DEFEATING SWARM DRONES WITH DIRECT ENERGY WEAPONS: STRATEGIES AND CHALLENGES

Lt Gen TSA Narayanan, AVSM (Retd)
Research Associate
Poornima University

Dr Suresh Chandra Padhy
President (Vice Chancellor)
Poornima University

Abstract

The increasing prevalence and threat posed by swarm drones necessitate the development of effective countermeasures. Direct energy weapons (DEWs) offer promising capabilities for countering swarm drones due to their speed, precision, and scalability. This paper characteristics and the threat posed by Swarm drones including some recent successful swarm drones attack by anti-national elements or terrorists. This paper explores the strategies and challenges involved in utilizing DEWs to defeat swarm drones. By examining the strategies and challenges involved in defeating swarm drones with DEWs, this paper aims to contribute to the ongoing discussions and developments in the field of counter-swarm technologies. The findings and recommendations provided herein can serve as a basis for operational planning in countering swarm drone threats using direct energy weapons.

Keywords:- Swarm Drones, Direct Energy Weapons, unmanned aerial vehicles (UAVs), Anti drone Technology, Lazer Based DEW and High Powered microwave DEW

I. INTRODUCTION

Swarm drones, characterized by the coordinated and synchronized actions of multiple unmanned aerial vehicles (UAVs), have emerged as a significant threat in modern warfare and security scenarios. Their ability to overwhelm traditional defences through sheer numbers, decentralized control, and rapid manoeuvrability presents a formidable challenge for military forces and security organizations. To effectively counter swarm drones, innovative and advanced technologies are required. Direct energy weapons (DEWs) offer promising potential in this regard, leveraging directed energy to engage and defeat swarm drones. This paper aims to explore the strategies and challenges involved in utilizing DEWs for defeating swarm drones, providing insights into their feasibility and effectiveness in countering this emerging threat.

The increasing proliferation of swarm drone technology has necessitated the development of new and adaptable defensive measures. Traditional kinetic-based weapons, such as missiles or gunfire, may struggle to keep up with the agility and speed of swarm drones. In contrast, DEWs offer unique advantages in terms of speed, precision, and scalability. By emitting focused

energy beams, such as lasers or high-powered microwaves, DEWs can engage multiple targets simultaneously, providing rapid response times crucial for combating swarm drones.

The paper will explore strategies for defeating swarm drones with DEWs, including target identification and tracking, scalability and rapid engagement, precision energy delivery, and considerations for countering potential countermeasures employed by swarm drones. Technical aspects such as power generation, beam control, and integration with existing sensor networks and command systems will be analysed to evaluate their impact on the effectiveness of DEWs in swarm drone defeat. A comprehensive overview of DEWs will be provided, highlighting the different types, their operational capabilities, and the advantages they offer in countering swarm drones. Additionally, the limitations and challenges associated with DEWs will be addressed to provide a balanced understanding of their practicality.

While DEWs hold promise in countering swarm drones, several challenges and future directions need to be considered. These include swarm drone adaptability to countermeasures, power requirements and logistical constraints, variability in operational environments, and ethical and legal considerations. By addressing these challenges, future research and development efforts can enhance the effectiveness and reliability of DEWs as a counter-swarm technology. The paper will conclude with a summary of findings, recommendations for further research, and implications for military strategies and policies. The insights gained from this research will contribute to the ongoing efforts in developing effective countermeasures against swarm drones and provide valuable guidance for decision-makers and defense organizations in mitigating the threats posed by this emerging technology.

II. SWARM DRONE

A. Characteristics.

Swarm drones are a category of unmanned aerial vehicles (UAVs) that operate in a coordinated and synchronized manner, often controlled by a centralized or decentralized command and control system. Swarm drones possess unique characteristics and pose specific threats that differentiate them from individual or small groups of UAVs. Understanding these characteristics and threats is crucial in devising effective countermeasures. The swarm drone characteristics and the threats they present:

1. **Numbers and Density.** Swarm drones operate in large numbers, ranging from dozens to hundreds or even thousands of individual UAVs. This sheer quantity allows swarm drones to overwhelm traditional defences and saturate the target area, increasing the difficulty of detection and engagement.

2. **Decentralized Control**. Swarm drones often employ decentralized control mechanisms, where individual drones communicate and coordinate with each other to achieve common objectives. This distributed decision-making capability enhances their adaptability, resilience, and agility in response to changing circumstances or attacks.

3. **Synchronization and Coordination**. Swarm drones can achieve high levels of synchronization and coordination in their movements and actions. They can execute

complex flight patterns, maintain formation integrity, and perform collaborative tasks, such as target tracking, surrounding targets, or distributing payloads.

4. **Scalability.** Swarm drones are highly scalable in terms of the number of drones involved. They can rapidly increase or decrease their swarm size based on the mission requirements or to confuse and overwhelm defences. This scalability makes them adaptable to different scenarios and difficult to predict.

5. **Redundancy and Robustness.** Swarm drones exhibit redundancy, meaning that the loss of individual drones does not significantly affect their overall effectiveness. The loss of several drones can be quickly compensated by the remaining swarm members, ensuring the continuity of their mission objectives. This redundancy enhances their robustness and resilience to countermeasures.

6. **Cooperative Attacks**. Swarm drones can engage in cooperative attacks, where multiple drones work together to execute a synchronized offensive action. This cooperative behaviour allows them to combine their capabilities, such as surrounding a target from multiple directions, overwhelming defences, or executing complex attack patterns.

B. Swarm Drone Threats

1. **Overwhelming Defences.** Swarm drones can saturate and overwhelm traditional defence systems, including anti-aircraft missiles, surface-to-air guns, or electronic warfare measures. The large number of drones can exhaust or confuse defence mechanisms, making it challenging to effectively engage and neutralize all incoming threats.

2. **Difficult Target Acquisition.** Swarm drones can present difficulties in target acquisition and tracking due to their small size, rapid movement, and close proximity to each other. This makes it challenging for radars and sensors to differentiate between individual drones and accurately track their positions, velocities, and intentions.

3. **Collaborative Attacks.** Swarm drones can execute coordinated attacks by exploiting vulnerabilities in defences. They can simultaneously approach a target from multiple angles or execute diversionary tactics, making it difficult for defenders to prioritize and effectively engage the swarm.

4. **Distributed Threats**. Swarm drones may distribute their payloads across multiple drones, increasing the potential damage they can inflict. By dispersing their payloads among swarm members, they can mitigate the impact of individual drone losses and maintain the ability to deliver their intended effects.

5. **Information Warfare**. Swarm drones can leverage information warfare techniques to confuse or deceive defenders. They can employ electronic warfare measures,

such as jamming or spoofing, to disrupt communication and coordination among defenders or manipulate their sensor systems.

Understanding the characteristics and threats posed by swarm drones is essential for developing effective countermeasures. These countermeasures may involve advanced detection and tracking systems, rapid engagement capabilities, autonomous or semi-autonomous defensive systems, and strategies to disrupt the swarm's communication and coordination. Addressing these challenges requires a comprehensive understanding of swarm drone behaviours, evolving technologies, and innovative defence mechanisms.

Fig1- Swarm Drones Army Day 2021

C. **Swarm Drone Threat Assessment**

Swarm drones present significant threats across various domains, including military operations, critical infrastructure, public safety, and civilian populations. Conducting a comprehensive threat assessment is essential for understanding the potential impacts and vulnerabilities associated with swarm drone attacks. Here are key elements to consider in a swarm drone threat assessment:

1. **Physical Damage**. Swarm drones can pose a direct physical threat by carrying explosives, chemical agents, or other payloads. They can target infrastructure, military assets, or densely populated areas, potentially causing significant damage to buildings, vehicles, or critical facilities.

2. **Surveillance and Reconnaissance.** Swarm drones equipped with cameras, sensors, or other intelligence-gathering capabilities can conduct surveillance and reconnaissance missions. They can collect valuable information about military deployments, sensitive installations, or critical infrastructure, potentially compromising security and operational integrity.

3. **Targeted Attacks**. Swarm drones can execute targeted attacks against specific individuals, high-value assets, or critical systems. They can coordinate their actions to overwhelm personal security details, breach perimeter defences, or exploit vulnerabilities in cyber security systems, leading to potential harm, data breaches, or disruption of critical services.

4. **Disruption of Communications and Networks**. Swarm drones can employ electronic warfare techniques to disrupt communications networks, including radio frequencies, Wi-Fi, or cellular networks. By jamming or spoofing signals, they can hamper the ability to communicate, coordinate responses, or access critical information, impacting military operations or emergency response capabilities.

5. **Psychological Impact**. Swarm drone attacks can have significant psychological effects on targeted populations. The visual spectacle and perceived threat of multiple drones flying in synchronized patterns can cause fear, panic, and anxiety among individuals, impacting public safety and disrupting normal activities.

6. **Cyber Threats**. Swarm drones can be used as platforms for cyber-attacks, such as deploying malware, conducting network intrusions, or launching distributed denial-of-service (DDoS) attacks. By infiltrating networks or exploiting vulnerabilities, swarm drones can compromise critical systems, steal sensitive data, or disrupt online services.

7. **Countermeasure Adaptability.** Swarm drones have the ability to adapt their tactics and behaviour in response to defensive countermeasures. They can employ evasive manoeuvres, change formation, or employ decoys to mitigate the effectiveness of defensive systems, making it challenging to neutralize the swarm.

When conducting a swarm drone threat assessment, it is crucial to consider the specific context and environment in which the threat exists. Factors such as geographical location, critical infrastructure vulnerabilities, operational requirements, and potential targets should be evaluated to determine the level of threat posed by swarm drones. This assessment can inform the development of effective countermeasures, including early detection systems, integrated defensive networks, training and awareness programs, and the deployment of specialized counter-swarm technologies.

D. **Successful Swarm Attacks**

In the past decade large number of swarm drone attacks have been carried out successfully even when countries had the best of Air Defence systems. Kamikaze Drones are very economical compared to missiles and cannot be easily detected due to their low radar cross section and low altitude flight. Some of the successful drone attacks which could not be detected or counter measures taken are:-

1. **Saudi Arabia (2019).** In September 2019, oil facilities in Saudi Arabia, including the Abqaiq and Khurais oil processing plants, were targeted by a swarm drone attack. The attack was claimed by Houthi rebels in Yemen, who utilized unmanned aerial vehicles (UAVs) in coordination to target the facilities.

This incident highlighted the vulnerability of critical infrastructure to swarm drone attacks.

2. **Syria (2020).** Swarm drone attacks have been observed during the ongoing conflict in Syria. Various factions and armed groups have employed small drones, often in swarms, to carry out surveillance, reconnaissance, and occasionally as weapons platforms. These drones have been used in both offensive and defensive operations, posing challenges to military forces operating in the region.

3. **Armenia and Azerbaijan (2020).** During the conflict between Armenia and Azerbaijan over the Nagorno-Karabakh region, swarm drones played a significant role. Both sides utilized small, inexpensive quad copters equipped with explosives or small munitions to carry out attacks against military targets. These swarm drone attacks showcased the evolving nature of modern warfare and the potential impact of drone technology on the battlefield.

4. **Yemen (2021).** Yemen has witnessed multiple swarm drone attacks in recent years. Houthi rebels have employed drones, including both explosive-laden and surveillance-oriented models, in large numbers to target military installations, infrastructure, and airports in Saudi Arabia and within Yemen itself. These swarm drone attacks have posed challenges for the Saudi-led coalition and have raised concerns about the proliferation and use of this technology by non-state actors.

5. **Venezuela (2018).** In August 2018, during a military parade in Caracas, Venezuela, President Nicolás Maduro was targeted in an alleged assassination attempt using swarm drones. Several drones carrying explosives detonated in the vicinity of the event. While the attack was unsuccessful, it raised concerns about the potential use of swarm drones for high-profile political assassinations.

6. **Crimea 29 Oct 22**. Ukraine used Nine drones in swarm formation and carried out a "massive" attack on the Black Sea Fleet in the Crimean port city of Sevastopol, damaging one warship.

Swarm drones present unique challenges compared to traditional missile threats, which can contribute to the perceived limitations of existing defence systems. Swarm drones typically consist of a large number of small, agile drones that can overwhelm traditional defence systems designed to counter larger threats like missiles or aircraft. The sheer volume of targets can strain the capability of existing systems to engage and intercept all of them effectively. Swarm drones often operate with decentralized decision-making capabilities, meaning they can autonomously adapt their flight paths and formations based on real-time information or communication with other drones. This dynamic and adaptive behaviour can make it challenging for existing defence systems to accurately track and predict their movements. Thus a different system which can cover a wide area and is economical is required to counter swarm drones and DEW fits the bill.

III. DIRECT ENERGY WEAPONS (DEWS)

Direct Energy Weapons (DEWs) represent a new frontier in military technology, offering the potential to revolutionize warfare and security strategies. Unlike traditional kinetic weapons that rely on projectiles or explosives, DEWs utilize directed energy beams, such as lasers or microwaves, to inflict damage on targets. DEWs operate at the speed of light, offering rapid and precise engagement capabilities. The concept of DEWs has been explored for decades, but recent advancements in technology and increasing global security concerns have propelled their development and deployment to the forefront of military research. DEWs offer numerous advantages over conventional weapons, including enhanced accuracy, virtually unlimited ammunition, reduced logistics burden, and the ability to engage multiple targets simultaneously. The potential applications of DEWs are extensive. They can be utilized for air and missile defence, providing rapid response and interception capabilities against incoming threats. DEWs can also be employed in ground-based operations, offering enhanced precision and non-lethal effects for crowd control or area denial. Furthermore, DEWs can be integrated into maritime platforms for ship self-defence or countering small boat threats.

A. Types of DEWs.

DEWs can be classified into different types based on the energy source employed, such as laser-based, microwave-based, particle beam weapons, or radio frequency weapons. Each type has its own unique characteristics and operational capabilities, making them suitable for specific scenarios and target sets.

1. Laser-Based DEWs.

a. Laser-based direct energy weapons utilize focused beams of light to deliver energy to a target. These weapons operate by generating a high-intensity laser beam and directing it towards the intended target. The laser energy can be absorbed by the target's surface, leading to heating, melting, or vaporization. Laser-based DEWs offer several advantages, including high precision, speed of light delivery, and the ability to engage targets at various distances. They can be further categorized based on their power levels, such as low-power lasers for non-lethal applications and high-power lasers for offensive purposes. Laser-based DEWs have found applications in areas such as anti-aircraft defence, counter-electronics, and precision targeting.

b. The laser beam can be generated through different methods, such as solid-state lasers, fibre lasers, or gas lasers. These technologies enable the production of intense laser beams with exceptional beam quality, coherence, and control. The advantages of laser-based DEWs lie in their accuracy, speed, and scalability. The high precision of laser beams allows for pinpoint targeting and the ability to selectively engage specific components of a target, minimizing collateral damage. Additionally, lasers have a rapid engagement time, enabling near-instantaneous

delivery of energy onto the target. The scalability of laser systems allows for adjustable power levels, making them suitable for various mission requirements and threat scenarios.

c. Laser-based DEWs have a wide range of potential applications across different military domains. In the field of air and missile defence, lasers can be used to intercept and destroy incoming projectiles, including missiles, rockets, or unmanned aerial vehicles (UAVs). By rapidly engaging and neutralizing these threats, laser-based DEWs provide an effective defence mechanism with a high rate of success. Furthermore, laser-based DEWs can be employed in ground-based operations, offering capabilities such as precision strike, target designation, and counter-electronics. These weapons can disable or destroy enemy equipment, such as vehicles, communication systems, or sensors, thus disrupting enemy operations and providing a tactical advantage.
d. Another consideration is the power requirements for laser-based DEWs. Generating and sustaining high-energy laser beams demands substantial power sources and efficient thermal management systems to prevent overheating and ensure continuous operation. Advances in power sources, such as solid-state or fibre lasers, have significantly improved the energy efficiency and power density of laser systems.
e. One of the challenges associated with laser-based DEWs is atmospheric attenuation. Laser beams can experience losses due to scattering, absorption, or degradation as they propagate through the atmosphere, particularly in adverse weather conditions. These factors can affect the range and effectiveness of laser-based DEWs, necessitating mitigation techniques such as adaptive optics or wavelength optimization.

Fig 2: DRDO Developed Laser Based DEW

2. Microwave-Based DEWs.

a. Microwave-based direct energy weapons employ focused microwave beams to disable or destroy targets. These weapons operate by emitting high-frequency electromagnetic waves that interact with the target's electronics, causing disruptions, damage, or destruction. Microwave-based DEWs have advantages such as long-range capabilities, ability to penetrate various materials, and potential for non-lethal effects. They can be utilized for disabling enemy electronics, neutralizing explosive devices, or crowd control purposes. However, they face challenges such as atmospheric attenuation and the need for precise targeting to ensure effectiveness.

b. Microwaves, which are electromagnetic waves with wavelengths ranging from one meter to one millimetre, can be generated by various means such as magnetrons, klystrons, or solid-state devices. Microwave-based DEWs emit intense microwave beams that can be directed towards the target with precision and control.

c. One of the key advantages of microwave-based DEWs is their ability to affect a wide range of targets. Microwaves have the capability to penetrate solid materials, including metal and composite structures, making them effective against electronic systems, sensors, and communications equipment. Microwave beams can induce high levels of electrical current within target components, resulting in damage or disruption.

d. Microwave-based DEWs offer unique operational characteristics. They can engage multiple targets simultaneously, allowing for the engagement of multiple threats within a short timeframe. Additionally, microwave beams can be electronically steered, providing flexibility in target tracking and engagement.

e. The applications of microwave-based DEWs are diverse. In the field of air defence, these weapons systems can be used to disable or disrupt electronic systems on enemy aircraft, drones, or missiles, rendering them ineffective or causing them to malfunction. By targeting critical components such as guidance systems or communication links, microwave-based DEWs can neutralize threats without causing physical damage or collateral harm.

f. In ground-based operations, microwave-based DEWs can be employed for electronic warfare purposes. They can disrupt or disable enemy communication networks, radar systems, or other electronic systems, degrading the adversary's ability to coordinate and operate effectively. Microwave beams can also be utilized for crowd control or non-lethal effects, such as inducing temporary pain or discomfort to deter or disperse hostile individuals.

g. Challenges associated with microwave-based DEWs include the development of compact and efficient power sources, as well as managing the heat generated by high-power microwaves. Advancements in solid-state microwave technologies have improved power efficiency and reduced the size and weight of microwave systems, making them more feasible for deployment.

3. Other Types of DEWs

a. **Particle Beam Weapons.** Particle beam weapons utilize charged particles, such as electrons or ions, to generate a high-energy beam that can be directed towards the target. These beams can cause damage by delivering a concentrated stream of particles to the target, leading to thermal or mechanical effects.
b. **Radio Frequency (RF) Weapons**. RF weapons employ high-power radio frequency waves to disrupt or disable electronic systems. They can interfere with or overload electronic circuits, causing malfunctions or damage to the target's electronics. RF weapons are particularly effective against communication systems, sensors, and other electronic devices.
c. **High-Powered Microwaves (HPM)**. HPM weapons produce short pulses of high-energy microwave radiation that can disrupt or destroy electronic systems. They can induce electrical surges, overload circuits, or cause electromagnetic interference, leading to temporary or permanent damage to the target's electronics.
d. **Sonic Weapons**. Sonic weapons use intense sound waves or infrasound to incapacitate or deter targets. These weapons can generate high-pressure acoustic waves that can cause physical discomfort, disorientation, or even damage to the target's auditory system.
e. **Electromagnetic Pulse (EMP) Weapons**. EMP weapons release a short burst of electromagnetic energy that can disrupt or damage electronic systems over a wide area. They can be designed to emit a high-energy pulse that induces electrical currents in electronic devices, causing them to malfunction or fail.
f. Each type of DEW has its own unique characteristics, advantages, and limitations. The selection of a specific DEW type depends on factors such as the target type, operational requirements, and desired effects. Advances in technology and research continue to drive the development of new and improved DEW systems, expanding the range of options available for military and security applications.

IV. ANTI DRONE TECHNOLOGY

Anti-drone technology utilizing lasers involves the use of directed energy beams to disable or destroy drones by overheating or burning critical components. Laser systems offer precision targeting, fast engagement times, and potential long-range operation. However, they can be affected by atmospheric conditions and may have limited effectiveness against drones with reflective or heat-resistant materials. On the other hand, high-power microwave (HPM) devices generate electromagnetic pulses to disrupt or disable electronic systems on drones, regardless of their construction. HPM devices are effective against a wide range of drones, but their range is typically shorter than lasers, and their effectiveness depends on the drone's shielding and hardening against electromagnetic interference. Both laser systems and HPM devices can be

integrated into existing defence systems and have their own cost considerations and potential regulatory restrictions. The choice between these technologies depends on specific requirements and the nature of the drone threat. A comparison Table outlining the main characteristics of laser systems, high-power microwave (HPM) devices, and other Directed Energy Weapon (DEW) technologies as anti-drone technologies is as under:-

Anti-Drone Technology	**Laser Systems**	**High-Power Microwave (HPM)**	**Other DEW Technologies**
Principle of Operation	Directed energy beams to disable/destroy drones	Electromagnetic pulses to disrupt/disable electronic systems	Various energy-based methods to disable/disable drones
Targeted Components	Critical drone components (sensors, motors, communication systems)	Electronic systems (communication, control, navigation)	Electronic systems, structural integrity
Advantages	Precision targeting, fast engagement times, potential long range	Effective against a wide range of drones, regardless of construction	Versatility, ability to target multiple components
Limitations	Affected by atmospheric conditions, limited effectiveness against reflective/heat-resistant drones	Shorter range compared to lasers, effectiveness depends on drone shielding/hardening	Range limitations, potential collateral damage
Potential Impact	Overheats/burns critical components, disables/destroys drones	Disrupts control/navigation, may damage electronics	Disables electronics, disrupts systems, damages structure
Integration Potential	Can be integrated into existing defense systems	Can be integrated into existing defense systems	Can be integrated into existing defense systems
Cost	Expensive due to high-energy laser technology	Moderate cost, depends on power requirements	Cost varies depending on the specific technology

The above table only provides a general overview, and the specific performance and effectiveness of DEW technologies can vary based on various factors, as mentioned earlier. Additionally, regulations and legal considerations surrounding anti-drone technologies differ among countries, so it's crucial to consult local laws and regulations when implementing them. The category of "Other DEW Technologies" encompasses a broad range of energy-based methods that are not specifically categorized as lasers or high-power microwave devices.

A. **Strategies for Swarm Drone Defeat with DEWs**

Defeating swarm drones using direct energy weapons (DEWs) requires careful planning and the implementation of effective strategies. Here are some key strategies to consider when utilizing DEWs to counter swarm drones:

1. **Target Identification and Tracking**. Accurate target identification and tracking are crucial for effective engagement. DEW systems should be equipped with advanced sensors, such as radar, lidar, or electro-optical systems, capable of detecting and tracking multiple swarm drones simultaneously. Real-time data fusion and target prioritization algorithms can help in identifying the most imminent threats and directing the DEW beams accordingly.

2. **Scalability and Rapid Engagement**. Swarm drones operate in large numbers, necessitating DEW systems with scalable capabilities. DEWs should be capable of engaging multiple targets simultaneously or in quick succession. This requires robust power generation, beam control, and thermal management systems to ensure sustained and rapid engagement without compromising effectiveness.

3. **Precision Energy Delivery**. DEWs should deliver precise and controlled energy to neutralize swarm drones effectively. By adjusting the power, duration, and focus of the energy beams, DEWs can disable or destroy individual swarm drones while minimizing collateral damage to surrounding structures or assets. High beam quality and stabilization technologies are essential for accurate energy delivery.

4. **Countermeasures and Adaptive Tactics**. Swarm drones may employ countermeasures to evade or mitigate DEW attacks. DEW systems should be capable of countering these tactics by utilizing adaptive beam steering, frequency hopping, or modulation techniques to maintain effective engagement. Real-time analysis of swarm drone behaviours and tactics can help in adapting DEW strategies to overcome countermeasures.

5. **Integration with Sensor Networks and Command Systems**. DEWs should be integrated into existing sensor networks and command systems for comprehensive situational awareness and effective coordination. Sharing real-time data with other defence systems, such as radars, electronic warfare systems, or air defence networks, enhances the overall effectiveness of swarm drone defeat operations.

6. **Environmental Considerations**. DEW systems should account for environmental factors that can affect their performance, such as atmospheric conditions, weather, or terrain. Understanding the impact of these factors on beam propagation and energy absorption is crucial for optimizing DEW effectiveness and range. Adaptive optics or beam control technologies can help mitigate environmental effects.

7. These strategies, when combined with continuous research, development, and testing, can enhance the effectiveness of DEWs in countering swarm drones. It is essential to consider the evolving nature of swarm drone tactics and technologies, conducting regular assessments and adapting DEW strategies accordingly to stay ahead of emerging threats.

B. **Technical Considerations**

When developing and deploying direct energy weapons (DEWs) for countering swarm drones, several technical considerations must be taken into account. These considerations help ensure the effectiveness, reliability, and safety of the DEW systems. Here are some key technical considerations to keep in mind:

1. **Power and Energy Requirements**. DEWs require substantial power and energy to generate and sustain the directed energy beams. Adequate power sources, such as generators or power grids, must be available to supply the necessary energy for continuous operation. Power management systems should be designed to optimize power usage and minimize energy wastage.

2. **Beam Control and Tracking**. Accurate beam control and tracking capabilities are essential for precise targeting of swarm drones. DEW systems should have advanced beam control mechanisms, including fast-steering mirrors, gimbal systems, or phased array antennas, to direct the energy beams towards the intended targets. Real-time tracking algorithms and high-speed servo systems enable the DEW to maintain accurate tracking, even against agile and evasive swarm drones.

3. **Range and Scalability.** DEW systems should have an effective range that allows engagement of swarm drones at various distances. The range depends on factors such as the power of the DEW, atmospheric conditions, and the capabilities of the beam propagation system. DEWs should also be scalable to engage multiple swarm drones simultaneously or adapt to changing swarm sizes, ensuring that they can effectively counter dynamic threats.

4. **Thermal Management.** DEWs generate intense heat during operation, which can lead to thermal issues that may affect system performance and longevity. Proper thermal management is crucial to dissipate heat and maintain optimal operating temperatures. Cooling systems, heat sinks, and thermal insulation measures should be employed to prevent overheating and ensure the reliability of the DEW system.

5. **System Integration and Interoperability**. DEWs need to be integrated into existing defence systems and command networks for effective coordination and interoperability. Integration with sensor networks, radar systems, and command-and-control systems allows for seamless data sharing, target identification, and coordinated engagement. Standardized interfaces and protocols facilitate interoperability with other defence assets.

6. **Safety Considerations**. DEW systems must prioritize safety to prevent unintended harm to personnel, bystanders, or unintended targets. Safety mechanisms, such as

beam shut-off systems, fail-safe mechanisms, and interlocks, should be implemented to ensure that the DEW operates within predetermined safety parameters. Safety protocols and training for operators and maintenance personnel are essential to minimize the risk of accidents.

7. **Reliability and Maintenance**. DEW systems should be designed for high reliability to ensure sustained operational readiness. Regular maintenance, calibration, and testing are necessary to identify and rectify any system issues or degradation. Spare parts availability, repair procedures, and a robust logistics support system contribute to maintaining the reliability and availability of DEW systems.

8. **Testing and Evaluation**. Rigorous testing and evaluation are crucial for DEW systems to verify their performance, validate their capabilities, and identify any areas for improvement. Controlled testing environments, such as test ranges or simulated scenarios, allow for comprehensive evaluation of the DEW's effectiveness, beam quality, range, and engagement capabilities.

C. **Operational Considerations**

In addition to technical considerations, operational considerations play a vital role in the effective use of direct energy weapons (DEWs) for countering swarm drones. These considerations encompass factors related to deployment, operational planning, training, and integration with existing defence systems. Here are some key operational considerations to keep in mind:

1. **Mission Planning and Engagement Tactics**. Effective mission planning is critical to maximize the use of DEWs against swarm drones. This includes identifying operational objectives, defining engagement criteria, and determining optimal deployment locations for DEW systems. Developing specific engagement tactics and procedures for different swarm scenarios can enhance the overall effectiveness of DEW operations.

2. **Target Prioritization**. Proper target prioritization is crucial when countering swarm drones. Not all swarm drones may pose an immediate threat, and resources should be allocated to engage the most critical targets first. A robust target identification and tracking system, combined with real-time analysis and decision-making capabilities, enables effective target prioritization and engagement sequencing.

3. **Integrated Defence Networks**. DEW systems should be integrated into existing defence networks and command-and-control systems. This integration allows for seamless communication, data sharing, and coordinated engagements with other defensive assets, such as radar systems, surface-to-air missile systems, or electronic warfare platforms. Integration enhances situational awareness, target identification, and engagement effectiveness.

4. **Training and Operator Proficiency**. Proper training of DEW operators is essential for their effective and safe use. Operators should receive comprehensive training on the functionality, operation, and maintenance of DEW systems. Training should also include scenario-based exercises and simulations to develop proficiency in target engagement, beam control, and tracking techniques. Regular training updates and proficiency assessments help ensure optimal operator performance.

5. **Situational Awareness and Intelligence**. Accurate situational awareness is vital for effective DEW operations. Integration with intelligence systems, such as surveillance radars, unmanned aerial vehicles, or intelligence gathering platforms, provides real-time information on swarm drone activities, their capabilities, and tactics. This enables proactive engagement, timely response, and effective countermeasures.

6. **Continuous Evaluation and Improvement**. Ongoing evaluation and assessment of DEW operations are essential to identify areas for improvement and to adapt to evolving swarm drone threats. Lessons learned from operational experiences and feedback from operators should be incorporated into future planning, training, and system enhancements. Collaboration with research and development institutions, industry partners, and other defence agencies contributes to advancing DEW capabilities.

7. **Logistic Support and Maintenance** A robust logistic support system is necessary to ensure the operational availability of DEW systems. Adequate spare parts, maintenance procedures, and personnel training on system maintenance and repair are crucial to minimize downtime. Efficient logistic support helps sustain operational readiness and enhances the overall effectiveness of DEW operations.

D. Challenges and Future Directions

While direct energy weapons (DEWs) hold promise in countering swarm drones, several challenges and areas for future development must be addressed to enhance their effectiveness. Here are some key challenges and future directions to consider:

1. **Power and Energy Efficiency**. DEWs require substantial power to generate and sustain the directed energy beams. Enhancing power generation and energy efficiency is crucial to increase operational endurance and reduce logistical constraints. Advancements in power storage technologies, compact energy sources, and improved energy conversion efficiency can significantly enhance DEW capabilities.

2. **Range and Scalability**. DEWs need to operate effectively across varying distances and engage multiple swarm drones simultaneously. Extending the operational range and scalability of DEW systems can provide greater flexibility and coverage. Advances in beam propagation techniques, adaptive optics, and power scaling technologies can enhance the range and scalability of DEWs.

3. **Countermeasures and Adaptive Tactics.** Swarm drones are likely to employ countermeasures to evade or mitigate DEW attacks. DEWs need to continually adapt to these tactics and overcome them effectively. Research and development efforts should focus on developing counter-countermeasure technologies, such as advanced beam control, frequency agility, or rapid re-targeting capabilities.

4. **Miniaturization and Mobility**. DEWs should be developed in compact, lightweight forms for enhanced mobility and flexibility. The miniaturization of DEW components, power sources, and thermal management systems can enable their integration into mobile platforms, such as ground vehicles, unmanned aerial vehicles, or ships. This enhances the versatility and rapid deployment capabilities of DEWs.

5. **Integration with Sensor Networks and Autonomous Systems**. DEWs should be seamlessly integrated with sensor networks, autonomous systems, and artificial intelligence (AI) capabilities for enhanced situational awareness and autonomous engagement. Collaborative engagement between DEWs and other defence systems, such as radar networks, unmanned systems, or AI-enabled decision-making systems, can optimize swarm drone defeat operations.

6. **System Cost and Affordability.** DEW systems must become more cost-effective and affordable to facilitate widespread deployment. Advances in manufacturing processes, economies of scale, and component integration can help reduce the overall cost of DEW systems. Collaborations between defence agencies, industry partners, and research institutions can drive cost reduction and increase accessibility.

E. Implications for Military Strategies and Tactics

The emergence of direct energy weapons (DEWs) and their potential to counter swarm drones has significant implications for military strategies and tactics. Here are some key implications to consider:

1. **Enhanced Defence Against Swarm Threats**. Swarm drones pose unique challenges due to their ability to overwhelm traditional defence systems. DEWs offer a new layer of defence, providing the capability to engage and neutralize multiple swarm drones simultaneously. Integrating DEWs into existing defence systems enhances overall situational awareness and increases the effectiveness of defence against swarm threats.

2. **Force Multiplier**. DEWs can serve as force multipliers by augmenting existing military capabilities. They provide a versatile and rapid response option for countering swarm drone attacks. DEWs can be deployed alongside other defensive assets, such as missile systems or electronic warfare platforms, creating a layered defence approach that improves the overall effectiveness of military operations.

3. **Dynamic and Adaptive Tactics.** Swarm drones are known for their agility, coordination, and adaptive tactics. DEWs must respond with equally dynamic and adaptive tactics to effectively engage and neutralize swarm threats. Military strategies need to account for the evolving nature of swarm tactics and the ability of DEWs to adapt their engagement parameters, beam control, and tracking to counter these tactics effectively.

4. **Integration of Sensors and Networks.** DEWs operate most effectively when integrated into a network-centric defence system. This integration allows for seamless information sharing, target identification, and coordinated engagement with other sensors and defence assets. Military strategies should emphasize the integration of sensor networks, intelligence systems, and command-and-control structures to optimize the deployment and effectiveness of DEWs.

5. **Operational Flexibility and Rapid Deployment**. DEWs can be deployed on various platforms, including ground-based systems, airborne platforms, or naval vessels. This operational flexibility allows for rapid deployment and engagement in different operational scenarios. Military strategies should incorporate the ability to rapidly deploy DEWs to areas of need, adapting to the dynamic nature of swarm threats and providing timely defence.

6. **Training and Doctrine Development**. The introduction of DEWs necessitates the development of new training programs and doctrines. Military personnel need to be trained in the operation, maintenance, and tactical utilization of DEWs. Doctrine development should encompass tactics, techniques, and procedures for integrating DEWs into overall military strategies, including swarm drone engagement and coordination with other defence assets.

F. **Case Study**

1. **Tactical High-Power Operational Responder (THOR) Microwave Weapon.** The Tactical High-Power Operational Responder (THOR) is a real-world microwave weapon developed by the United States Air Force Research Laboratory (AFRL). THOR is designed to be a non-lethal directed energy weapon system that uses high-power microwaves to disable or destroy enemy electronic systems. It is an ideal weapon for swarm of Drones. It was tested on 5 April 2023 in an engagement with a swarm of multiple targets at the Air Force Research Laboratory (AFRL) located at Kirtland Air Force Base, USA. Here are some key points about THOR.

Fig 3: Tactical High Power Operational Responder(THOR).

Courtesy Air force Tech Magazine

a. **Function.** THOR is primarily designed to counter and neutralize threats posed by unmanned aerial systems (drones) and other electronic systems used by adversaries. It targets the electronic components of these systems, causing disruption or damage.

b. **Microwave Technology.** THOR operates by generating and releasing a concentrated beam of high-power microwaves. These microwaves can be directed towards a specific target, and upon impact, they interact with the electronic components, inducing strong electromagnetic fields that overload and damage the circuitry.

c. **Non-Lethal Weapon**. THOR is classified as a non-lethal weapon, meaning it is designed to incapacitate or disable the targeted systems without causing significant harm to human life. It provides a more precise and controlled alternative to kinetic weapons like missiles or bullets.

d. **Versatility and Scalability**. THOR is intended to be a versatile system that can be deployed in various operational environments. It can be mounted on different platforms such as vehicles, ships, or aircraft, depending on the mission requirements. The system is also scalable, allowing for different power levels to be utilized depending on the target and the desired effect.

e. **Range and Effectiveness**. The exact range and effectiveness of THOR have not been publicly disclosed in detail. However, it is known that THOR has been successfully tested against a range of targets, including unmanned aerial systems.

The system is designed to be highly effective in disrupting or disabling the electronic systems of these threats.

It is important to note that the information available about THOR may be limited due to the classified nature of the technology. The development and deployment of military systems like THOR are typically subject to strict operational security considerations.

G. **Recommendations for Further Research**

Further research in the field of direct energy weapons (DEWs) and their effectiveness in countering swarm drones can contribute to their continued development and optimization. Here are some recommendations for further research:

1. **Comprehensive Field Testing**. Conducting comprehensive field tests that simulate real-world swarm drone scenarios is crucial to assess the performance of DEWs in practical environments. These tests should consider various factors such as different swarm sizes, drone behaviours, environmental conditions, and engagement distances. The data collected from these tests can provide valuable insights into the capabilities and limitations of DEWs.

2. **Experimental Validation of Simulation Results**. Validate simulation results through physical testing and evaluation to ensure their accuracy and reliability. Comparative studies between simulation outcomes and real-world test results can help verify the effectiveness of DEWs in countering swarm drones and identify areas where improvements are needed.

3. **Countermeasures and Adaptive Tactics**. Research should focus on understanding and countering swarm drone countermeasures and adaptive tactics. Investigate methods to improve DEW effectiveness against advanced swarm drone behaviours such as evasive manoeuvres, decentralized decision-making, or rapid reconfiguration. This includes developing advanced beam control algorithms, frequency agility techniques, and tracking strategies to overcome these challenges.

4. **Power Generation and Energy Efficiency**. Explore advancements in power generation technologies and energy-efficient components to enhance the operational endurance of DEWs. Investigate alternative power sources, such as compact and high-energy-density batteries or fuel cells that can sustain DEW operations for longer durations without compromising performance.

5. **Scalability and Range Extension**. Develop techniques to extend the operational range and scalability of DEWs. This includes research into beam propagation optimization, adaptive optics, and power scaling technologies to enable DEWs to engage swarm drones effectively over larger distances and against larger swarm formations.

6. **Integration with Sensor Networks and Autonomous Systems**. Investigate the integration of DEWs with sensor networks, autonomous systems, and artificial intelligence (AI) capabilities. Develop algorithms and decision-making frameworks

that enable DEWs to autonomously detect, track, and engage swarm drones in collaboration with other defence assets. This integration can enhance situational awareness, optimize engagement strategies, and improve overall defense capabilities.

7. **Human Factors and Training**. Study the human factors associated with DEW operations, including operator training, situational awareness, and decision-making under high-stress scenarios. Develop training programs that familiarize operators with DEW systems, their capabilities, and potential swarm drone engagement tactics. Additionally, consider human-machine interface improvements to enhance operator effectiveness and reduce response times.

8. **Cost Optimization and Affordability**. Research should focus on cost optimization measures to make DEW systems more affordable and accessible. Investigate manufacturing processes, component integration, and economies of scale to reduce overall system costs without compromising performance or safety.

V. CONCLUSION

In conclusion, the development and utilization of direct energy weapons (DEWs) for countering swarm drones hold significant promise. While specific case studies and experimental results may be limited in the public domain, the findings and trends in this field indicate the potential effectiveness of DEWs in addressing the swarm drone threat. DEWs offer advantages such as the ability to engage multiple targets simultaneously, adaptability to evolving swarm tactics, and integration with sensor networks and autonomous systems. They have the potential to enhance defence capabilities, serve as force multipliers, and create dynamic and adaptive tactics against swarm drone attacks.

However, further research is essential to advance the field of DEWs and swarm drone defeat. Comprehensive field testing, experimental validation of simulation results, and a focus on countering swarm drone countermeasures and adaptive tactics are recommended. Additionally, improvements in power generation, scalability, integration with sensor networks, and addressing human factors and training are areas that warrant further exploration. Overall, continued research and development efforts, combined with real-world testing and validation, will further enhance our understanding of DEWs' capabilities in countering swarm drones. The evolving nature of swarm drone threats calls for ongoing advancements in DEW technologies, strategies, and tactics to maintain a robust defence against these emerging challenges.

References

1. Zachary Kallenborn, “InfoSwarms: Drone Swarms and Information Warfare” The US Army War College Quarterly: Parameters, Number 2 Volume 52, Number 2 Summer Issue 5-18-2022
2. M. Dorigo, M. Birattari, and T. Stutzle, "Swarm robotics: A review from the swarm engineering perspective," IEEE Transactions on Robotics, vol. 17, no. 4, pp. 446-466, 2001.
3. H. Hamann and F. H. Durr, "Swarm robotics: A formal approach," in Swarm Robotics: A Formal Approach, Springer, 2018, pp. 3-26.
4. K. Suresh Kumar and Y. Raghu Reddy, "The future of drone swarms: Applications and challenges," International Journal of Swarm Intelligence Research, vol. 11, no. 4, pp. 1-19, 2020.
5. D. Lefeuvre, A. Oertel, and C. Cariou, "Cooperative swarm drones for surveillance missions: Challenges and opportunities," in 2018 International Conference on Unmanned Aircraft Systems (ICUAS), 2018, pp. 148-153.
6. M. Aggarwal, M. Shukla, and B. Mehta, "Swarm robotics: A review on the challenges and constraints," in 2021 International Conference on Inventive Computation Technologies (ICICT), 2021, pp. 1572-1577.
7. A. A. Abu-Hudrouss and A. Rida, "Swarm drone networks: Challenges and future directions," in 2020 International Conference on Innovative Trends in Communication and Computer Engineering (ITCE), 2020, pp. 163-167.1. Fisher, R. M., Corman, J., & Finneran, M. (2017). Directed Energy Weapons: Promise and Prospects. Center for a New American Security.
8. Hafner, J. L., Johnson, E. A., & Stein, G. L. (2018). Directed Energy Warfare: A New Generation of Defense. Journal of Directed Energy, 4(1), 1-9.
9. Pike, J. (2020). Directed-Energy Weapons. GlobalSecurity.org.
10. U.S. Department of Defense. (2017). Report on Directed Energy Weapon Systems.
11. U.S. Department of Defense. (2020). The Role of Directed Energy Weapons in Counter-Unmanned Aircraft Systems.
12. Zaytsev, A. (2019). Direct Energy Weapons: Current Status and Future Prospects. Military Thought, 28(3), 44-56.
13. Davis, B. L., & Hulka, W. J. (2018). Directed Energy Weapons: Technology, Applications, and Limitations. In Proceedings of the 59th Annual Symposium on Explosives and Pyrotechnics (pp. 176-191).
14. Gervais, D. (2019). Directed Energy Weapons: A Futuristic Technology Enters the Present. Journal of Conflict Studies, 39(2), 66-89.
15. Kester, M., Blough, J., & Nitsch, C. (2017). High Power Microwave (HPM) and Radio Frequency (RF) Directed Energy Weapons (DEWs) for Air Defense

Applications. In 2017 IEEE International Symposium on Technologies for Homeland Security (HST) (pp. 1-6).

16. Koechling, J. M., & Wood, M. C. (2019). The Science and Applications of Directed Energy Weapons. In Directed Energy Summit.
17. Kumar, S., Kumar, A., & Mishra, A. (2017). A Review on Directed Energy Weapons and Its Applications. In 2017 International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC) (pp. 1-4).
18. Lewis, J. (2020). Directed Energy Weapons and the New Era of Warfare. Strategic Studies Quarterly, 14(1), 24-46.
19. Malek, M. M., Al-Odibat, A. O., & Amayreh, A. (2019). Advanced Direct Energy Weapons: A Review. IEEE Access, 7, 99947-99968.
20. Swami, V., & Banerjee, P. (2021). A Review on Laser-Based Directed Energy Weapons for Defense Applications. Optik, 232, 166246.