Research on the Issue of CBRN Drone Attacks in Island Control and Stability Maintenance Operations of the Armed Police Force

Xuan Wang*, Dayong Jiang
College of Equipment Management and Support, Engineering University of PAP, Xi'an, Shaanxi, China
**Corresponding Author.*

Abstract: With the rapid development of military drone technology, its widespread application in military and civilian fields has introduced new security challenges. In particular, the potential threats posed by drones during mission execution present risks to public safety and social stability. This paper aims to explore the potential impact of CBRN (Chemical, Biological, Radiological, and Nuclear) drones on control and stability maintenance operations and corresponding countermeasures. By analyzing the advantages of drones in terms of low cost, high efficiency, and flexibility, this paper examines how drones can serve as effective operational tools and proposes targeted prevention and emergency response measures. The research indicates that drones can swiftly and covertly deliver hazardous substances, posing significant security risks, especially in controlled environments with high population density. The paper suggests establishing a comprehensive counter-drone system, optimizing early warning and defense measures, and strengthening emergency response capabilities to effectively address related threats.

Keywords: Drone; Stability Maintenance Operations; Counter-Drone Defense; Remote Warning; Countermeasures

1. Introduction

With continuous advancements in technology, the application of drone technology in military and security fields has surpassed traditional boundaries, particularly in the deployment of Chemical, Biological, Radiological, and Nuclear (CBRN) weapons. Drones can not only efficiently execute reconnaissance, surveillance, and attack missions but also carry these hazardous weapons, making their delivery and dissemination more covert and effective. Professor Randall K. Nichols' open-access eBook DRONE DELIVERYV OF CBNRECy-DEW WEAPONS, published by New Prairie Press, discusses how drones and unmanned vehicles can serve as effective payload delivery systems for CBRN weapons [1]. The book explores methods and pathways for integrating drones with nuclear, biological, and chemical weapons, cyberattack weapons, and directed-energy weapons. Given the significant international media impact and high social sensitivity of island control and stability maintenance operations, hostile forces may seize the opportunity to disrupt such actions.

In the face of increasingly complex security threats, addressing the potential threat of drones carrying CBRN weapons has become a pressing issue. Strengthening the tracking and early warning capabilities for adversarial weapon systems is crucial to ensuring the successful implementation of control and stability maintenance operations. This paper aims to explore the potential threats posed by the combination of drones and CBRN weapons and their impact on island control and stability maintenance. It reviews cutting-edge research in this field, analyzes the integration of drones and CBRN weapons in both warfare and non-warfare operations, and identifies existing research gaps. Based on the current defense systems, this paper proposes effective strategies for counter-drone defense, remote warning, and response to CBRN threats.

2. Characteristics of CBRN Drone Attacks on Control and Stability Maintenance Operations

2.1 Low Cost and High Cost-Effectiveness

The cost of drones ranges from a few thousand

to tens of thousands of yuan, making them significantly more affordable compared to manned aircraft. In non-warfare sabotage operations, drones possess flight speed and reliability sufficient to support such actions. Additionally, there are almost no technological bottlenecks in developing chemical reagent release devices or biological agent dispersal systems, allowing for low-cost manufacturing and deployment. The resulting destructive effects pose a severe threat to island control and stability maintenance operations, making them a convenient tool for achieving unlawful objectives. Moreover, since drones do not require human pilots, they can carry out missions without exposing the operators. This enables malicious actors to conduct sabotage operations at low cost, with high efficiency and concealment, further increasing the difficulty of preventing such attacks [2].

2.2 Sudden Onset and Difficulty in Prevention

Drones are small, lightweight, and highly maneuverable, allowing them to complete sabotage missions in a short time. Their low-altitude flights are difficult to detect via early warning systems, making it challenging to obtain accurate intelligence [3]. During control and stability maintenance operations, large crowds increase the difficulty of identifying and preventing drone threats. The biochemical weapons they carry can include military-grade toxins and hazardous chemicals such as pesticides, insecticides, and other flammable, explosive, toxic, harmful, or corrosive chemical substances. Additionally, drones can be used to deploy containers carrying fleas, mosquitoes, and other pathogens, mimicking the ceramic bacterial bombs once used by Japan's Unit 731. Such attacks could lead to the spread of epidemics with unforeseeable consequences. At the same time, due to their small size, drones are difficult to detect by traditional security systems, often making it impossible to respond effectively in a short period. This significantly increases the difficulty of emergency response to sudden incidents, leading to more severe consequences.

2.3 Wide Coverage and High Lethality

The combination of CBRN weapons with drones enhances their mobility and rapid delivery capabilities. In control and stability maintenance operations where large crowds gather in confined spaces, such attacks can cause severe casualties and rapid proliferation of harm. Targeted strikes on key locations not only cause direct damage but can also trigger mass panic, stampedes, and secondary injuries. Response forces must manage stability maintenance while also addressing their own protection needs, making the issue of CBRN drone threats particularly complex. Drones can carry a variety of payloads and conduct simultaneous attacks on multiple locations, creating a powerful coordinated disruption effect. This exponentially increases the difficulty of response and rescue efforts, necessitating the development of more sophisticated and flexible countermeasures to address multi-dimensional threats.

3. Countermeasures Against CBRN Drone Disruption in Control and Stability Maintenance Operations

3.1 Establishing a Comprehensive Anti-Drone Disruption System

Efforts should be made from two aspects: contingency planning and military-civilian cooperation. First, a detailed anti-drone disruption contingency plan should be formulated, considering factors such as the timing, location, methods, and targets of potential hostile drone disruptions. Countermeasures should be developed based on key scenarios. Second, collaboration with government and public security propaganda departments should be strengthened by widely setting up warning signs and alert markers, implementing signal jamming and drone countermeasures around critical targets, and maintaining close-range destruction capabilities to ensure a systematic and effective defense strategy. Through multi-party collaboration and rigorous preemptive preparations, anti-drone disruption measures can be swiftly and effectively implemented. Regular inspections and drills should be conducted to continuously improve the overall countermeasure capabilities, ultimately forming a true all-weather defense network.

3.2 Focusing on Remote Warning and Response

To address the threat of drone disruptions in

control and stability maintenance operations, a well-developed remote filtering system must be established to optimize the deployment of defensive forces [4]. Differentiating between air and ground defenses, aerial interception should follow a tiered configuration with layered defenses. Early warning radars must respond promptly to detect sources, while disruption equipment should be specifically targeted for chain-breaking measures. On the ground, security efforts should emphasize information sharing and key area defense. Cooperation mechanisms should be established with public security and national security agencies to enable seamless exchange of intelligence, closely monitoring reports of stolen or lost nuclear, biological, and chemical materials. Special attention should be given to tracking terrorist-related individuals, drone components, and other key people and items. Security checks should be strengthened, and countermeasures should be meticulously implemented. Through multi-party collaboration and rigorous preemptive preparations, anti-drone disruption measures can be swiftly and effectively implemented. Regular inspections and drills should be conducted to continuously improve the overall countermeasure capabilities, ultimately forming a true all-weather defense network.

3.3 Enhancing Anti-Disruption Measures

Considering the CBRN threat, counter-drone measures should focus on three aspects: early warning equipment, interception and disruption equipment, and command and control systems. Early warning measures should emphasize low-altitude radar detection and signal reconnaissance. Interception should focus on radio frequency jamming, information flow disruption, and net-based drone capture. Command and control should prioritize intelligence-driven, digitalized, and highly efficient operations by establishing a streamlined and effective command chain, simplifying decision-making processes, delegating handling authority, and reducing reaction time. This ensures a well-coordinated and multi-pronged response in case of an incident [5]. Continuous optimization of technical methods and command processes should be pursued to achieve a comprehensive, multi-layered countermeasure capability, ensuring rapid response and effective handling of complex situations while minimizing risks to the greatest extent possible.

3.4 Strengthening CBRN Response Capabilities

Opportunities for fundamental training, routine protective exercises, and specialized defense training should be fully utilized to enhance nuclear, biological, and chemical response capabilities [6-8]. Training should cover toxin identification, decontamination procedures, and protective equipment usage, alongside drills simulating unexpected CBRN incidents at stability maintenance sites. Special emphasis should be placed on equipping reconnaissance and protective gear for civilian hazardous chemicals, ensuring full-body protection for task forces, monitoring radioactive contamination, and deploying vehicle decontamination equipment. These preparations guarantee rapid deployment and timely response in case of an emergency [9,10]. By integrating scientific training methods with extensive practical drills, emergency response capabilities can be significantly enhanced. Every team member should be trained to maintain high alertness and composure in the face of sudden incidents, ensuring that all protective measures are seamlessly integrated and precisely executed.

4. Countermeasures for the Disruption of Control and Stability Maintenance Operations by CBRN Drones

4.1 Strengthening Intelligence Collection and Analysis Capabilities

When addressing the threat of CBRN drones, the accuracy and timeliness of intelligence are critical. It is necessary to enhance the collection of intelligence related to drones, particularly through in-depth analysis of potential hostile forces' activities. By obtaining information from multiple sources and integrating satellite reconnaissance, ground surveillance, and cyber intelligence, a comprehensive intelligence network can be established to detect potential threats before drone harassment occurs. Intelligence collection should not only focus on adversary actions but also emphasize the analysis of key drone technical parameters and flight trajectories. By leveraging big data and

artificial intelligence technologies, early warning and forecasting can be enhanced, improving the precision and efficiency of defensive responses.

4.2 Improving Coordinated Operations Mechanisms

In control and stability maintenance operations, a rapid response and effective coordination are essential once drone harassment occurs. To enhance response efficiency, it is necessary to strengthen collaboration mechanisms among different departments. Public security, national security, military, and intelligence agencies should establish a unified command and dispatch system and use an information-sharing platform to ensure that all departments can update the latest intelligence on drone harassment in real-time and develop a consistent response plan. Special emphasis should be placed on strengthening communication with local governments and the public, raising awareness across all sectors of society to facilitate the efficient flow of intelligence and countermeasure resources, thereby forming a coordinated and comprehensive societal defense system.

4.3 Enhancing Drone Interception and Destruction Technology Development

As drone technology continues to evolve, traditional defense methods face increasing challenges. The interception and destruction of CBRN drones require high-precision technological solutions. Research and development should focus on new drone countermeasure equipment, such as microwave weapons, laser weapons, and high-precision electromagnetic interference devices, to improve the capability to intercept and neutralize drones. At the same time, a multi-layered defense structure for drone countermeasure systems should be developed. This could include coordinated operations of drone swarms and multiple interception points forming a three-dimensional strike capability against incoming drones, thereby increasing the difficulty and cost of drone-based disruption activities.

4.4 Strengthening Emergency Response and Post-Disruption Recovery Capabilities

After a drone harassment incident, a swift emergency response is crucial to minimizing damage. Emergency response procedures should be optimized to ensure that rescue forces can be rapidly organized to handle the aftermath of a drone attack. This includes medical treatment for casualties, site cleanup, and the elimination of security threats. Post-disruption recovery capabilities should also not be overlooked, necessitating the restoration and reconstruction of critical infrastructure to ensure that control and stability maintenance operations can resume as soon as possible. A post-disruption information recovery mechanism should be established to promptly update the security status of affected areas and provide the public with necessary psychological support and security assurances, ensuring societal stability.

By reinforcing intelligence reconnaissance, coordinated operations, countermeasure technology development, and emergency response mechanisms, a comprehensive and effective defense system can be established to counter the increasingly complex threats posed by CBRN drone attacks. This will ensure that control and stability maintenance operations can proceed smoothly under various threats.

5. Conclusion

This paper conducts an in-depth analysis of the characteristics and potential hazards of CBRN drones in disrupting control and stability maintenance operations and proposes corresponding countermeasures, which hold significant practical value. However, as technology continues to advance, existing counter-strategies may face challenges from new technological breakthroughs. Additionally, emergency response capabilities in complex environments, particularly in terms of information sharing and interdepartmental collaboration, still require further enhancement. Future research should focus on innovations in counter-drone technologies, especially in the application of artificial intelligence, big data, and 5G communications. Moreover, optimizing interdepartmental coordination mechanisms and institutionalizing real-world drills are essential for improving overall defense capabilities and ensuring long-term social stability. By continuously advancing technological measures and emergency response mechanisms, national stability maintenance capabilities in complex security environments can be effectively strengthened,

providing a robust safeguard for sustained social stability.

References

[1] Nichols, Randall K.; Sincavage, Suzanne; Mumm, Hans; Lonstein, Wayne; Carter, Candice; Hood, John Paul; Mai, Randall; Jackson, Mark; Monnik, Mike; McCreight, Robert; Slofer, William; and Harding, Troy, DRONE DELIVERY OF CBNRECy – DEW WEAPONS Emerging Threats of Mini-Weapons of Mass Destruction and Disruption (WMDD) (2022). NPP eBooks. 46. https://newprairiepress.org/ebooks/46

[2] Junyan Shi, Dianning Hou. Research on the Coordination of Micro Unmanned Aerial Vehicles and Ground Unmanned Systems in Urban Counter-Terrorism Operations. Naval Electronic Engineering, 2022, 42(9): 36-40. DOI: 10.3969/j.issn.1672-9730.2022.09.008.

[3] Qiangkai Zeng, Zhixian Liang, Jinjuan Zhou. A Brief Analysis of the Application of Drones in Armed Police Forces. Science and Education Guide: Electronic Edition, 2018(4): 1. DOI: 10.3969/j.issn.1674-6813(s).2018.02.197.

[4] Wei Zhang. AI and New Sensors Empowering Drone Warfare. Tank & Armored Vehicles 12 (2024).

[5] Tong Wu, Weipeng Xie, Tongshuai Qi. Analysis of Tactics and Strategies for Counter-Drone Swarm Operations. Journal of China Academy of Electronics and Information Technology, 2024, 19(4): 375-379.

[6] Xunhu Dong, Na Ou, Hao Zhou, et al. Progressive Training of Foreign CBRN Defense Units. Chinese Journal of Hygiene Rescue, 2021, 7(1): 39-41.

[7] Letian Zhao, Yun Gao. Analysis and Insights on the U.S. Military Chemical, Biological, Radiological, and Nuclear Defense Plan. Journal of Chemical Defense Research, 2008(4): 3.

[8] Zengli Zhang, Manlin Wang. The Latest Advances in Global CBRN Protection Equipment Technology. ConMilitary, 2014, 0 (7): 50-53.

[9] Zhihua Zhu, Haitao Bai. Development Status of Portable and Multifunctional Systems in the Field of CBRN Protection (Part 1). Foreign CBRN Defense Technology Trends, 2012 (2): 6.

[10] Yanan Zhang, Jun Xu, Ruiping Zheng, et al. Research Progress on CBRN Protective Clothing. Cotton Textile Technology, 2022, 50(2): 5. DOI: 10.3969/j.issn. 1001-7415.2022.02.003.

