DOI: 10.53477/3045-2309-25-18

DRONES – A THREAT TO SECURITY?

Ana-Raluca STAN, PhD,

Centre for Defence and Security Strategic Studies, "Carol I" National Defence University, Bucharest, Romania. E-mail: stanraluca12@gmail.com

Abstract: Drones present both opportunities and challenges, offering significant benefits in various sectors (military, law enforcement and public safety, surveillance, media, agriculture, delivery and logistics services, etc.), and also posing threats that need to be addressed. Harnessing their benefits while minimising their potential threats can present an international security issue. It is important to focus our attention on the potential security risks they pose and implement regulations and countermeasures to mitigate these threats. Their overall impact on international security will depend on how they are managed, regulated, and controlled in the coming years.

This paper addresses the contentious issue of employing drones and examine their potential negative effects on international security using a qualitative research method, mainly focusing on UAVs.

Keywords: drones impact on security; drones as weapons; current security challenges; technology development; modern warfare; military innovation; SWOT analysis on drones.

1. Overview of Drone Technology

Unmanned aerial vehicle (UAVs), "also known as drones, are aircraft that operate without a human pilot onboard, vary in size and weight and, due to their cost effectiveness and efficiency, are being deployed across industry for a myriad of purposes. They can be controlled by a human or operate autonomously, using pre-programming and automation" (Cooperative Research Centres, 2024). "As UAV technology continues to evolve, they are becoming increasingly sophisticated, fitted with state-of-the-art sensors, cameras, and image processing software to provide more efficient and accurate data" (Cooperative Research Centres, 2024).

These devices could be misused in ways that threaten human security and may serve as tools for illegal activities or weapons that could impact global security.

There are several types of unmanned systems categorized based on the domain they operate in:

- *UAVs (Air)*, already mentioned, are autonomous aerial systems used for surveillance, delivery, agriculture, and military applications. Regarding a possible confusion between the term UAV and UAS (unmanned Aircraft Systems), in essence UAV is the vehicle while UAS refers to the complete system required to operate a UAV;
- *UGVs* (*Unmanned Ground Vehicles*), vehicles designed for ground-based operations, including military robotics, disaster response, and agricultural automation;
- USVs (Unmanned Surface Vehicles), autonomous or remotely controlled vessels that operate on water surfaces, often used for surveying, monitoring, and naval operations;
- *UUVs* (*Unmanned Underwater Vehicles*), subdivided into: AUVs (Autonomous Underwater Vehicles), operate independently for exploration, mapping, and data collection; ROVs (Remotely Operated Vehicles), tethered and controlled by operators for underwater tasks such as repairs and inspections;
- Unmanned Space Systems, include satellites and robotic space exploration vehicles like rovers.

The impact of drones has its origins in military innovation, technological advancement, and the development of civilian applications. The concept of drones can be traced back to 1849, even before the advent of modern aviation. During the Austro-Italian War of 1866, Austria deployed unmanned balloons filled with explosives against Venice, marking one of the earliest recorded uses of remotely delivered weaponry. This early usage inspired further exploration of automated aerial systems.

Nikola Tesla contributed foundational ideas that influenced the development of remote-controlled devices, including UAVs. In 1898 he demonstrated a remote-controlled boat during an electrical exhibition at Madison Square Garden in New York, called "teleautomaton" (Photo no. 1: 1898 – Telautomaton – Nikola Tesla). By introducing the wireless control and envisioned their usage in warfare and other applications laid the groundwork for later innovations in remotely piloted vehicles. His work remains an inspiration for the broader field of robotics and remote-controlled systems.

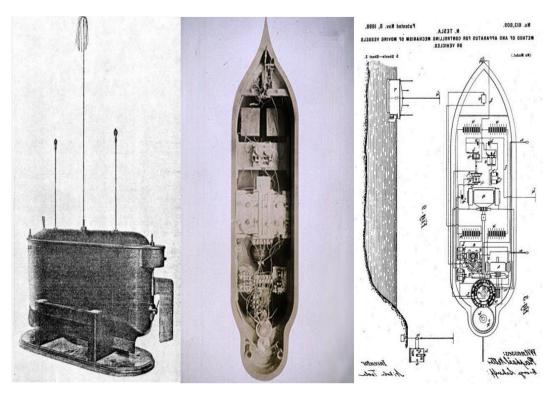


Figure no. 1: 1898 – Telautomaton – Nikola Tesla (Cyberneticzoo, 2010)

Thereafter, in 1916, during World War I, British engineer Archibald Montgomery Low¹, working under the Royal Flying Corps (RFC), created one of the first powered drone aircraft which was a prototype of a pilotless aircraft that utilised radio signals for control-*the Aerial Target*. Although it was never deployed in combat, its development marked the beginning of the journey toward modern drones.

 $^{^{1}}$ Archibald Montgomery Low (17 October 1888 – 13 September 1956) developed the first powered drone aircraft. He was an English consulting engineer, research physicist and inventor, and author of more than 40 books. He has been called "the father of radio guidance systems" due to his pioneering work on planes, torpedoes boats and guided rockets.



Figure no. 2: Aerial target –RFC in the First World War (Imperial War Museums n.d.)

The pressures of World War II (1939-1945) significantly accelerated the development of drones. The Germans introduced the *V-1 flying bomb (also known as a "buzz bomb" or "doodlebug")*, a cruise missile capable of traveling hundreds of kilometres, making it one of the first widely used unmanned aerial systems in warfare. Meanwhile, the United States (US) developed drones such as *the Radioplane OQ-2*, manufactured by the Radioplane Company, which was primarily used for target practice to train gunners. This was followed by the updated version, the *OQ-3*, which became the most widely used target drone in US service (Newcome, 2004).

During the Cold War (1947-1991), drones evolved from basic technology into essential tools for surveillance and intelligence gathering. The US military's *Ryan Firebee* (*Ryan Model 124/BQM-34A Firebee*), introduced in the 1950s, was one of the earliest jet-propelled unmanned aerial vehicles capable of collecting reconnaissance data. As tensions between global powers increased, drones became essential for conducting high-risk intelligence missions, particularly over enemy territory.

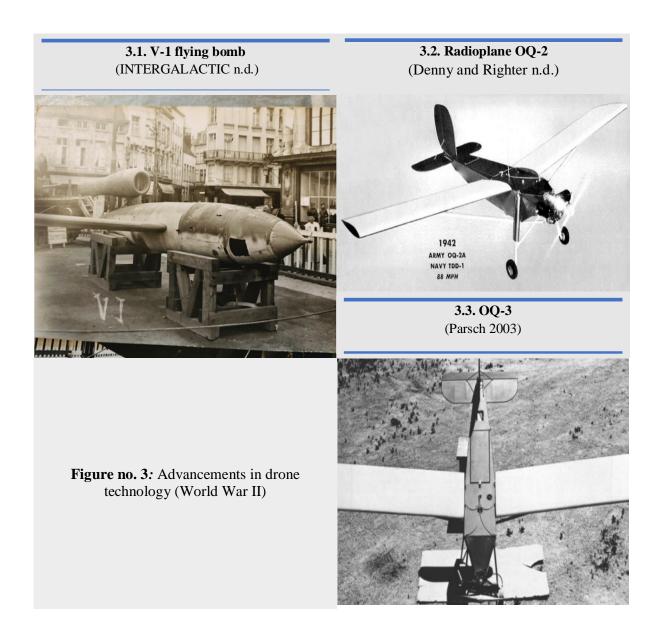
The advancements in drone technology during the 1960s and 1970s highlighted their significance in reducing risks faced by pilots, especially during the Vietnam War. *The Ryan Model 147 "Lightning Bug" (AQM-34)*, derived from the Firebee, conducted hundreds of surveillance missions over Vietnam and the surrounding regions, demonstrating the significant value of drones in providing real-time battlefield intelligence.

The emergence of modern drones became prominent during the period from the 1980s to the 2000s. The 1980s marked a turning point with the introduction of more autonomous and versatile drones. The *IAI Scout*, developed by Israel, was first used in combat missions by the South African Defence Force against Angola during Operation Protea². IAI Scout was among the first UAVs to integrate video transmission for real-time surveillance, influencing US designs.

bases at Xangongo and Ongiva.

_

² Operation Protea was a military operation during the South African Border War and Angolan Civil War in which South African Defence Forces (SADF) destroyed several South West Africa People's Organisation (SWAPO) bases in Angola. During the operation, which took place from 23 August to 4 September 1981, up to 5,000 SADF soldiers occupied Cunene province, Angola. Its objectives were to destroy the SWAPO command and training centre at Xangongo and its logistic



During this period, drones designed for precision strikes were developed, with the *MQ-1 Predator* project emerging in the 1990s. The Predator³ was extensively deployed in the Gulf War and subsequent conflicts. Equipped with cameras, sensors, and weapon systems, it played a significant role in redefining modern combat (Kaplan, 2018).

³ Development of the Predator actually began in the 1980s. The decade that brought us big hair parachute pants, and Punky Brewster also brought us improved unmanned aerial technology. Aerospace engineer and Israeli immigrant Abraham E. Karem built the first Predator prototype, the "Albatross", in his garage. In 1996, the Department of Defense chose the US Air Force to operate the Predator, and the drone entered combat over the skies of Bosnia. By the late 1990s, the Predator was equipped with a live satellite video link and a laser designator to illuminate targets and guide weapons dropped from other aircraft.

The early 2000s presented the MQ-9 Reaper, an upgrade Predator, combined long flight endurance with advanced strike capabilities, solidifying their role in counter-terrorism operations (led wars in Iraq and Afghanistan)⁴.

Initially, drones were primarily used for military purposes, but in the 2010s, they started to enter civilian markets due to advancements in miniaturization and affordability. They quickly became popular tools for photography, film-making, agriculture, and delivery services. Additionally, drones proved to be vital in disaster response, environmental monitoring, and medical deliveries.



2. Drones – Impact on Security

As presented, mostly in the military domain, drones are a technological asset due to their capacity of "unique tactical advantages and enhanced the operational efficiency in various combat scenarios" (Allen, 2022) "In Ukraine drones have become an important weapon to gain an asymmetric edge over Russian forces. Their availability, rapid development, ease of deployment and use make

⁴ The Predator's exceptional surveillance capabilities were immediately evident, but no real effort to equip it with targeting systems or weapons occurred until 2000. By summer 2001, successful trials with the AGM-114 Hellfire and an onboard targeting system were complete and the Predator had fired missiles against targets in Afghanistan before year-end.

them indispensable in the military operations on Ukrainian soil. While this technology has altered the character of modern warfare, the UAVs have not had a decisive effect on the adversary to date" (Allen, 2022). In the Russia-Ukraine war, as illustrated in Photo no. 5: Drones attacks in the Russia-Ukraine war, drones have played a transformative role marking one of the first large-scale conflicts to heavily integrate unmanned aerial systems (UAS) for both offensive and defensive purposes. Mention some of the type of UAVs used:

- Shahed-136 (Iranian drone), the "kamikaze" drone used by Russia for long-range attacks;
- Bayraktar TB2 (Turkish drone), a game-changer used by Ukraine for ISR and precision strikes, has played a significant role in targeting Russian artillery and supply lines;
- Orlan-10, a Russian reconnaissance drone providing battlefield intelligence and artillery targeting;
- *DJI Mavic Series*, used by both Russia and Ukraine, consumer drones, widely modified for combat, being employed in reconnaissance and grenade drops, facing the risks of detection and targeting when operating them;
- FPV drones⁵, custom-built drones used by Ukraine, equipped with explosives are used for precision attacks on tanks and other targets, often controlled via first-person view cameras;
- *UJ*-22, this Ukrainian designed long-range drone can strike targets up to 800 km away, targeting deep within Russian territory;
- *Kronshtadt Orion*, managed by Russia, comparable to the US Reaper drone, it has been used for air-to-ground missile strikes (AGM)⁶.

Also, the exploitation of drones, properly equipped, could increase criminal activities, smuggling contraband across borders (illegal drugs, tobacco, weapons, etc.), contraband into prisons, espionage, and targeted crimes, being very difficult for the authorities to detect or intercept their operations. Their accessibility, low cost, and ability to bypass traditional security measures is the reason why drones have increasingly become tools for criminal activities.

Even if we do not know the veracity of the press information, "it is said that drones have been detected in the UK as being used to monitor areas where criminal activity is taking place, serving as a lookout to alert criminals in the event of law enforcement intervention" (Weinstein, 2023). Another example is along the US-Mexico border drones are employed to deliver small quantities of narcotics while avoiding detection. These methods are cost-effective and limit human involvement, reducing the risks to traffickers if the drone is intercepted (Russo, Dulani Woods, Michael J. D. Vermeer, & Brian A. Jack, 2024).

As beneficial inputs, providing both efficiency and cost-effectiveness, drones have the ability to gather data, provide real-time surveillance, and carry out tasks with precision and safety has made them indispensable tools. One of the most significant advancements is the U.S. military's focus on AI-driven drones designed to operate with minimal human intervention, offering increased efficiency and enhanced operational effectiveness in high-risk environments. This development is part of a broader strategy by the Department of Defence (DoD) to modernise defence technologies, particularly in response to growing security challenges in regions like the Indo-Pacific (U.S. military prioritizes AI-powered drones in defense modernization, 2024).

⁵ First Person View Drone (FPV).

⁶ AGM is a missile designed to be launched from military aircraft at targets on land or sea.

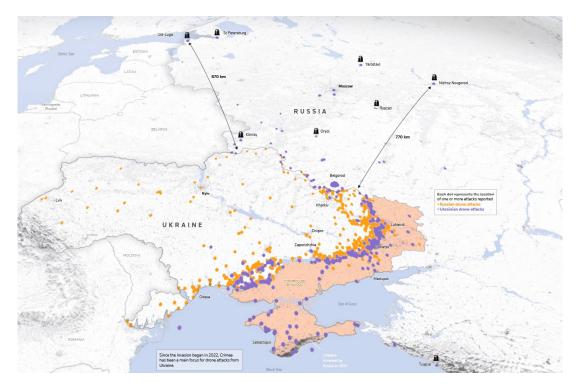


Figure no. 5: Drones attacks in the Russia-Ukraine war (Reuters 2024)

One of the most notable examples of a drone attack that posed a significant security threat occurred on September 14, 2019, when drones were used to attack two major oil facilities in Saudi Arabia. The attack exacerbated tensions in the Middle East, particularly between Saudi Arabia and Iran, and highlighted the risks posed by drones in regional conflicts. This incident provides a clear illustration of how drones can be weaponized to carry out large-scale attacks with substantial consequences.

Drones have become an increasingly important tool in global security operations, with both positive and negative implications for international security. Therefore, the SWOT analysis will present an overall picture of employing drones and their potential impact on security. Why SWOT? Because, from my point of view, the SWOT framework is a well-established method for analysing any system or technology, which makes the analysis easy to follow and provides a clear understanding of drones' multifaceted impact.

SWOT analysis on drones	
Strengths	Weaknesses
- used for surveillance and reconnaissance missions, allowing military and intelligence agencies to gather valuable information on potential threats and monitor conflict zones without putting personnel at risk.	- having the capacity to intrude upon personal privacy by clandestinely capturing images, videos, and various forms of confidential data from private properties and individuals without obtaining explicit consent (drones that are equipped with high-resolution cameras and other sensors).
- used in targeted airstrikes to eliminate	- raising important ethical, legal, and strategic
targets that have a significant impact	inquiries that must be carefully considered to
(terrorist leaders), in remote or difficult to	

reach areas; providing a more targeted approach to military engagement. - used in perilous environments, providing surveillance during protests, criminal incidents, or natural disasters, without compromising human lives.	ensure that they are used responsibly and in accordance with international law.
- having the potential to enhance global security by providing valuable intelligence and precision strike capabilities.	- leading to unintended civilian casualties, prompting criticism and the demand for increased transparency and accountability in drone operations.
	- posing a significant challenge for global security efforts being difficult to track and prevent the use of drones by non-state actors.
 more cost effective to purchase, operate, and maintain than traditional manned aircraft. maritime drones are saving operational 	- having limited battery life (most commercial drones) reducing their effectiveness for extended missions.
costs, such as crew and vessel maintenance.	
- adaptable and can be quickly deployed in various situations, from monitoring large events to inspecting infrastructure.	- the overall efficiency of the drone systems can be affected by harsh weather easily disrupting their operations.
	- drones are reliant on wireless communication, rendering them susceptible to potential threats: jamming, hacking, signal loss.
	- the usage of drones can interference with stringent laws and government regulations, especially in urban areas, limiting their deployment.
	- small drones with limited payload capacity have restricted ability to accommodate additional equipment (advanced sensors or heavier cameras, etc.).
	- lacking the capability to engage in direct communication with civilians for acquiring
	intricate intelligence.
Opportunities	<u>Threats</u>
- improvements in battery life, AI, and autonomous flight systems could enhance the capabilities of drones in security, along with the high level of technological advancement drones can be integrated into urban security systems, working alongside IoT and surveillance networks.	- violations of sovereignty, and the potential for misuse or abuse. In October 2024, two suspected drones breached Romanian airspace on consecutive days. These incidents raised concerns about violations of national sovereignty and the potential risks posed by unauthorized aerial vehicles (Donlevy, 2024).
- drones can play a crucial role in disaster management, providing real-time data for search and rescue missions or assessing damage in dangerous areas, boosting disaster response.	- proliferation of drones has made it easier for non-state actors, such as terrorist organisations, to acquire and use drones for malicious purposes, such as surveillance, reconnaissance, and attacks.

- -beyond surveillance, drones can be used in law enforcement for mass control, crime scene documentation, and suspect tracking, enhancing security applications.
- partnering with police forces or military can further expand the use of drones for national security or defence applications, expanding and consolidating inter-institutional cooperation.
- terrorist groups can use drones to deliver explosives or other harmful payloads to specific targets; drones can be modified to carry and release dangerous substances, making them a potential tool for attacks in populated areas.
- their ability to fly at high altitudes and capture detailed imagery makes them a valuable tool for spying; can be used for espionage purposes by gathering intelligence on governmental, military, or corporate activities.
- In January 2025 German authorities are investigating suspected Russian espionage following drone sightings over several military sites including airfields in Bavaria. The drones described as having longer ranges than civilian models, are believed to be conducting surveillance operations (Crossland, 2025).
- drones are increasingly being used to smuggle contraband, such as drugs, weapons, and other illicit items, across borders and into prisons; ability to bypass traditional security measures makes them an effective means for illegal transport.

As an example, Spanish authorities dismantled a criminal network in Algeciras that used drones to traffic hashish from Morocco. These "narcodrones" were manufactured in Ukraine and transported to Spain for use in the Campo de Gibraltar and Costa del Sol regions. The operation resulted in ten arrests and the seizure of three drones, control devices, and large sums of money and drugs (Orellana, 2024).

- unauthorized drones flying near airports or in restricted airspace can disrupt flights and potentially lead to accidents; drones can interfere with air traffic and pose a risk to aviation safety. At the begging of 2025 unauthorized drones interfered with firefighting operations in Los Angeles leading to collisions with firefighting aircraft and posing significant risks to emergency response efforts (Wise, 2025).
- drones can be hacked and controlled remotely by unauthorized individuals; this could allow malicious actors to use drones for unauthorized surveillance, data collection, or even weaponization.

- drones can be used to conduct surveillance on or attack critical infrastructure such as energy infrastructure (renewable energy infrastructure, natural gas production grids, power plants, etc.), communication networks, transportation systems, etc.; can disrupt services and cause significant damage.

Mentioning notable incidents regarding the energy infrastructure:

"Al-Houthi and Saudi Arabia Conflict (2019), Yemeni al-Houthi rebels attacked Saudi Arabian oil refineries and energy infrastructure using 10 long-range UAV-X drones. The strikes interrupted 5.7 million barrels per day of oil production, affecting Saudi Arabia's economy, regional security, and global energy markets; Russian-Ukraine Conflict (2022-present), the Ukrainian government has retaliated with a series of drone attacks targeting Russian power plants, gasoline distribution depots, and industrial refineries; Red Sea Conflict (2023-present), Al-Houthi forces in Yemen have increasingly used drones and ballistic missiles against civilian vessels, posing a new danger to the Red Sea's energy infrastructure and public transportation systems" (Ghenai, 2024).

- in crowded public events, drones can cause injuries if they malfunction or are deliberately flown into crowds; the potential for panic and harm is considerable in such scenarios.

An example is the drone show at Lake Eola Park in Orlando, Florida where multiple drones malfunctioned and fell into the audience. A young boy was struck by a falling drone resulting in serious injuries that required emergency openheart surgery (Sawyer, 2024).

The SWOT analysis only covers potential scenarios and highlights possible threats. The analysis provides a solid foundation for understanding the strategic, ethical, and operational impact of drones on international security. The aspects determined in the analysis, legal challenges, cybersecurity, proliferation, and ethical considerations are highly relevant in today's geopolitical landscape, where drone technology is rapidly evolving.

Although, following the analysis, drones have the potential to transform the security environment, it is important to address their weaknesses and mitigate threats to successfully and sustainably integrate them. Their long-term impact will be determined by investments in technological innovation and careful navigation of regulatory and ethical issues. Regarding their strengths, such as enhanced surveillance capabilities, rapid response potential, and cost efficiency, position drones as a transformative tool in improving security systems. They are invaluable in areas like border control, disaster response, and urban safety, offering innovative ways to detect threats and protect critical infrastructure. However, their weaknesses, such as vulnerability to hacking, technical limitations, and dependency on weather conditions, underscore the need for robust design and

operational safeguards. The opportunities drones provide, including advancing technologies like AI integration and multi-domain collaboration, can help address emerging threats and create proactive security strategies.

Conversely, threats like misuse by malicious actors, regulatory gaps, and ethical concerns about privacy must be actively managed. Addressing these challenges requires collaboration among governments, industries, and communities to ensure drones are used responsibly, effectively, and with proper oversight.

Through the SWOT analysis, the question of whether *drones are a threat to security* becomes nuanced. While drones offer strategic advantages (precision, surveillance, cost-effectiveness), they also present significant risks (proliferation, vulnerabilities, and ethical dilemmas). Their threat potential largely depends on how they are used and regulated. In the hands of both state and non-state actors, drones can either enhance security or create new avenues for conflict and instability.

To address various threats posed by drones, several mitigation strategies can be implemented:

- o governments can establish strict regulations on drone usage, which may include mandatory registration, licensing, and flight restrictions in sensitive areas;
- o the development of drone detection and neutralization technologies (radar systems, jamming devices, and nets) can help safeguard against unauthorized drone activities;
- o educating the public about the potential risks and promoting responsible drone usage can mitigate some of these threats;
- o critical infrastructure and sensitive sites can adopt enhanced security measures, including physical barriers and advanced surveillance systems, to detect and deter drone incursions;
- o collaboration among government agencies, the private sector, and international organisations can facilitate information sharing and the development of comprehensive strategies to combat drone threats.

Conclusions

Drones undeniably present significant security threats, particularly when used by malicious actors for espionage, smuggling, sabotage, or even terrorism. Their accessibility, low cost, and ability to bypass traditional security measures make them an attractive tool for nefarious purposes. Moreover, vulnerabilities such as hacking, GPS spoofing, and unauthorised surveillance amplify the risks they pose to privacy, infrastructure, and national security.

However, labelling drones solely as a threat overlooks their potential as security enablers when used responsibly and within a regulated framework. They can strengthen defence systems, aid in surveillance, and enhance emergency response capabilities. Thus, the threat they pose is highly dependent on the context of their use, the robustness of counter-drone technologies, and the effectiveness of regulatory measures in mitigating misuse.

In conclusion, the paper underlines that while drones present evolving threats to security, they also offer transformative opportunities for protection. Balancing these dual aspects requires proactive policies, technological innovation, and international cooperation to ensure their benefits outweigh the risks.

BIBLIOGRAPHY:

***, "A Brief History of Drones", *Imperial War Museums*. https://www.iwm.org.uk/history/a-brief-history-of-drones

Allen, G. C. 2022. Across Drones, AI, and Space, Commercial Tech Is Flexing Military Muscle in Ukraine. Retrieved from Centre for Strategic and International Studies (CSIS).:

- https://www.csis.org/analysis/across-drones-ai-and-space-commercial-tech-flexing-military-muscle-ukraine
- Cooperative Research Centres. 2024. FLIGHT CRITICAL: DRONES, CYBER SECURITY AND CRITICAL INFRASTRUCTURE. Retrieved from https://cybersecuritycrc.org.au/sites/default/files/2024-05/Flight% 20Critical.pdf
- Crossland, D. 2025. Drones spotted over German air bases prompt Russian spy fears. January 13. Retrieved from *THE TIMES* & *THE SUNDAY TIMES*: https://www.thetimes.com/world/europe/article/russia-spy-germany-drones-base-332v9sgfr
- Donlevy, K. 2024. Two suspected drones breach Romanian airspace in as many days, violating NATO sovereignty. October 19. Retrieved from *NEW YORK POST*: https://nypost.com/2024/10/19/world-news/two-drones-breach-romanian-airspace-in-as-many-days/
- Ghenai, C. 2024. Countering the Growing Threat of Drone Attacks on Energy Infrastructure. May 14. Retrieved from *NEW LINES INSTITUTE*: https://newlinesinstitute.org/environmental-challenges/countering-the-growing-threat-of-drone-attacks-on-energy-infrastructure/
- Gregory Quarles. 2023. *The Security Implications of Drone Threats*. 22 May. ASIS International: https://www.asisonline.org/security-management-magazine/articles/2023/05/uncrewed-aerial-systems/security-implications-drones/
- Kaplan, C. 2018. Aerial Aftermaths: Wartime from Above (Vol. Vol. 58). Press, Duke University. doi:10.1215/9780822372219
- Newcome, L. R. 2004. *Unmanned Aviation: A Brief History of Unmanned Aerial Vehicles*. January 1. American Institute of Aeronautics and Astronautics. doi: https://doi.org/10.2514/4.868894
- Orellana, J. S. 2024. *Dismantles a network of "narcodrones" that operated between Spain and Morocco*. November 28. Retrieved from Sociedad Española de Radiodimisión: https://cadenaser.com/andalucia/2024/11/28/desmantela-una-red-de-narcodrones-que-operabaentre-espana-y-marruecos-ser-malaga//
- Russo, J., Dulani Woods, Michael J. D. Vermeer, & Brian A. Jack. 2024. March. *Countering the Emerging Drone Threat to Correctional Security*. Retrieved from https://www.rand.org/pubs/research_reports/RRA108-21.html
- Sawyer, D. 2024. At least 5 shows cancelled after drones fell from the sky at Orlando holiday event. December 28. Retrieved from CNN: https://edition.cnn.com/2024/12/28/us/drone-shows-canceled-after-orlando-injury/index.html
- Shouthiri Partheepan, Farzad Sanati, Jahan Hassan. 2023. *Autonomous Unmanned Aerial Vehicles in Bushfire. Management: Challenges and Opportunities*. 10 January. URL: https://doi.org/10.3390/drones7010047
- U.S. military prioritizes AI-powered drones in defense modernization. 2024. August. Retrieved from Global Defence News 2024: https://www.armyrecognition.com/news/army-news/army-news-2024/u-s-military-prioritizes-ai-powered-drones-in-defense-modernization?utm_content=cmp-true
- Wise, J. 2025. *New York Magazine*. January 10. Retrieved from Intellingencer: https://nymag.com/intelligencer/article/los-angeles-firefighters-drones.html