PERSPECTIVE

How to prevent malicious use of intelligent unmanned swarms?

Qi Wang,[1,2,*] Tingting Li,[1] Yongjun Xu,[1,2] Fei Wang,[1,2] Boyu Diao,[1,2] Lei Zheng,[3] and Jincai Huang[4]

[1]Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100190, China

[2]University of Chinese Academy of Sciences, Beijing 100049, China

[3]61212, Beijing 100000, China

[4]College of Systems Engineering, National University of Defense Technology, Changsha 410073, China

*Correspondence: wangqi08@ict.ac.cn

Received: December 13, 2022; Accepted: February 14, 2023; Published Online: February 16, 2023; https://doi.org/10.1016/j.xinn.2023.100396

Citation: Wang Q., Li T., Xu Y., et al., (2023). How to prevent malicious use of intelligent unmanned swarms? The Innovation **4(2)**, 100396.

With advancements in swarm intelligence, artificial intelligence, and wireless mobile network technology, unmanned swarms such as unmanned aerial vehicles, ground vehicles, ships, and other unmanned systems are becoming increasingly autonomous and intelligent. Benefiting from these technologies, intelligent unmanned swarms are able to efficiently perform complex tasks through collaboration in various fields. However, malicious use of intelligent unmanned swarms raises concerns about the potential for significant damage to national infrastructures such as airports and power facilities. Defending against malicious activities is essential but challenging due to the swarms' abilities to perceive, understand complex environments, and make accurate decisions through multi-system collaboration. This perspective sheds light on recent research in counter-measures and provides new trends and insights on how to prevent malicious actions by intelligent unmanned swarms.

The unmanned swarms are comprised of various unmanned systems, such as unmanned aerial vehicles, unmanned ground vehicles, and unmanned ships. These swarms are becoming more autonomous and intelligent due to advancements in swarm intelligence, artificial intelligence,[1] and wireless mobile network technology. This allows intelligent unmanned swarms to have the capabilities of environment perception and awareness, task allocation, decision-making, and autonomous control through machine learning and collaboration among multiple agents. Specifically, unmanned systems equipped with electro-optical and thermal, as well as acoustic, radar can achieve comprehensive environmental awareness, recognition, and an overall understanding of the environment. Based on the large amount of data generated through interactions of unmanned systems, efficient task allocation and trajectory planning decisions are made to collaboratively complete complex tasks in various applications.

Intelligent unmanned swarms have a wide range of uses, from leisure activities like light shows to practical applications like disaster response, emergency services, industry, and agriculture. However, they can also pose a threat to critical infrastructures such as airports, power facilities, and schools. To mitigate these risks, counter-measure methods need to be implemented. However, due to the high degree of resilience and self-organization in intelligent unmanned swarms,[2] preventing malicious activities remains a major challenge.

There are several traditional counter-measures for defending against malicious unmanned swarms, including physical counter-measures[3] and cyber counter-measures,[4] as shown in Figure 1. Physical counter-measures involve directly destroying individual members of the swarm through collision, shooting, or capture. Cyber counter-measures focus on intercepting and disruption the communication wireless networks between members of the swarm. Cognitive counter-measures are novel methods by camouflage, deception, and adversarial behaviors that aim to break down the ability and act of nullifying, and these are promising methods for defending against malicious intelligent

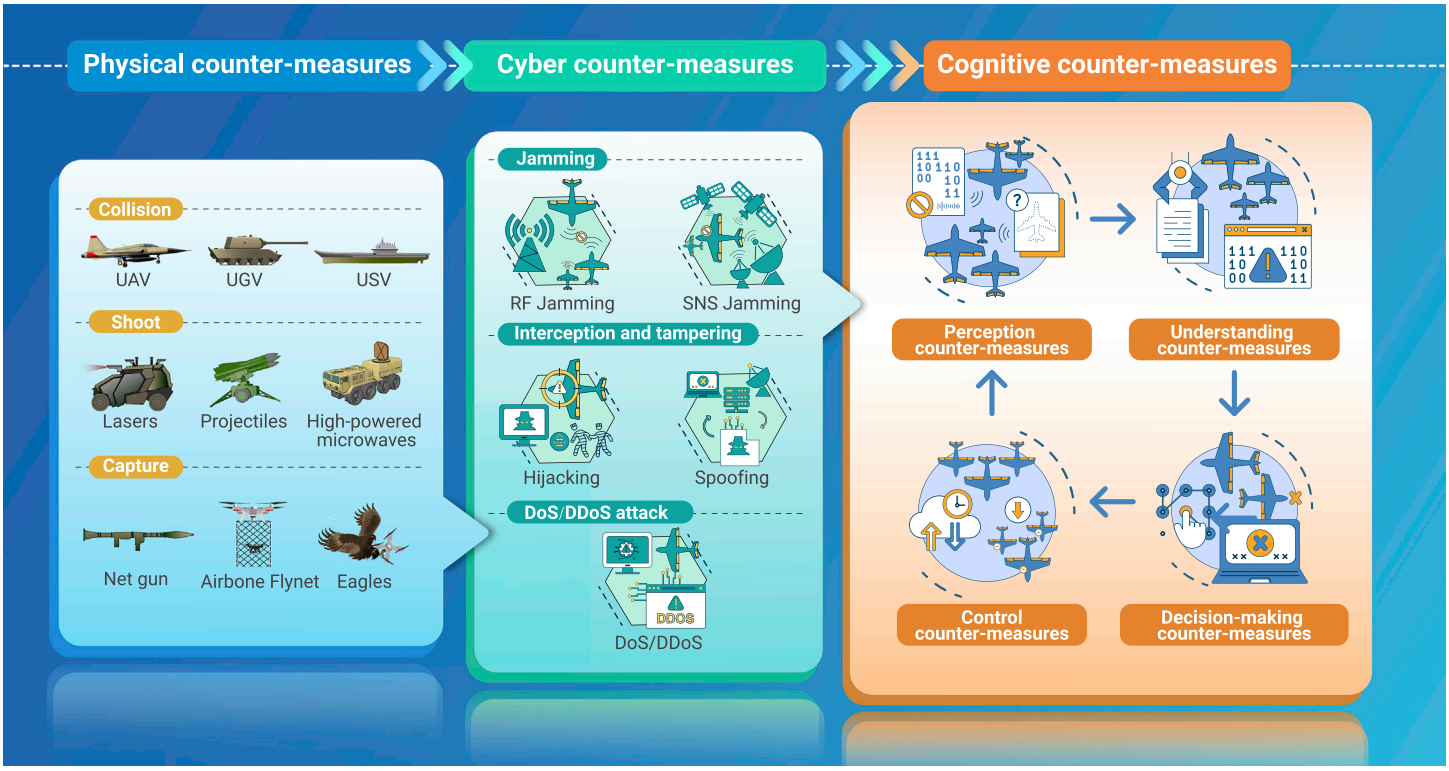

Figure 1. Counter-measures for defending against malicious unmanned swarms

unmanned swarms. These three counter-measure methods operate in different domains and have different levels of effectiveness to prevent malicious activity by unmanned swarms.

PHYSICAL COUNTER-MEASURES

Physical counter-measures involve colliding with one or several moving adversary targets; shooting with projectiles, lasers, or high-powered microwaves, or capturing with nets and eagles. For example, projectiles and lasers are used to completely or partially destroy unmanned systems using ammunition and energy, respectively, while high-powered microwaves are used to disable the electronic systems. To defend against drones, an anti-drone system[5] that employs multiple passive surveillance technologies has been proposed, allowing for detection, localization, and jamming. However, these physical counter-measures, which aim to destroy individual members or part of swarms, are less effective in defending against malicious intelligent unmanned swarms. Since intelligent unmanned swarms are highly autonomous and distributed, they can perceive and understand their surroundings and make optimal decisions through collaboration and autonomous movement. Thus, even if some members of the intelligent unmanned swarms are destroyed, the remaining systems can quickly reorganize and continue with their tasks.

CYBER COUNTER-MEASURES

Cyber counter-measures for unmanned swarms consist of disrupting communication, such as jamming, denial of service (DoS)/distributed DoS (DDoS) attacks, and interception and tampering with the swarm's information. These methods aim to interfere in cyberspace and disrupt the communication between the swarms and the controller. One common approach is radio frequency (RF) jamming, which is used to disrupt the RF link between the swarm and its controller. Another approach is jamming the satellite navigation system (SNS), such as GPS, GLONASS, and BeiDou, to interfere with the swarm's navigation capabilities. However, RF jamming and SNS jamming may not be effective against intelligent unmanned swarms, which have the ability to fly autonomously and coordinate without relying on external controls or satellite systems. In recent years, there have been designs for intelligent unmanned swarms that are capable of navigation independently with full autonomy and coordination without external facilities in challenging environments, such as dense bamboo forests.[6] Additionally, jamming can cause serious problems because it interferes with other systems operating on the same communication frequency.

DoS/DDoS attacks occur when an excessive amount of service requests are sent to a network, leading to network congestion and hindering the delivery of services or control commands from the ground controller to the swarms. Despite the existence of security techniques to defend against these types of attacks, they may not be successful against intelligent unmanned swarms.

Cyber counter-measures that involve intercepting the information of swarms can be accomplished by obtaining information such as positions and control instructions. However, attempts to hijack or spoof by injecting manipulated information may be prevented by various security techniques, including digital signatures, strong authentication, and message encryption. While these counter-measures may not be fully effective against intelligent unmanned swarms, it should be noted that the interception and tampering of information is illegal in some countries. As a result, cyber counter-measures for defending against intelligent unmanned swarms may not achieve satisfactory effectiveness.

COGNITIVE COUNTER-MEASURES

The intelligent unmanned swarms equipped with cameras, various sensors for detection and localization-and-tracking actions, and wireless networks are capable of perceiving, cognizing, and understanding of the complex environment, autonomous decision-making and coordinated control. The counter-measures, breaking down these abilities and nullifying collaboration behaviors of swarms in cognitive[7] space, are a potential further research direction. Cognitive counter-measures are designed to disrupt the following capabilities of these swarms: perception through deception of the senses, understanding through confusion of intention, decision-making through adversarial policies, and control through interference from adversaries or increased transmission delay. These methods aim to neutralize the collaboration and coordination of the swarms in the cognitive domain.

Intelligent unmanned swarms rely on their perception ability, which includes the use of imaging systems, laser detection, and ranging-based systems, to detect and identify targets and their surroundings. Despite recent advancements[8] in detection and classification algorithms using machine learning, these systems can still be vulnerable to adversarial examples that cause misdetection and misclassification. However, as the detection and classification schemes are combined from multiple sensors and fuse data collaboratively from multiple unmanned systems to improve the accuracy of detection and classification, it remains a significant challenge to construct effective adversarial examples that can successfully impair the perception ability of intelligent unmanned swarms.

The cognitive and understanding ability is to analyze and judge the behavioral intentions of the swarms based on perceived information, which is essential to make decisions. Since intentions are mainly judged through behaviors, adversarial intention recognition and disguise algorithms can be used to mislead the analysis of intentions[9] to combat malicious activity from intelligent unmanned swarms. However, accurately estimating the probability of the opponent's behavior is a major challenge in intention recognition and disguise, as the opponent's behavior is only partially observable, and imperfect information about the game state can negatively impact these processes.

The decision-making ability is to allocate the tasks, plan the trajectory, and take action for each unmanned system by traditional rule-based decision algorithms or by state-of-the-art reinforcement learning (RL)-based decision algorithms. While rule-based decision algorithms are difficult to apply to dynamic and intelligent unmanned swarms, RL-based decision algorithms have proven effective in dynamic autonomous swarms. However, RL algorithms can be manipulated through adversarial policies[10] that alter observations and lead to abnormal behavior, while previous studies have explored adversarial policies in one-on-one games, such as zero-sum robotics games, aiming to fail one well-trained agent by training adversarial policies using RL against black-box opponents. These simple adversarial policies are limited in their ability to address the complex multi-agent competition and cooperation that is required when countering intelligent unmanned swarms. Recent advancements in multi-agent RL (MARL) hold promise for addressing these challenges, but designing effective adversarial policies remains a significant research focus, as it involves estimating team rewards and dealing with the exponential growth of action space as the number of agents increases.

The control ability of intelligent unmanned swarms involves ensuring consensus among the systems, such as formation control and coordinated control. However, the consensus process can be interfered with by adversaries that eavesdrop on the initial information of unmanned systems in a swarm, modify the values in the communication links, or increase the transmission delay, which deteriorates the consensus control of multi-unmanned systems. Thus, interfering with the control ability is a way to prevent the completion of malicious activities by these swarms.

CONCLUSION

The malicious use of intelligent unmanned swarms poses a threat to critical national infrastructures. While traditional physical and cyber counter-measures may be effective against traditional threats from swarms, they are limited when it comes to intelligent unmanned swarms with advanced capabilities such as perception, understanding of complex environments, autonomous decision-making, and coordination. We shed light on the new research trends of cognitive counter-measures, but they still have some challenges to overcome, especially with respect to technology and practical use. Research in this area should focus on understanding the formation mechanisms and inherent vulnerabilities of intelligent unmanned swarms and developing effective counter-measures. Furthermore, it is worthwhile to investigate evaluation frameworks to evaluate the effectiveness of these counter-measures and implement a practical counter-intelligent unmanned swarming system to defend against intelligent unmanned swarms.

REFERENCES

1. Xu, Y., Liu, X., Cao, X., et al. (2021). Artificial intelligence: a powerful paradigm for scientific research. Innovation **2**, 100179.
2. Michel, A.H. (2019). Counter-drone systems. https://dronecenter.bard.edu/files/2019/12/CSD-CUAS-2nd-Edition-Web.pdf.

3. Swinney, C.J., and Woods, J.C. (2022). A review of security incidents and defence techniques relating to the malicious use of small unmanned aerial systems. IEEE Aerosp. Electron. Syst. Mag. ***37***, 14–28.
4. Valianti, P., Papaioannou, S., Kolios, P., et al. (2022). Multi-agent coordinated close-in jamming for disabling a rogue drone. IEEE Trans. Mob. Comput. ***21***, 3700–3717.
5. Shi, X., Yang, C., Xie, W., et al. (2018). Anti-drone system with multiple surveillance technologies: architecture, implementation, and challenges. IEEE Commun. Mag. ***56***, 68–74.
6. Zhou, X., Wen, X., Wang, Z., et al. (2022). Swarm of micro flying robots in the wild. Sci. Robot. ***7***, eabm5954.
7. Hartley, D.S., III, and Jobson, K.O. (2020). Cognitive Superiority: Information to Power (Springer Nature).
8. Huang, S., Papernot, N., Goodfellow, I., et al. (2017). Adversarial attacks on neural network policies. Preprint at arXiv.
9. Strouse, D.J., Kleiman-Weiner, M., Tenenbaum, J., et al. (2018). In Learning to share and hide intentions using information regularization. Advances in Neural Information Processing Systems (MIT Press), p. 31.
10. Gleave, A., Dennis, M., Wild, C., et al. (2020). Adversarial policies: attacking deep reinforcement learning. In International Conference on Learning Representations (ICLR) (Elsevier).

ACKNOWLEDGMENTS

This work was supported by the Youth Innovation Promotion Association CAS.

DECLARATION OF INTERESTS

The authors declare no competing interests.