Human Factors in Design, Engineering, and Computing, Vol. 238, 2026, 1872–1876
https://doi.org/10.54941/ahfe1008415

The Impact of Human Factors on Counter-Drone Systems

Chaumette Serge

Université de Bordeaux, CNRS, Bordeaux INP, LaBRI, UMR 5800, F-33400 Talence, France

ABSTRACT

Drones—particularly small and medium-sized systems—have become a major asset on the battlefield. Whether deployed individually or in swarms, coordinated or not, they have demonstrated significant impact in conflicts such as those in Ukraine and in regions like the Strait of Hormuz. The scale of damage they can inflict has become a growing concern. While systems have long existed to automatically detect and counter large drones, they are significantly less effective against small and medium-sized ones. Thus, due to late and limited detection, the human operator who makes the final decision on whether or not to engage a countermeasure has become central. In this paper, we explain why this is the case, highlighting its role and the mental load that is placed on him/her.

Keywords: Drones, Counter drone systems, Operator, Operator Mental load, Swarms

INTRODUCTION

In recent years, drones have been used to carry out large-scale attacks against both military forces and civilians. Their impact can be devastating. To cite just one example, a drone strike on a hospital in Sudan in March 2026 killed 70 people. The United Nations reported that at least 306 people were killed in Sudan in October (United Nations, 2026).

Civilian sites targeted include hospitals, schools, markets, and other critical civilian infrastructure. Although no large public gatherings have been "successfully" targeted so far, numerous potential mass-casualty events have been averted thanks to intelligence services. However, this must not create a false sense of security. **The threat remains real, and robust security measures are essential to protect civilian populations and prevent mass-casualty attacks.**

However, counter-drone technologies continue to lag behind advances in drone technology. An additional dimension must also be considered: the human factor. This paper examines these challenges from an operational perspective, highlighting the central role of the command-and-control (C2) operator.

FIRST CHALLENGE: DETECTING DRONES

The first challenge is detecting these systems. They are smaller than the targets typically detected by military radars and can be made largely of materials such as plastic or even cardboard (see for example (Air Kamuy,

Received November 1, 2026; Revised November 14, 2026; Accepted November 17, 2026; Available online December 1, 2026

© 2026 The Authors. This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License.
For more information, see https://creativecommons.org/licenses/by-nc-nd/4.0/

s.d.)) resulting in radar signatures that are too weak for reliable detection. Their speed, which can reach several hundred kilometers per hour in the case of racing drones, further complicates detection.

Swarms (Chaumette, 2016) introduce an additional level of complexity. By saturating detection systems (see Figure 1), an adversary can generate a high volume of alerts, making it difficult for human operators to distinguish genuine threats from false positives. Coordinated or "smart" swarms may also use approach maneuvers designed to conceal individual drones or their overall strategy until the last moment, for example, by adopting specific flight formations that mask their number or even their presence.



Figure 1: A swarm of 1,000 drones achieving saturation (Courtesy Icarus Swarms).

Here are a number of reasons for detection difficulties:

- Physical characteristics of the system
  - Drones made from cardboard or other lightweight materials
  - Stealth drones, *e.g.* the nEUROn developed by Dassault Aviation

- Autonomy
  - Absence of radio link to a command-and-control (C2) system
  - Absence of air-to-ground communications for data transmission or other purposes

- Speed and flight profile
  - Racing drones (see Figure 2) can reach speeds of several hundred kilometers per hour
  - Rotary-wing drones can remain stationary in the air, potentially hiding, making them harder to detect

- Swarms
  - Saturation effects (Hu, Ru, Lu, & Wang, 2023) can be achieved relatively easily
  - Coordinated tactics can be used to mislead detection systems (Do, et al., 2021)

- Size
  - Military drones can be as small as 0.25 meters (Military Hub, 2026)



Figure 2: Ukrainian military FPV drone by АрміяІнформ, via Wikimedia Commons. Licence CC BY 4.0. Cropped original image.

SECOND CHALLENGE: ONCE DETECTED, THESE SYSTEMS REMAIN DIFFICULT TO NEUTRALIZE

The second challenge is that, once detected, these systems remain difficult to neutralize. This is largely due to the same factors that make them difficult to detect in the first place. Moreover, when dealing with swarms, the potentially large number of drones can overwhelm both defense systems and the operator—the human in the loop—who must ultimately decide which targets to prioritize.

Several approaches have been developed to neutralize these systems, either destructive or non-destructive.

Two major non-destructive strategies exist:

- **Taking control:** This approach relies on detecting the radio link between the drone and its operator or an associated C2. It generally requires good knowledge of the brand of drone being targeted. It also assumes that a connection exists, making it ineffective against autonomous (Nextech) systems that have no radio link to the ground. Control can also be taken through GNSS spoofing. This is more difficult to achieve and does not apply to systems that do not rely on GNSS for navigation, such as those using cameras or points of interest (POIs).
- **Capture:** For example, eagles have been trained by various police forces and armies. Net-based systems also exist. This approach is only applicable to small, slow-moving systems.
- **Context of operation disruption:** It is also possible to place drones in a context of operation in which they cannot operate, for example through GNSS or radio jamming. The goal of these approaches is not to take control of the drones, but to force them to land or return to their home position (the position from which they took off).

Although these approaches are non-destructive in principle, they still involve risks. Assume a drone carries a NBC (Nuclear, Biological, Chemical) payload. It may detect that it has been captured and release its payload, potentially causing catastrophic consequences (see section *When to Engage* bellow).

Destructive methods have also been developed, using technologies such as lasers or microwaves. Here again, if a drone is destroyed, it will fall to the ground, potentially triggering a NBC payload.

Because of these potential consequences, all these approaches raise the question of when to engage.

THIRD CHALLEGE: WHEN TO ENGAGE

The third challenge relates to the military doctrine, particularly the question of "when to engage." Consider, for example, a drone detected over a large stadium during events such as the Olympic Games or the Football World Cup. Neutralizing the drone could have significant collateral consequences: depending on its payload, intercepting it might cause more harm than allowing it to continue its operation. This becomes a matter of carefully weighing risks against potential benefits. Once again, this places a substantial burden on the operator, as the system cannot act with full autonomy given the complexity and implications of the decision.

MAN IN THE LOOP

During all the process (see Figure 3), a human remains in the loop to make the final decision. This introduces delays and raises concerns about potential collateral effects that the operator may consider attributable to him/her. Thus, even once the technical issues are resolved, the operator's mental and emotional load (Matin Ghasempour, Tazim, Shuchisnigdha, & Mahmudur, 2025) remains the cornerstone of the entire process. He/she has little time to make a decision that potentially has a big impact.

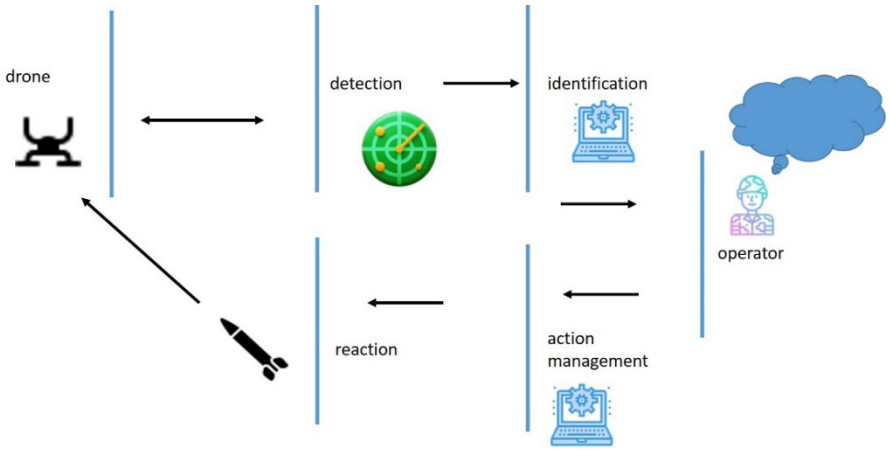


Figure 3: The counter drone chain and process.

CONCLUSION

Drones and drone swarms are used asymmetrically in both civilian and military theatres of operation. No approach can guarantee a 100% interception success rate. From a technological perspective, numerous solutions are available. However, as discussed in this paper, their effectiveness is limited by several factors that we do not yet know how to address.

Furthermore, the need to keep a human in the loop, mainly to avoid potential collateral effects, entails significant risks due to the heavy burden placed on the operator, who must make decisions under pressure, often weighing the risks and benefits of each decision. Additionally, he/she has little time to make these decisions.

By highlighting the issues that we have described in his paper, we aim to emphasize the fact that the operator is the keystone of the system. We believe that 100% protection against drone attacks cannot be achieved as long as a human remains in the loop. Among the potential approaches that could be a first step to address this issue is the use of explainable artificial intelligence to provide the operator with a range of "validated" strategies for countering a hostile drone or swarm of drones. This would most likely relieve him/her of a significant part of his/her mental burden.

REFERENCES

Air Kamuy. (s.d.). *AIr Kamuy 150*. Retrieved from Air Kamuy: https://en.airkamuy.com/

Chaumette, S. (2016). Chapter 8: Cooperating UAVs and Swarming. Dans J. H. Kamesh Namuduri, *UAV Networks and Communications*. Cambridge Press.

Do, H., Hua, H., Nguyen, M., Nguyen, V.-C., Nguyen, H., & Nguyen, N. (2021). Formation Control Algorithms for Multiple-UAVs: A Comprehensive Survey. *EAI Endorsed Transactions on Industrial Networks and Intelligent Systems*.

Hu, S., Ru, L., Lu, B., & Wang, W. (2023). Efficiency analysis of intercepting UAV swarm by various air defense methods. *Journal of Physics Conference Series*.

Matin Ghasempour, A., Tazim, A., Shuchisnigdha, D., & Mahmudur, R. (2025). Cognitive Workload in Drone Operations: A Literature Review and Conceptual Framework. *IISE Annual Conference* (pp. 1–6). Institute of Industrial and Systems Engineers (IISE).

Military Hub. (2026, June 29). *How Big Are Military Drones? A Size Guide by Drone Type*. Retrieved from Military Hub: https://www.military-hub.com/how-big-are-military-drones-a-size-guide-by-drone-type/

Nextech. (s.d.). *8 Levels of Drone Autonomy.* Récupéré sur nextech.online: https://nextech.online/drone-autonomy/

United Nations. (2026, October 23). *Sudan: Drone strikes killed at least 306 people in three weeks*. Retrieved from United Nations web site: https://news.un.org/en/story/2026/10/1168661