SWARM of UAS Modeling and Simulation Methodology

Cesar Sosa
Systems Analysis Division, U.S. ARMY
Picatinny Arsenal, NJ
USA

cesar.e.sosa.civ@army.mil

ABSTRACT

Unmanned Aerial Systems (UAS) swarm attacks present a significant and evolving threat to defensive systems due to their overwhelming nature, versatility, and potential to exploit vulnerabilities. As defensive capabilities strive to keep pace with advancing UAS swarm technologies, the need for effective assessment methodologies becomes paramount. This paper explores the development of a Modelling and Simulation (M&S) methodology tailored to evaluate defensive systems' capabilities against UAS swarm attacks, aiming to identify the factors contributing most to defeating this multifaceted threat. The proposed M&S framework integrates various elements, including UAS swarm characteristics, defensive system parameters, and lethality to aid in the development and refinement of tactics, techniques, and procedures (TTPs) against this threat. Through detailed research and analysis, key capability factors are identified and prioritized based on their effectiveness in countering UAS swarm threats. These factors encompass sensor capabilities, interception methods, decision-making and threat prioritization algorithms, and resource allocation strategies. The methodology employs advanced simulation and statistical analysis techniques to replicate swarm attack scenarios within the realm of what may be possible today, and in the future, enabling comprehensive evaluation of defensive system performance under varying conditions. Through strategic M&S design considerations, the simulation model can easily accommodate various defensive solutions. By identifying and prioritizing capability factors crucial for countering UAS swarms, the proposed M&S methodology provides valuable insights for defence stakeholders, enabling them to develop more robust and effective defensive strategies in an era of evolving unmanned technologies.

KEYWORDS

Unmanned Aerial Systems, Drone Swarms, Autonomous Systems, Multi-Agent Systems, Simulation Framework, Swarm Coordination, Cooperative Behaviour, Performance Analysis, Swarm Control, Distributed Coordination, UAS Swarm Behaviour, UAS Swarm Algorithm, UAS Swarm Dynamics

1.0 INTRODUCTION

The rapid evolution of unmanned aerial systems (UAS) technology presents a significant challenge not only to the Department of Defence [1] but to all agencies around the world responsible for securing airspace. The versatility in mission types and execution methods, combined with the availability and relative affordability of UASs, has introduced an unprecedented challenge in the theatre. The traditional methods of physical prototyping and testing to evaluate new systems' performance are becoming less feasible due to logistical constraints and the accelerating pace of technological advancements. [17] It is clear that frameworks and methodologies need to be readily available and be adaptable to assess not only effectiveness but efficiencies against this volatile threat. Especially given "No single solution exists to defeat this threat; it will require the development of various materiel systems, the implementation of new training with an emphasis on emerging technologies, and the updating of doctrine to guide and instruct the Joint Force." [5] To address these challenges, the development of robust modelling and simulation (M&S) methodologies for simulating and assessing system performance against a swarm of UAS's has become critical. M&S offers a practical and efficient alternative, allowing for the prediction and analysis of system behaviours and interactions in a virtual environment where millions of scenarios can be generated. This approach not only reduces the dependency on extensive physical testing but also facilitates the exploration of various hypothetical scenarios and system configurations. Nevertheless, the integration of some level of physical testing remains essential to validate and refine the accuracy of M&S tools, ensuring they reliably represent real-world dynamics and enhance system development processes.

The development of an effective M&S methodology for assessing the performance of defensive systems and UAS swarms involves several key components. First, it requires a comprehensive understanding of the characteristics and behaviours of both UAS swarms, including their flight dynamics and potential strategies for both offensive and defensive manoeuvres and characteristics of the systems employed to attempt to counter the swarm threat. It will also require a modelling scheme that allows for seamless integration of various types of systems using object-oriented programming and ensuring functional modules are loosely coupled and highly cohesive. [14] Incorporating these elements into the simulation models ensures that the virtual environment is not rigid in design and lends itself to be readily adaptable to most systems looking to be represented through M&S.

Next, the M&S framework should allow for scenarios to be effortlessly scaled up or down and either the integration of low fidelity algorithms or advanced computational algorithms capable of handling varying levels of complexity. This can include leveraging artificial intelligence (AI) and machine learning (ML) techniques to model adaptive behaviours and decision-making processes within the swarm. In the absence of complex modules, simpler lower fidelity modules should be easily substituted using standardized application programming interfaces (API).

M&S facilitates the exploration of innovative tactics and strategies to counter UAS swarms, thereby aiding the development of more effective and adaptable defence systems. Implementing robust models requires gathering subject matter expertise from multiple disciplines, including aerodynamics, sensors, algorithms, fire control, and lethality. In cases where expertise in a specific discipline is lacking, statistical or lower-fidelity models can be used as stand-ins to approximate system performance until higher-fidelity models become available. Given the rapid pace of Research and Development (R&D), models involved in simulations are frequently subject to change. Therefore, a framework with strict interface control is essential for managing disparate models of varying fidelity, ensuring seamless integration, and maintaining the integrity of the simulation environment.

Presented in this paper is a methodology used for establishing a virtual environment that will lend itself for use in executing performance analyses of swarms and defensive systems. It has been developed to meet the demands of a highly dynamic and rapid prototyping environment. This M&S methodology as of the time of writing this paper has been sought after and utilized to assess performance of several defensive systems against a swarm threat. The paper will first discuss the challenges UAS swarms pose to national security. Next, it will delve into the design of the simulation framework and methodology, emphasizing modularity and interoperability to ensure flexibility and adaptability. Finally, the potential adaptations of the framework for other applications and future developments. As technological advancements continue to accelerate, the reliance on M&S will only grow, underscoring its critical role in the future of defence system development.

2.0 SWARM CHALLENGE

A swarm poses a unique problem unlike any other where "…there is no panacea that will stop all drones. UAS technology is evolving at a rate that makes it challenging to predict all the countermeasures that will be needed to disrupt them." (Parsons, 2020, p.10). With a lot of the disruption seeming to come from commercially available group 1 and group 2 UAS's, described in Figure 1, even "CENTCOM Commander General McKenzie highlighted the threat from these classes of UAS when he told the House Armed Services

Committee that “we aggressively pursue anything that will improve the capabilities, particularly against those group one and two UAS’.... That is one of the things that worries me the most in the theatre every day. It is the vulnerability of our forces to those small UAS.” [5]. Group 1 and 2 UAS’s can be outfitted with a variety of payloads, have a small profile, are highly manoeuvrable, difficult to detect, inexpensive, and collectively overwhelm most systems or operators.

Group	Maximum weight (lb)	Nominal operating altitude (ft)	Speed (kn)
1	0–20	< 1,200 AGL	100
2	21–55	< 3,500 AGL	< 250
3	< 1,320	< FL 180	
4	> 1,320		Any
5		> FL 180	

Figure 1: UAS Group Classification. Adapted from UAS Task Force Airspace Integration Integrated Product Team (15).

The undefined nature and unpredictability in movement, formation, objective, and payload of this threat at the cost to produce makes this threat a challenge unlike anything seen before. The asymmetry in cost driving most of the complexity in developing a solution to tackle this threat that can overwhelm many systems. Most importantly, “An inexpensive, rudimentary swarm in the hands of a terror organization could cause damage that rivals a sophisticated weapon system at a fraction of the cost.” (Thyberg, 2019 p.3). Illustrated in Figure 2. are a few architecture types for the employment of UAS’s. each posing different challenges for generating a solution to counter this threat type especially given infrastructure is likely to be unknown in an uncontrolled environment.

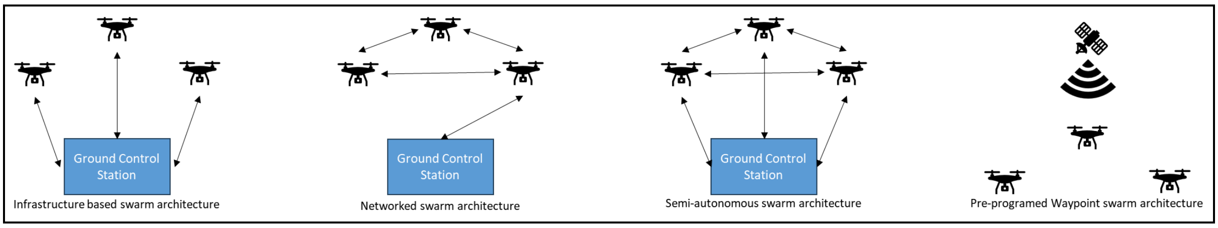

Figure 2: Example Information Exchange Swarm Architectures. Adapted from Parsons. (2020)

Estimating the effectiveness of current defensive systems against various swarm threat scenarios through physical experimentation is challenging due to the constraints and limitations of testing facilities. [10] Additionally, defining the threat to assess performance against is difficult because a mass coordinated UAS attack has not yet been observed. Given the variety of swarm control strategies, as illustrated in Figure 3, scenarios involving a large mass coordinated UAS attack must cover a wide spectrum. Additionally, the virtually endless swarm scenarios that need to be tested further complicate the process. Assessing the effectiveness of a countermeasure against a configurable threat through physical experimentation alone is impractical, especially as the complexity of the scenarios increases. This underscores the necessity for a M&S methodology that is as scalable and adaptable as the threat itself [10], enabling rapid prototyping and assessment of system effectiveness against such threats.

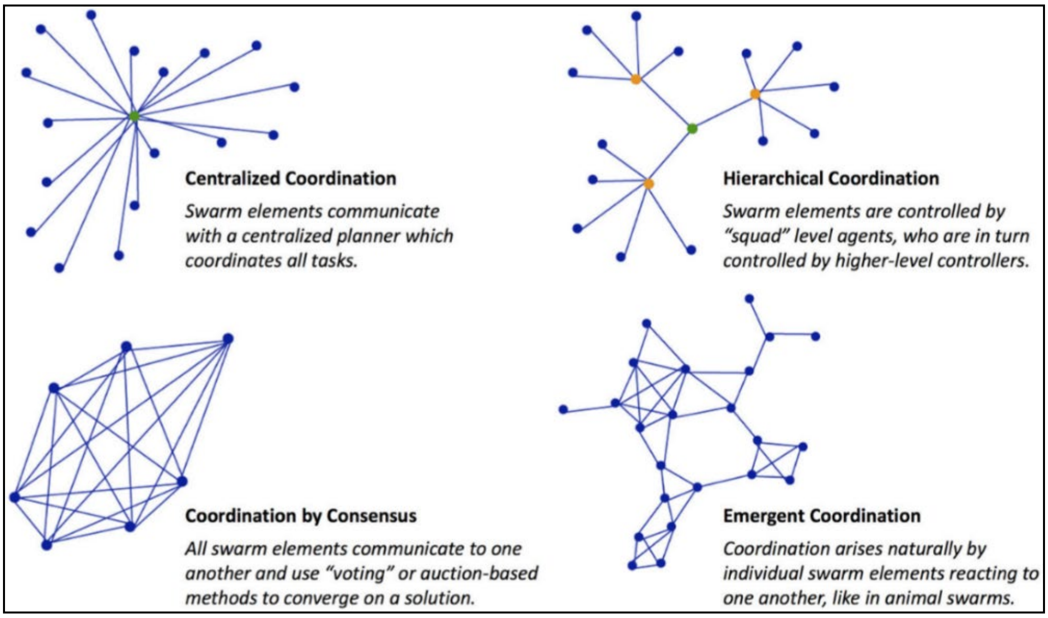

Figure 3: Example swarm control strategies reprinted from Scharre (2014).

3.0 M&S METHODOLOGY

The methodology outlined in this section aims to provide a structured and systematic approach to evaluating the performance of defensive systems against swarms of UAS or vice versa.

This approach focuses on identifying steps taken to establish a model framework suitable for simulating systems that can be scaled for the purpose of executing a performance analysis and analysing key system parameters. It also enables the testing of various fire control solutions, aiming to optimize weapon-target pairing, prioritization, and firing strategies. This area being crucial because of the overwhelming nature of the threat [3]. Reliance on algorithms to process the incoming threat, characterize, and prioritize the targets will increase as the sophistication of the swarm threat rises. The methodology comprises five main steps:

Step 1: Define analysis objectives.

Step 2: Define scenario.

Step 3: Functional decomposition of scenario

Step 4: Source or develop simulation models.

Step 5: Execute simulation and analyse results.

3.1 Step 1: Define Analysis Objectives

The first step is to clearly define the analysis objectives and metrics to be captured from the simulations. This involves identifying the primary purpose of the simulation, which could include testing defence strategies, understanding swarm behaviours, evaluating system sensitivities, or assessing mission effectiveness. Additionally, success criteria need to be determined to evaluate whether the simulation meets the desired outcomes. Defining the objectives of the analysis will determine the level of fidelity required for key aspects or functional areas of a system to ensure an effective evaluation. For instance, if the objective of the analysis is to assess the likelihood of collisions between UASs under specific conditions, accurately modelling the geometry of individual entities becomes crucial. Whereas if the objective is to evaluate communication robustness within the swarm, the focus would shift towards simulating network protocols and data exchange mechanisms.

3.2 Step 2: Define Scenario

The next step is to define the scenarios for the simulation. Realistic and detailed scenarios should be developed to reflect potential operational environments. The scenario definition should serve as the blueprint to follow for stages all actors within the simulation environment. This could include specifying environmental parameters like geographic features, obstacles, number of UAS's, payloads, location, etc. as illustrated in Figure 4. Mission parameters need to be precisely defined to ensure they align with the analysis objectives.

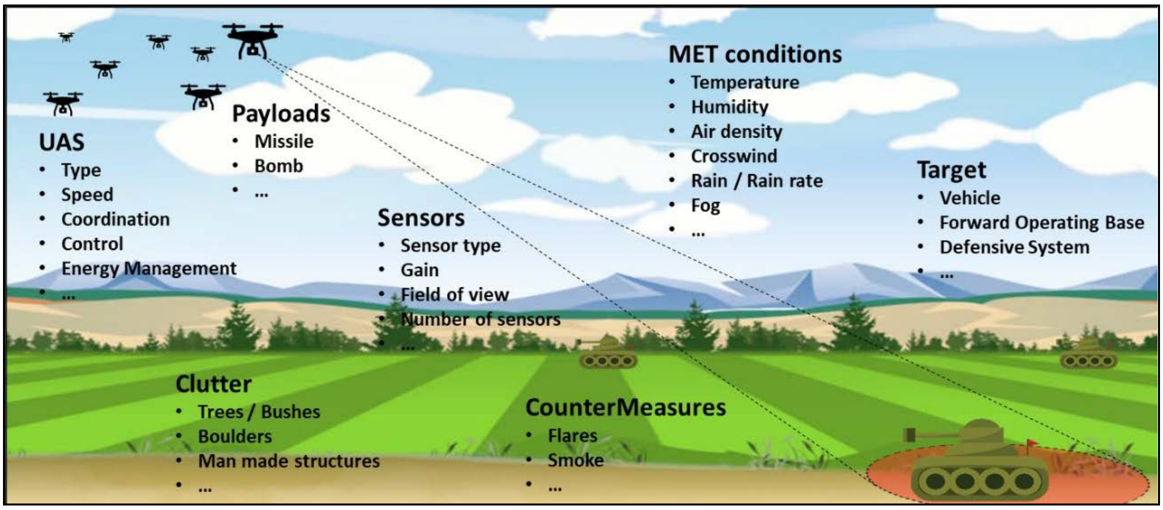

Figure 4: Illustration of a weapon-target-engagement scenario factors. Adapted from [9].

3.3 Step 3: Functional Decomposition of Scenario

Once the scenarios are defined, the next step is to perform a functional decomposition of the scenario. This involves identifying the key functions and tasks that the UAS swarm must perform, such as formation flying, and obstacle avoidance. The interactions between swarm and the environment, and external entities (e.g., threats) must be specified. Developing a functional flow diagram can help illustrate the sequence of tasks and interactions within the scenario, providing a clear understanding of the operational dynamics and dependencies as will be discussed in section 3.5.

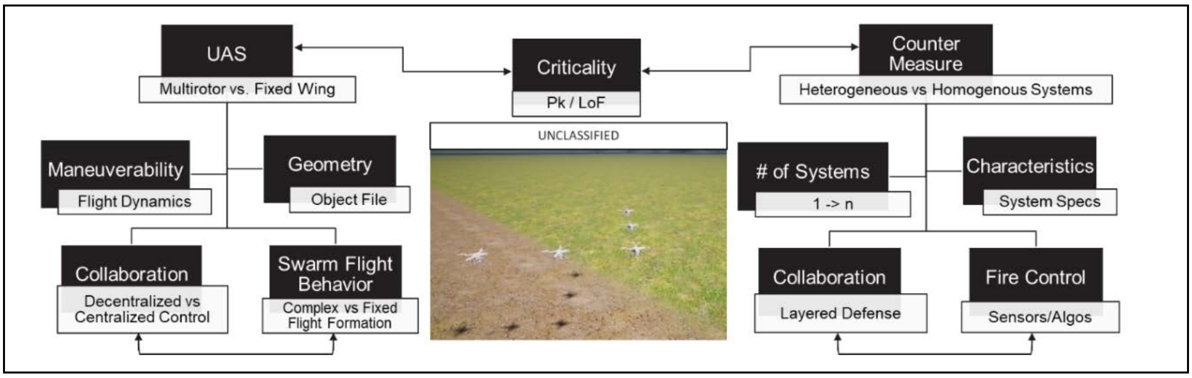

Figure 5: High-level decomposition of functional area for modeling defensive systems and swarms.

3.4 Step 4: Design and Develop Simulation Models

After the functional decomposition, the design and development of simulation models begin. Appropriate simulation tools and platforms must be selected to support the modelling of UAS swarms and their behaviours. Existing frameworks and algorithms can also be leveraged or used as a starting point for modelling swarm behaviours [12]. In addition to this, models for the defensive systems will also need to be developed to support the simulation of the engagement scenario. Models for individual UAS need to be developed, encompassing their aerodynamics, propulsion systems, sensors, communication modules, and control algorithms where applicable. Similarly, models for individual defensive systems need to be developed, encompassing the attributes necessary to accurately represent the system in the virtual environment. These models should be tailored to meet the requirements necessary for conducting the analysis. Additionally, algorithms that govern swarm behaviour, like coordination strategies, task allocation, formation control, and collision avoidance, should be adaptable to allow the user to design any number of swarm concepts as illustrated in Figure 6. with ease. These individual models and swarm algorithms are then integrated into a unified simulation framework to ensure compatibility and seamless interaction between all components.

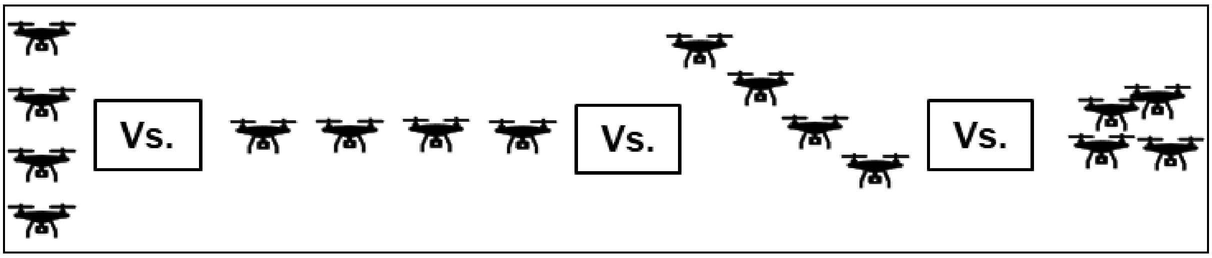

Figure 6: Example SWARM formations.

3.5 Step 5: Execute Simulation and Analyse Results

The final step is to execute the simulation and analyse the results. The simulation environment must be configured according to the defined scenarios. The simulation is then run for each scenario, with multiple iterations to account for variability and stochastic element if necessary. Statistical and analytical methods should be used to ensure the accuracy, reliability, and robustness of the simulation results for UAS swarm scenarios, facilitating informed decision-making and optimization of system performance.

4.0 HIGH-LEVEL SIMULATION SETUP

Figure 7 illustrates a simplified modelling framework for setting up an engagement scenario between a networked set of defensive systems and a UAS swarm. The high-level depiction demonstrates how this framework facilitates scalable simulations, allowing complexity to be adjusted by strategically compartmentalizing models based on their specific functions or representation of a system. The simulation driver functions as a low-overhead integrative framework, enabling the seamless incorporation of diverse models into a cohesive simulation for UAS swarm scenarios. The strategic compartmentalization of key system functions ensures efficient model development and updates across multidisciplinary Integrated Product Teams (IPTs), while the simulation driver sets the standard for the API and communication between models. The mission control model in this instance is representative of the model used to instantiate the entities within the user's scenario within the virtual environment. The swarm spawner module allowing one to simulate alternative conceptual swarm types as highlighted in [4]. This can appear as swarms comprising of separated groups of UAS's, one large mass, or individual UAS's. It allows for seamless data transfer between swarm groups allowing for highly complex and coordinated scenario development. Similarly, the UAS spawner module simplifies control and data exchange for the individual UASs within the swarm, enhancing the overall management of information exchange between models. Lastly, the UAS module encompasses all the characteristics and traits specific to the UAS being simulated, ensuring accurate representation and performance within the scenario at the individual entity level. The advantage of this structured approach is that it allows each model to vary in complexity if the expected inputs and outputs are reported from each functional area within the scenario. This same approach is taken when also modelling the defensive systems within a scenario.

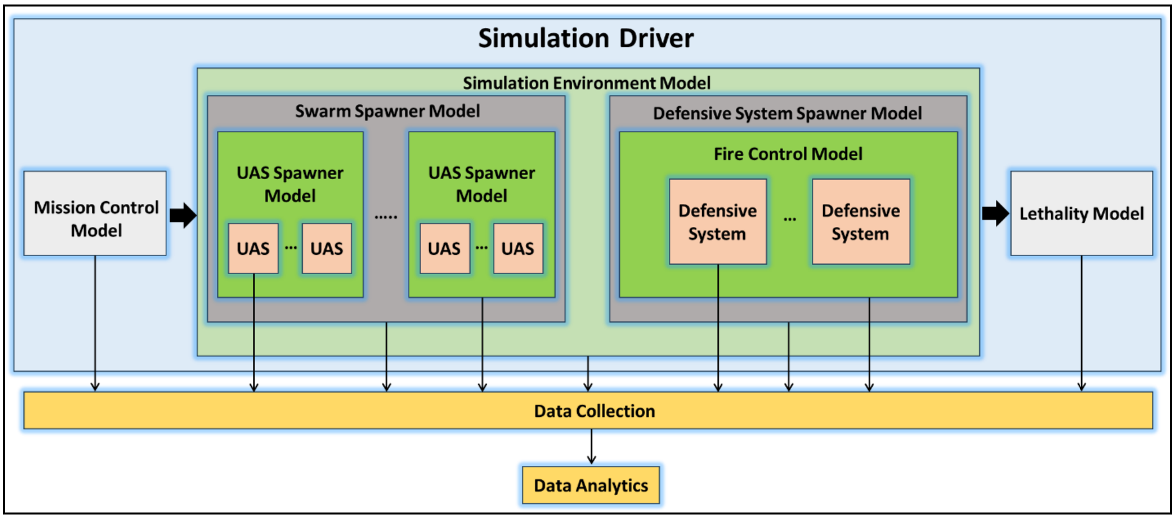

Figure 7: High level simulation setup.

5.0 CONCLUSION

In this paper, we explored the relevance of an inevitable future threat and the use of strategic simulation design to evaluate the performance of UAS swarms and networked defensive systems. The methodology described provides a blueprint for structuring the developments of a capability that will be effective for evaluating formation algorithms, defensive systems, weapon target pairing algorithms, etc. in a computationally efficient environment. This process emphasized the need to compartmentalize information exchange and functions within a simulation framework to ensure the development environment remains adaptable. As a result, this approach paves the way for robust and scalable solutions in the ever-evolving landscape of aerial defence technology allowing for easier updates, integration, and adaptation to evolving needs without disrupting the entire simulation environment. This framework would allow for flexible, scalable, and efficient representation of complex interactions and behaviours in dynamic environments.

6.0 REFERENCES

[1] M. Parsons, "Feasibility of Indirect Fire for Countering Swarms of Small Unmanned Aerial Systems", M.S thesis, Naval Postgraduate School, Monterey, California, USA, 2020. [Online] Available:https://www.dtic.mil/document;accessionNumber=AD1114696;type=TRECMS;searchText=swarm;relatedTerms=undefined

[2] R. Thyberg, "Design and testing of a multi-unit payload delivery and tracking system for guided munitions to combat UAV swarm threats", M.S thesis, Naval Postgraduate School, Monterey, California, USA,2019. [Online] Available: https://www.dtic.mil/document;accessionNumber=AD1080472;type=TR;searchText=swarm;relatedTerms=undefined

[3] C. Laird, "heterogeneous defensive naval weapon assignment to swarming threats in real-time", M.S thesis, Naval Postgraduate School, Monterey, California, USA, 2016. [Online] Available: https://www.dtic.mil/document;accessionNumber=AD1027464;type=TR;searchText=swarm;relatedTerms=undefined

[4] J. Llinas, "Multisensor Multitarget Tracking and Small UAV Swarms", University at Buffalo, Buffalo, New York, USA, 2023. [Online] Available: https://www.dtic.mil/document;accessionNumber=AD1216226;type=TRECMS;searchText=Modeling%20and%20Simulation%20SWARM;relatedTerms=undefined

[5] G. B. Morrison, "National Defense University Joint Forces Staff College Joint Advanced Warfighting School will a UAS Swarm Overwhelm the Joint Force?", National Defense University Joint Forces Staff college Joint Advanced Warfighting School, Norfolk, VA, USA, 2021. [Online] Available: https://www.dtic.mil/document;accessionNumber=AD1154005;type=TRECMS;searchText=UAS;relatedTerms=undefined

[6] C. Roberto, "Simulation Modeling and Dynamics of Rotorcraft-Based UAS", University of Maryland, College Park, MD, USA, 2024 [Online] Available: https://www.dtic.mil/document;accessionNumber=AD1229775;type=TRECMS;searchText=UAS;relatedTerms=undefined

[7] A. N. Golphin III and B. D. Offord II, "Counter-unmanned Aerial Systems (C-UAS) Interoperability in the Global Geopolitical Environment", M.S thesis, Naval Postgraduate School, Monterey, California, USA,2021. [Online] https://www.dtic.mil/document;accessionNumber=AD1164261;type=TRECMS;searchText=UAS;relatedTerms=undefined

[8] United States Air Force Unmanned Aircraft Systems Flight Plan 2009–2047. United States Air Force, Washington, DC, USA, 2009. Available: https://www.govexec.com/pdfs/072309kp1.pdf

[9] C. Sosa and A. Aguirre, "Sensor Fuzed Munition Modeling Framework", Picatinny Arsenal, Picatinny, NJ, USA, 2022. [Online] Available: https://www.xcdsystem.com/iitsec/proceedings/index.cfm?Year=2022&AbID=112946&CID=944

[10] Worth DB, Woolley BG, Hodson DD. SwarmSim: a framework for modeling swarming unmanned aerial vehicles using Hardware-in-the-Loop. The Journal of Defense Modeling and Simulation. 2021;18(2):105-124. doi:10.1177/1548512917715154

[11] Scharre P. Robotics on the battlefield part II: The coming swarm. Technical report, Center for a New American Security, October 2014.

[12] Campion, M., Ranganathan, P., & Faruque, S. (2018). UAV swarm communication and control architectures: a review. Journal of Unmanned Vehicle Systems, 7(2), 93-106.

[13] M. Campion, P. Ranganathan, and S. Faruque," A Review and Future Directions of UAV Swarm Communication Architectures", Department of Electrical Engineering University of North Dakota Grand Forks, ND, 2018. [Online] Available: https://und.edu/research/rias/_files/docs/swarm_ieee.pdf

[14] Ling, H.; Luo, H.; Chen, H.; Bai, L.; Zhu, T.; Wang, Y. Modelling and Simulation of Distributed UAV Swarm Cooperative Planning and Perception. Int. J. Aerosp. Eng. 2021, 2021, 9977262. [Online] Available: https://onlinelibrary.wiley.com/doi/10.1155/2021/9977262

[15] UAS Task Force Airspace Integration Integrated Product Team, Unmanned Aircraft System Airspace Integration Plan Archive.org, 2016, [Online] Available: web.archive.org/web/20160121155841/www.acq.osd.mil/sts/docs/DoD_UAS_Airspace_Integ_Plan_v2_(signed).pdf

[16] Christie, E.J. & Jensen, Daniel & Buckley, R.T. & Menefee, D.A. & Ziegler, Kyle & Wood, Kristin. (2012). Prototyping Strategies: Literature Review and Identification of Critical Variables. ASEE Annual Conference and Exposition, Conference Proceedings. 10.18260/1-2--21848.

[17] S. Qi, F. Wang and X. Wu, "The Challenges of Autonomous Unmanned Aerial System Test and Evaluation," 2021 IEEE International Conference on Unmanned Systems (ICUS), Beijing, China, 2021, pp. 752-756, doi: 10.1109/ICUS52573.2021.9641409.