-2 Spirit strategic bomber.

There key principles that govern the design and implementation of stealth technology are focused in reducing the detectability of the platforms by radar, infrared, visual and other sensors.

Shape and Geometry

The Radar Cross Section (RCS) is a measure of how detectable an object is by radar. Stealth technology aims to minimize the RCS by using special materials and shaping techniques that scatter or absorb radar waves.

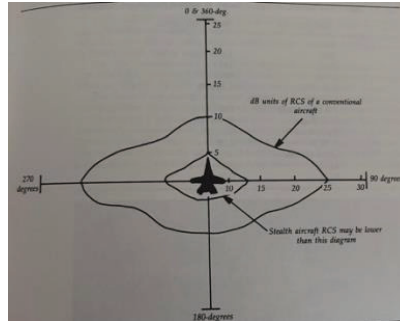


Figure 1. Airplanes Radar Cross Section (RCS).

Noise reduction: Stealth design aimed to minimize noise emissions making them harder to be detected by acoustic sensors.

Signature reduction: Design that uses special coating, absorbing paints, and materials together with techniques to reduce reflections and scattering of electromagnetic waves.

Sensor Fusion and Electronic countermeasures: Stealth vehicles employ various electronic countermeasures to confuse or jam opponent radar and communication systems.

Stealth technology could be applied to the different domains: airborne platforms, naval vessels and ground vehicles.

Wearables in the Battlespace

Another layer is the soldier wearables and portable military technologies that enhance physical capabilities, help in communications with the command centers, keep situational awareness, reducing risks in the battlefield and also monitoring their health.

As new technologies emerge and NATO countries increase their investments, the global soldier wearable technology market size is expected to reach US\$ 3.77 billion in 2033. The market is projected to reach US\$ 3.77 billion by 2033, with a growth rate (CAGR) of 1.8% during 2024-2033.

Those technologies range from exoskeletons, smart textiles, night vision technologies, biometric monitoring devices, communications equipment, navigation and GPS devices, and tech-fused armor.

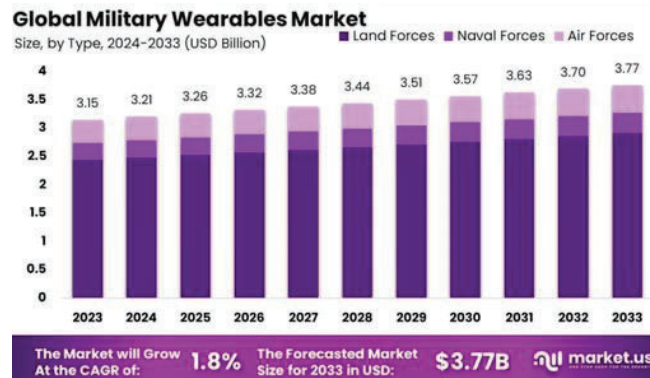


Figure 2. Military Wearables Market.

These are also used to identify soldiers and track their movements, analyze data from different sources, and share information about their surroundings, including maps, enemy positions, and mission objectives in real time with the different team members from the different dimensions, not only on ground.

Other Technology Enablers

Recent geopolitical events together with the low cost of COTS are democratizing more and more the use of uncrewed aerial systems during those conflicts in the form of swarm of drones to attack the enemy. Those drones could be used to overwhelm the defense capacities (as a decoy) and also to attack.

Those platforms are equipped with different sensors together with AI for autonomous navigation and obstacle avoidance. Sensors can be such E/O cameras, radar, LiDAR, IR. AI algorithms process this data in real-time, allowing drones to detect and avoid obstacles, navigate complex environments, and plan optimal flight paths.

Computer Vision and Object Recognition: Autonomous drones rely on computer vision techniques and object recognition algorithms to interpret visual data captured by their cameras.

Machine Learning and Deep Learning: This empowers drones to make precise, real-time decisions based on the data they collect.

Swarm Intelligence: Autonomous drones can operate collectively in swarms.

Sensor Fusion: Autonomous drones integrate data from a myriad of sensors, using sensor fusion techniques.

Automated Mission Planning and Execution: possess the capability to autonomously devise and execute missions based on predefined objectives.

Energy Efficiency and Autonomy: AI algorithms aid in optimizing energy consumption, enabling drones to undertake tasks for longer durations without frequent recharging.

Safety and Collision Avoidance: Ensuring safety is paramount in autonomous drone operations. AI-driven collision avoidance systems to identify and evade potential collisions with other drones, aircraft, or obstacles.

HUMAN-MACHINE TEAMING

Teaming is defined as a collective action targeted to reach supposedly joint and shared objectives. It is normally defined as a “distinguishable set of two or more people who interact dynamically, interdependently, and adaptively towards a common and valued goal/objective/mission, who have each been assigned specific roles of functions to perform, and who have a limited life-span membership” (Reference 2).

Human brain has 86 billion neurons and according to some studies (Reference 14) we do not use it to the full potential. A telepathic conversation with your manned-unmanned team members will be soon a reality in the war arena. As Former Deputy Secretary of Defense Robert Work, who led DoD’s 3rd offset, summarized trends with military technology as follows:

The coin of the realm during the Cold War was armored brigades, mechanized infantry brigades, multiple launch rocket system battalions, self-propelled artillery battalions, tactical fighter squadrons, among others. Now, the coin of the realm is going to be learning machines and human-machine collaborations, which allows machines to allow humans to make better decisions; assisted human operations, which means bringing the power of the network to the individual; human-machine combat teaming; and the autonomous network. (Reference 4).

The first developments took place approximately 40 years ago: this technology is capable of reading brain activity and decipher thoughts to carry out man-machine interaction tasks. Tasks that ranged from controlling devices such as a wheelchair up to medical interventions for cognitive rehabilitation. In the last 10 years, some of this research has become available to the public through different companies that have developed wearable, comfortable and accessible brain sensing devices that start to be part of our daily lives.(Reference 13).

Many predict the singularity is coming closer and some even have already a date in mind: between 2025 and 2030. It is expected a convergence between biotechnology and other technologies such holographic, visual devices, AI.

Human-Machine Interface (HMI) techniques use bioelectrical signals to gain real-time synchronized communication between the human body and machine functioning. Research has proved that this technology permits the simultaneous control of multiple functions, UAS sensors and platforms in that case, improve the speed of communication and enhance common situational awareness.

Since at least 2007, the military have been researching what it is called “synthetic telepathy” (Reference 5) type of non-invasive Brain Computer Interfaces (BCI) to be used by the warfighters.

In 2012, DARPA issued a \$4 million grant to build a non-invasive “synthetic telepathy” interface by placing sensors close to the brain’s motor centers to pick up electrical signals — non-invasively, over the skin.

Three years later, a paralyzed woman was able to steer virtually an F-35 with an implantable small microchip; and later another person was able to also receive signals from the simulated aircraft. Brain signals can be used to command and control various types of aircrafts.

Elon Musk’s Neuralink, recently became a reality and the first person to receive is currently under study. Those Brain-Computer Interfaces (BCI) are considered the initial step towards the “singularity”, melding human and machine. As BCIs transitions from basic research to a more operational and commercial applications it will be important to lay the basis for regulations and policies (Reference 6).

Ongoing R&D efforts include many dimensions of technology, in particular, there is an increasing focus on human-machine collaboration for improved decision making, including human-computer interaction (HCI) and cognitive teaming, assisted-human operations, swarm control and operation, and advanced manned and unmanned combat teaming.

All these new developments will come with associated vulnerabilities and risks, and ethical and legal responsibilities. In particular, cyber threats will show new points of failure, adversary access to information and new areas of exposure, manipulate, deceive or harm the rest of the team members. HMI technology will be transformative during combat and reconnaissance operations but capabilities will depend largely on its fidelity and reliability during those operations. How far you can trust your team members and what is this trust based on will be a key for future successful operations.

Future R&D on this topic must work towards integrating AI & human cognitive models, advance human-agent feedback loops, optimize trust/transparency, and advance sensor/data decision model.

TRUST AND TRANSPARENCY OPTIMIZATION AMONG MUM-T TEAM MEMBERS

As humans and machines will collaborate cognitively and think together, new challenges from merging AI, autonomy and HMI technologies will arise and form a new set of vulnerabilities. Trust or lack of it is one of those and it will be key for the success of the missions (Reference 7).

When humans build trust while working for common goals or in social interaction, uncertainty is reduced, stress levels go down and the likelihood to be successful in whatever endeavor they work it, is increased. At the same time, humans spend less cognitive resources to deal with the topic.

Trust in AI and its effects could also be compared to the infancy steps of unmanned aircrafts, where an accident could have damaged the whole efforts in order to launch the market of services and applications. A small AI error with catastrophic results could jeopardize public acceptance. With that in mind, a stepped approach towards trusting AI and its interaction with humans must be put in place.

In the context of AI, trust refers to the decision to use a technology based on the perception that it will reliably perform as expected in pursuit of shared goals (Reference 3).

Cyber-attacks will put not only technology but trust in general on the spot. Several types of trust issues could arise: deficit of trust in HMI technology, deficit of trust on the decisions taken by the different team members once human-machine system works together and the general threat of cyber-attacks.

Trust issues between the different team members such as potential erosion of unit cohesion, unit leadership among other critical interpersonal and inter platforms relationships will arise with unknown consequences.

How could we approach those trust issues?

One topic is the technology itself that the operator has to trust in. If not, any outcome of this technology will be doubted.

Another one, how to trust the final decision taken by the symbiosis of human-machine interaction? Layering the decisions taken through cognitive methods could be one way to segregate and go through a process of intention analysis.

An overall prerequisite would be to have effective cyber measures in place to safe guard the involved technological systems and the final result of the operation.

When humans take decisions they do it based in different thoughts such: How critical it is? Do we have time to decide? Is it life endangering? Will there be collateral damage? Who else in the chain will be impacted? How important is to have success here? Do we need to follow the rules? How public will perceive that? Could this endanger our relations with other nations?

Based on that above, humans may trust less or more the AI to take over in each scenario or situation. So it can be envisaged that in a mixed operation, trust in AI can vary ranging from pilot in the loop to fully autonomous.

In addition, once the pilot decides to trust the AI; relying in one AI only may not be enough to ensure operations will be risk free. As many security organizations have such the policy, it may be needed also to have a main AI umbrella that would make sure the secondary AI is not misbehaving due to an overtake by a nefarious attack.

ENTANGLED CYBERWAR AND AI TRUSTWORTHINESS

Soon manned and unmanned fighters will jointly cooperate in real scenarios leveraged by AI and HMIs teaming capabilities. The recent conflict with Israel and Iran is a perfect example on how a swarm of drones were used to overwhelm the defense capabilities of Israel, to distract them. Once the system collapsed, long range missiles were launched by Iran over Israel targets.

Not so far in the future, we can envisage an expanded scenario containing all the elements commented in the sections above.

We will analyze the following use case that is elaborated in more detail in my presentation:

Imagine a joint multi domain mission where different nations work together, having all of them different human-machine teams and connected not only to their concrete AI, but to a global AI that would make sure the mission is successful. It will be also important to define what attributes make a mission “successful”, so the AI will make sure it is keeping the operatives safe.

A unit is sending a team with one or several loyal wingmen unmanned aircraft to assess the enemy forces and send advance information to the rest of the unit, requesting additional resources if required and attack.

The use case describes a scenario in a highly contested environments characterizing current military missions, where uncertainty is high and new threats appear, making it difficult to assess a conflict situation. In order to generate a response, the commander is required to make assumptions and inferences. At some point there are so many and they come so quick that a human cannot properly process and handle them.

There is also uncertainty whether a situation will develop into a wider conflict or not, so decisions need to be taken into the same moment it happens.

Humans find it difficult to accept uncertainty, acting on pretended knowledge which may lead to overconfidence, accepting risks that they would not if they would really understand the situation.

Military have developed dedicated methods for conducting their decision making processes (ex. NATO Allied Doctrine for Operational Planning). Every commander at every level goes through a decision making process and depending on the level of the commander, and the complexity of the mission, the process is becomes more difficult. This process can be very time consuming leading to the inability to handle the situations or conflicts properly.

Intelligence systems can help to overcome the vulnerabilities of human decision making, the diversity and complexity of conflict situations, the information and technology means employed in warfare and the amount of information needed to be processed in real time.

The previous section brings up some questions that have to be answered for this concrete use case:

How critical it is? Do we have time to decide? It is life endangering? Will there be collateral damage? Who else in the chain will be impacted? How important is to have success here? Do we need to follow the rules? How public will perceive that? Could this endanger our relations with other nations?

There are several ways to take over manned and unmanned aircrafts through their sensors, connections and communications by a cyber-attack. HMI systems are as exciting as delicate, a hacker could gain access and hack the rest of the ecosystem including taking over the AI system, which is the core of the operation and mislead the human pilot. Furthermore, in joint multidomain missions, the hackers could get to other nations ecosystem. The difficulty with a human in the loop is to be able to detect an anomaly in system behavior at all.

So how to ensure there is a process in place to follow and to evaluate the level of trust or uncertainty of AI decisions? At the level of human-machine, there should be a secured redundancy AI system, that is not connected to the same network, that would evaluate the behavior of the MUM-T AI. This segregated AI would take over in case it detects abnormal behavior or some type of attack to any of the MUM-T ecosystem components.

In addition to that, a human-AI decision level process should be in place. Some research follow a stepped out approach to assess the trust and transparency of the AI interaction (Reference 6), (Reference 8), (Reference 9).

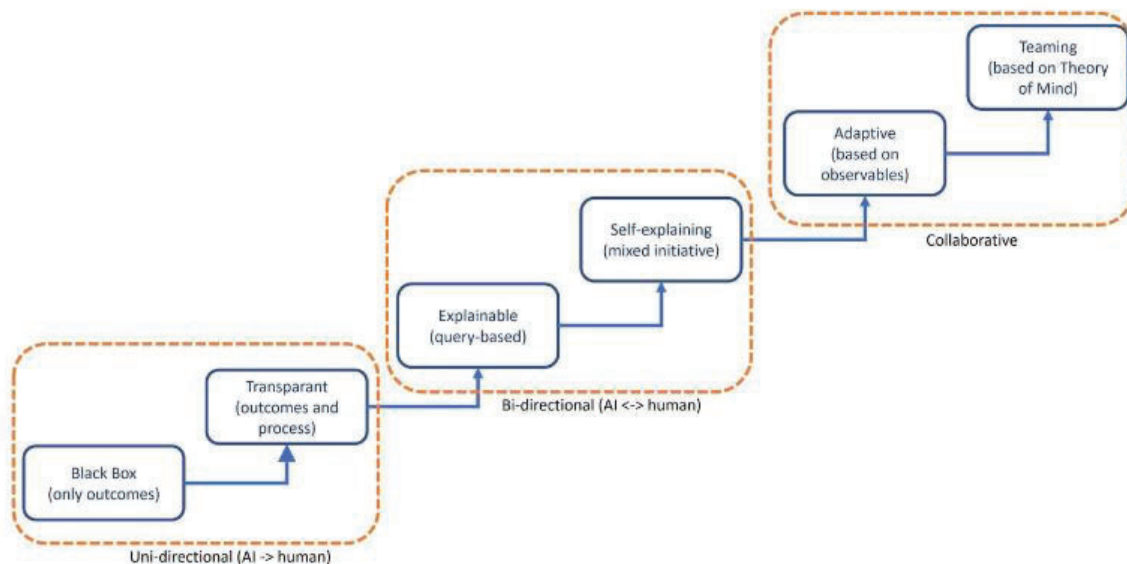


Figure 2. Levels of human-AI collaborative decision making.

This human-AI collaborative decision making approach will also help to enhance the transparency of those systems. Figure 2 shows a stepped approach towards fully AI autonomy going from the basic step, where AI is considered as a black box up to human-AI teaming, achieving the highest step.

In the use case presented above, the mission may develop towards a more complex conflict scenario, requiring lots of data processing capability and high speed decision making. The loyal wingman (Reference 12) sent to inspect the field in advance may encounter different challenges while performing their intended mission of acquiring pre battle field data. The risk of collateral damage may be a factor as the opponents base is close to a residential area but it is a target of high priority. Additionally, international regulations have to be adhered to and public perception should be kept under control.

It could occur that meanwhile this mission is progressing a cyber attack is launched, to defeat the MUM-T AI and/or its components, in order to gain control of the whole ecosystem: loyal wingman sends wrong positioning of the opponents, to send its own loyal wingman to attack friendly forces,... It will be then the moment when a supervisory AI would be needed to inspect all the MUM-T decision making steps applying a human-AI collaborative approach.

CONCLUSIONS

MUM-T architectures will be the future of how wars will be fought, posing advantages over the adversaries but also challenges.

There is still more research required towards integrating AI & human cognitive models, refine the stepped approach human-machine feedback loops, optimize trust vs transparency, how to have a common ground, and develop new advances in sensor/data acquisition decision models.

In parallel, it will be key to be aware if decisions taken by HMT are the result of hacking event, as a MUM-T ecosystem is filled by different nodes prone to be taken over.

ACKNOWLEDGMENTS

Thank you to all that made it possible my mentor Jere, Jim Atkinson and Enrico Mollenhauer for their support and inspiration.

REFERENCES

- ¹ VVAA, “Manned-Unmanned Teaming: Research and Applications Panel”, HFES DARPA 2021.
- ² Col. Livio Rossetti, “Manned-Unmanned Teaming”, NATO JAPCC Magazine. 2021
- ³ Gp Capt (Dr) D. Kumar, “MUMT – AD: Exploring to dominate in a contested environment”, 2023.
- ⁴ VVAA, , “Brain Computer Interfaces: US Military Applications”, RANDT Corp 2020.
- ⁵ J.M Rickli, “Neurotechnologies and Future Warfare”, RSiS 2020.
- ⁶ Lit. Col R. Ichaso, “Neurotechnology. Artificial Intelligence – Human Symbiosis in Fighter Aircraft End of the Fighter Jet Era or a New Evolution?”, JAPCC NATO, 2022.
- ⁷ VVAA, “Human-AI Cooperation to Benefit Military Decision”, S&T NATO
- ⁸ VVAA, “Humans and Autonomy: Implications of Shared Decision Making for Military Operations”, US Army Research Laboratory Aberdeen Proving Ground US, 2017.
- ⁹ G. Kuczynsk, “US Military Decision Process: Organizing and Conducting Planning”, 2023.
- ¹⁰ VVAA, “Unmanned Aircraft Systems: Roles, Missions, and Future Concepts”, GAO 2022.

¹¹ Dr. R. O'Toole, "FY Annual Report 2023", Operational Test and Evaluation, 2024.

¹² Clay J. Humphreys, Major, USAF, "Optimal Control of an Uninhabited Loyal Wingman", Airforce Institute of Technology, WPAF Ohio, 2016.

¹³ VVAA, "Above and Beyond: SoA of UAS Combat Aerial Systems and Future Perspectives", Istituto Affari Internazionali, 2023.

¹⁴ C.Caruso, "New Field of Neuroscience Aims to Map Connections in the Brain", Harvard Medical School, 2023.