**CHAPTER**

**1**

**THE OVERVIEW OF EMERGING DISRUPTIVE TECHNOLOGIES IN MILITARY**

*Radziah Mohamad and Izyan Izzati Kamsani*

* 1. **INTRODUCTION**

The rapid development of new disruptive technologies is having a significant impact on the military landscape. Changes in paradigm and the introduction of new capabilities are hallmarks of these technologies, redefining how military operations are conducted. State-of-the-art new disruptive technologies, such as artificial intelligence, robotics, and cybersecurity, are rapidly advancing in the military.

Emerging developments in today's most cutting-edge science and technology fields are cited as having the potential to transform government structures, economies, and international security. Some have argued that these technologies will lead to doomsday scenarios and that their military applications can profoundly shift the balance of power even more than nuclear weapons. Nanotechnology, including meta-materials; robotics, including lethal autonomous systems; Artificial Intelligence /Machine Learning; the cognitive neurosciences; synthetic/systems biology; biotechnology; high-energy weaponry; and the intersection of each with information and computing technologies, collectively known as the converging sciences.

The operational environment is continually evolving due to the use of new technologies in the design of combat weapons or their usage by adversaries in civilian or dual-use facilities or equipment. Automation, computerization, and robotization are solid proof of the trend of technological progress in military organizations, where the objective is to accomplish human-safe activities with minor collateral material damage (Raţiu & Roşu, 2020).

The history of military art is a specialized topic into which the history of culture is fragmented. Wars, which broaden the extent of a nation's viability, give the military institution a prominent position in the country's structure. Military technology refers to the application of technology to battle. It consists of the types of technology uniquely military in character and have no civilian application, typically because they lack a practical or legal civilian application. Typically, scientists and engineers research and create military technologies for use in combat by the armed services.

As state of the art in new disruptive technologies continues to advance, military organizations, researchers, and policymakers must remain educated and adapt to the changing environment. By adopting these technologies responsibly and proactively tackling associated difficulties, the military sector may maximize the potential of new disruptive technologies to gain a competitive edge, improve national security, and define the future of combat.

* 1. **MOTIVATION FOR EXPLORING EMERGING DISRUPTIVE TECHNOLOGY IN MILITARY**

Disruptive technologies refer to those that abruptly and unexpectedly displaces an existing technology from the market. In the military realm, this refers to a technological advancement that alters the rules or conduct of conflict within one or two generations. Globalization has aided in the quicker spread of disruption, which has shortened the time required for the military to adjust. In addition, the ongoing disruption in the military domain, caused by developing technology, has adopted a fundamentally distinct approach. The usual strategy was to multiply existing systems so that more soldiers could be armed, however, the present strategy appears to be going the opposite way by minimizing the human element (Review & Anand, 2019).

Diverse factors motivate the investigation of developing disruptive technologies in the military domain, particularly computational approaches for intelligent weapon systems and military education training command systems, as well as cybersecurity for unmanned weapon systems. These motivations derive from the need to increase military capabilities, enhance training effectiveness, and address cybersecurity challenges in a wartime environment that is constantly evolving. These technologies can transform the efficacy and efficiency of military operations, assuring mission accomplishment while minimizing collateral harm.

The importance of military education and training command systems in preparing people for the difficulties of modern combat cannot be overstated. Exploring computational approaches for military education training systems arises from a need to improve training efficacy. By utilizing simulations, virtual reality, and artificial intelligence, training systems may provide people with realistic and immersive training experiences, allowing them to develop their skills, decision-making ability, and tactical expertise in a controlled setting.

Drones and autonomous vehicles are now critical components of modern military operations. However, these systems are susceptible to cyber threats that could jeopardize their integrity, operation, or control. Cybersecurity research for autonomous weapon systems is motivated by the need to address these vulnerabilities and safeguard military assets from cyberattacks. Robust cybersecurity measures are required to protect the confidentiality, availability, and integrity of unmanned weapon systems and prevent unwanted access or manipulation by enemies.

As the development of disruptive technologies continues, it is essential to investigate their potential dangers and address the ethical issues associated with their deployment. The need to mitigate risks and ensure responsible use motivates the study of computational methods for intelligent weapon systems, military education training systems, and cybersecurity for unmanned weapon systems. By proactively addressing ethical concerns and developing robust frameworks for risk management, military organizations can minimize unintended consequences and uphold ethical standards in applying these technologies.

Exploring emerging disruptive technologies in the military domain presents the possibility of gaining a strategic advantage. Military forces can gain a competitive advantage over their adversaries by adopting computational methods for intelligent weapon systems and military education training systems and implementing stringent cybersecurity measures for unmanned weapon systems. These technologies allow for quicker decision-making, increased operational efficiency, enhanced training outcomes, and better protection of military assets, enhancing the military's overall preparedness and effectiveness.

* 1. **CONTRIBUTION OF KNOWLEDGE**

Emerging disruptive technologies, particularly computational methods, and cybersecurity, have made substantial contributions to the military domain's body of knowledge. In military operations, computational approaches such as data analysis, machine learning, and artificial intelligence have considerably enhanced situational awareness. These technologies enable the processing and analysis of massive volumes of data from several sources, thereby offering operational environment insights in real time. By integrating and evaluating multiple data streams, military leaders obtain a holistic understanding of the battlefield, allowing for informed decision-making and efficient resource allocation.

The application of computational technologies has transformed military training and simulation. Virtual reality, augmented reality, and computer simulations provide realistic and immersive training experiences, allowing military personnel to practice and enhance their skills in a controlled setting. These technologies create interactive scenarios, replicate complex events on the battlefield, and facilitate collective training exercises. In addition, computational technologies enable adaptive training systems that tailor the learning experience to the needs and performance levels of each individual.

The emergence of disruptive technologies has brought about new challenges in terms of cybersecurity and defense in military operations. Cybersecurity measures, including encryption, network monitoring, and intrusion detection systems, contribute to safeguarding military systems, infrastructure, and data from cyber threats. Advancements in cybersecurity technologies have enhanced the resilience of military networks, mitigated vulnerabilities, and protected critical assets from unauthorized access or exploitation.

The military's exploration of computational technologies and cybersecurity has prompted significant ethical concerns. Issues pertaining to human control, autonomous systems, and the use of disruptive technology responsibly are being actively addressed. In this context, the contributions of computational methods and cybersecurity include the establishment of ethical frameworks, policy guidelines, and regulatory frameworks to ensure the responsible and ethical application of these technologies in military operations.

* 1. **OVERVIEW OF EDITED BOOK**

This book is divided into two sections relating to disruptive emerging technologies in the military. The first section is cybersecurity, which examines the weaknesses and risks that unmanned systems face, as well as the significance of implementing comprehensive cybersecurity procedures to prevent future attacks. The second section investigates the transformative potential of computational techniques for improving intelligent weapon management systems and military education training systems.

Chapter 1 describes the current state of new military technologies. Emerging technology is typically a new technology or the continued development of an existing technology that will transform future military capabilities, strategy, and operations.

The focus of Chapter 2 is the incorporation of data science and artificial intelligence (AI) approaches into unmanned weapon systems to enhance their capabilities in future battle scenarios. This chapter examines how data-driven techniques and AI algorithms might enhance several aspects of unmanned weapon systems, including target detection, decision-making, and mission planning.

The third chapter focuses on incorporating high-performance computing (HPC) techniques and approaches into autonomous weapon systems to improve their effectiveness in future battle scenarios. This chapter examines the potential of high-performance computing to optimize many elements of autonomous weapon systems, including data processing, decision-making, and mission execution.

Chapter 4 presents an overview of the significance of cybersecurity in unmanned weapon systems and examines the tactics, technologies, and practices for protecting and empowering these systems in future battle situations. It analyses the tactics, technologies, and best practices for ensuring the protection and resilience of these systems in future combat scenarios.

The fifth chapter examines how data-driven approaches can improve intelligent weapon management systems' effectiveness, efficiency, and decision-making capabilities. It emphasizes the incorporation of data science approaches and methods into the management of intelligent weapon systems.

Integration of high-performance computing (HPC) techniques and approaches into the management of intelligent weapon systems is the subject of Chapter 6. It presents an overview of the use of high-performance computing techniques in intelligent weapon management systems. It investigates further how HPC may improve the computing power, speed, and efficiency of intelligent weapon management systems, resulting in enhanced performance and decision-making capacities.

The seventh chapter examines ambient computing and its application to intelligent weapon management systems. It examines the fundamentals of ambient intelligence, such as pervasive sensing, context awareness, and adaptive interfaces, as well as integrating these aspects into weapon management systems.

Last but not least, chapter 8 examines specific military education and training command system applications of ambient computing. This includes using ambient sensors and ubiquitous connectivity to collect real-time data on trainees' performance, thereby enabling tailored and adaptive training interventions. It also investigates the incorporation of context awareness and adaptive interfaces to deliver relevant and interesting learning experiences for trainees.

**REFERENCES**

Raţiu, A., & Roşu, O. (2021)

The Impact of Some Emerging Technologies in Modern Military Actions. Scientific Bulletin, 26(2), 188–194. https://doi.org/10.2478/bsaft-2021-0023

Review, B., & Anand, V. (2019)

Technological Revolution and the Emerging Military Environment. 9658(ii), 285–288.