Second Version Paper Title: The Future for Cyber Wargaming: An Applicable Expansion for the Cyber and Space Domains

2024 Conference Title: Cyber Wargaming in the Space Domain: Enhancing National Security Through Integration and Innovation

Mohammad Tasrif Khan (Mo Khan)[1]

Advanced Abstract (Version One)

In the contemporary era of space exploration and emerging technologies, this project accentuates the critical role of cybersecurity in the space domain, positioning it as a linchpin for developing and maintaining a secure cyber environment throughout the lifecycle of space missions. The intricate integration of diverse government, military, and commercial elements into a cohesive full-range cycle necessitates a steadfast commitment. Cyber-attacks on space infrastructure, such as malware installation, ransomware attacks, and data/system hacking breaches, present substantial threats. This study identifies the industry's most susceptible to these attacks, including telecommunications, supply chains, national security, IoT/Internet access, and global economies of scale. The project highlights key objectives, explores the evolving landscape of cyber wargaming and its expansion into both cyber and space domains, analyzes the current state of cyber wargaming, identifies emerging trends, and lastly proposes a robust framework for integrating cyber and space-domain environments with meaningful effects.

The comprehensive examination evaluates both technical and non-technical strategic approaches, emphasizing collaboration across public and private entities. The study structure delves into the background and significance of cyber wargaming, highlighting its limitations and the need for expansion into cyber and space domains. It establishes objectives, including the analysis of the current state of cyber wargaming, identification of trends, and the development of a framework for integration. The technical approaches section explores cyber wargaming, the current technological landscape, the integration of the space domain, advanced simulation technologies, and case studies from military (public) and civilian (private) sectors. The non-technical strategic approaches section covers policy and legal considerations, human factors, collaboration, and information sharing, along with ethical considerations. The conclusion summarizes key findings, proposes a framework, and discusses the significance and outlook, contributing to the discourse on enhancing national security through the innovative and strategic integration of cyber operations and space wargaming.

[1] American Military University Alumni (Space Operations Studies), Embry-Riddle Aeronautical University, Florida (Graduate Student-Cyber and Space Operations Major), U.S. Student & UAS Pilot with FAA certifications.

Basic Abstract (Version Two)

This project highlights the importance of cybersecurity in the space domain as a focal point for building and ensuring a secure cyber environment throughout the life cycle of space missions in the modern age of space exploration and rapidly developing technologies. The complex merging of heterogeneous elements of government, armed forces and business into a single full-range cycle requires an unwavering commitment. Cyber-attacks targeting space infrastructure, which include malware installation, ransomware attacks, and data/system hacking breaches, are very serious threats. This study reveals the sectors that are more vulnerable to such attacks, such as telecommunications, supply chains, national security, IoT/internet access, and global economies of scale. The project outlines primary goals, addresses the transformation of the cyber wargaming landscape and its transition to both cyber and space realms, describes the current state of cyber wargaming, identifies trends, and concludes with a sound framework for incorporating cyber and space-domain environments with significant impacts.

The holistic evaluation is technical and non-technical approaches of strategic planning that stresses collaboration across public and private entities. The study design focuses on the history and importance of cyber wargaming, its weaknesses and the necessity of its expansion into cyber and space domains. It sets goals such as analyzing the current situation with cyber wargaming, determining trends, and defining a system of integration. The technical approaches section focuses on cyber wargaming, technological environment, integration of the space domain, advanced simulation technologies, and case studies from military (public) and civilian (private) sectors. The non-technical strategic approaches section includes policy and legal issues, the human factor, cooperation, and information sharing, and ethical issues. The conclusion provides a summary of the key findings; proposes a framework and discusses the importance and outlook, contributing to the debate on the innovative and strategic integration of cyber operations and space wargaming as a method to improve national security.