Check for updates

RESEARCH ARTICLE

REVISED Employment of uncrewed systems in attacks on critical infrastructure: a hybrid threat perspective. Security challenges related to recent developments in technology.

[version 2; peer review: 1 approved with reservations, 6 not approved]

Michał Piekarski[1], Małgorzata Wolbach[2], Magda Okuniewska[2]

[1]University of Wrocław, Wrocław, Poland
[2]Polish Platform for Homeland Security, Poznań, Poland

v2 **First published:** 28 Jun 2024, **4**:129
https://doi.org/10.12688/openreseurope.17797.1
Latest published: 14 Jan 2025, **4**:129
https://doi.org/10.12688/openreseurope.17797.2

Abstract

Background

The uncrewed systems, known colloquially as drones are nowadays widely used in various roles, including strictly civilian, law enforcement and military. The pace of technological development is high, following modern technologies, like artificial intelligence. Due to the growing threat to critical infrastructure that includes physical attacks, a fundamental question arises: how the development of uncrewed systems transforms the threat to critical infrastructure.

Methods

Historical analysis of historical cases of uncrewed system development and employment was used to describe evolution of said systems. For assessment of possible threat to critical infrastructure, a scenario – based analysis was conducted. Seven scenarios, divided into three groups were described as typical contemporary scenarios of uncrewed system use. For assessment of influence of new and emerging technologies especially artificial intelligence, three further scenarios were analyzed.

Results and Conclusions

Scenario – based analysis show that the uncrewed systems has shown that evolution of uncrewed system, especially use of artificial intelligence increases potential threats to critical infrastructure, due to

Open Peer Review

Approval Status ✗ ✗ ✗ ✗ ? ✗

	1	2	3	4	5	6
version 2 (revision) 14 Jan 2025			✗ view	✗ view	? view	✗ view
version 1 28 Jun 2024	✗ view	✗ view	✗ view			

1. **Zachary S Kallenborn**, University of Maryland, College Park, USA
George Mason University, Fairfax, USA
Center for Strategic and International Studies,, Washington DC, USA

2. **Domenico Pascarella**, Italian Aerospace Research Centre (CIRA), Capua, Italy
Raffaele Elia, University of Campania Luigi Vanvitelli, Aversa, Italy
Massimiliano Rak, University of Campania Luigi Vanvitelli, Aversa, Italy

3. **Benjamyn Scott**, Universiteit Leiden Instituut voor Publiekrecht, Leiden, The Netherlands
Oyku Kurtpinar, Leiden University Leiden

growing capabilities. Therefore, it is recommended that future research work on countering such type of threat is required.

Keywords
Uncrewed systems, critical infrastructure, hybrid warfare, hybrid threats, drones

H2020 This article is included in the Horizon 2020 gateway.

University College The Hague, The Hague, The Netherlands

4. **Tijeni Delleji**, Military Research CenterScience and Technology for Defense Lab (STD), Aouina, Tunisia
5. **Nguyen Dinh Dung**, Le Quy Don Technical University, Hanoi, Vietnam
6. **Julian Estevez**, University of the Basque Country, San Sebastian, Spain

Please see the article web page for additional reviewers.

Any reports and responses or comments on the article can be found at the end of the article.

Corresponding authors: Małgorzata Wolbach (malgorzata.wolbach@ppbw.pl), Magda Okuniewska (magda.okuniewska@ppbw.pl)

Author roles: Piekarski M: Conceptualization, Investigation, Methodology, Resources, Writing – Original Draft Preparation; **Wolbach M**: Conceptualization, Methodology, Project Administration, Supervision, Writing – Review & Editing; **Okuniewska M**: Conceptualization, Methodology, Project Administration, Supervision, Writing – Review & Editing

Competing interests: No competing interests were disclosed.

Grant information: This work was supported by the Horizon 2020 Framework Programme [EU-HYBNET; 883054].

Copyright: © 2025 Piekarski M *et al*. This is an open access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

How to cite this article: Piekarski M, Wolbach M and Okuniewska M. **Employment of uncrewed systems in attacks on critical infrastructure: a hybrid threat perspective. Security challenges related to recent developments in technology. [version 2; peer review: 1 approved with reservations, 6 not approved]** Open Research Europe 2025, **4**:129 https://doi.org/10.12688/openreseurope.17797.2

First published: 28 Jun 2024, **4**:129 https://doi.org/10.12688/openreseurope.17797.1

REVISED **Amendments from Version 1**

We have undertaken a comprehensive revision of the article, aligning it with reviewers' feedback. Following their suggestions, the section addressing AI-related aspects has been omitted, as this topic necessitates further in-depth exploration. Instead, we have chosen to concentrate on a detailed analysis of potential attack scenarios, incorporating a broader perspective on advancements in drone technology. In particular, our revised focus considers emerging trends in drone usage, with special attention to developments observed during the ongoing conflict in Ukraine. These trends provide valuable insights into the evolving capabilities of drones and their implications for security and defense strategies. By refining the article in this way, we aim to provide a more targeted and relevant examination of the subject matter.

Any further responses from the reviewers can be found at the end of the article

Introduction

While uncrewed systems (US), more colloquially known as drones, have been known and used in various forms to perform multiple tasks for decades, they have become an increasingly visible issue in contemporary security studies due to significant changes and developments in this field. The first examples of weaponized drones represent various experiments from World War II and the Cold War. However, the threat of weaponized use of uncrewed systems has been changing in recent years and has serious implications for the security of critical infrastructure (CI).

There are several observed trends, including the proliferation of commercially available systems and the employment of artificial intelligence (AI) and machine learning. Other trends are particularly visible in the context of the Russo-Ukrainian war, such as the development of weaponized uncrewed maritime vessels and the weaponization of first-person perspective (FPV) drones. A key research question arises: How do current trends in the development of uncrewed systems influence possible scenarios of physical attacks on critical infrastructure systems and facilities?

Therefore, the first part of this article aims to describe the definition of critical infrastructure as well as uncrewed systems in general. These devices operate in several domains. Most of these are operating in the air domain - uncrewed aerial systems (UAS), which are helicopters, planes, and other flying machines. The other groups are maritime drones: surface and subsurface (underwater). Finally, the systems are employed in the land domain. All of them may also be divided by their assumed use: there are systems that were built for strictly military purposes and those that were designed for civilian markets and may be weaponized.

Methodology

To address the security challenges posed by recent technological developments, a scenario-based approach was adopted. Initially, risks associated with physical attacks on critical infrastructure and the development of uncrewed systems were examined, along with documented cases of their use against such infrastructure. This foundation enables a deeper assessment of the potential impact of recent advancements, including artificial intelligence. The scenarios were developed by the authors, with the analysis of AI's potential role being the authors' original work.

Critical infrastructure – definitions

Probably, the most intuitive definition of critical infrastructure (CI) would be strictly lexical, assuming that this is the part of infrastructure critical for accomplishing the mission of certain actors (persons or business entities). In a more formal approach, it is possible to compare some legal definitions to describe this sector better. The European Union legal system (Directive (EU) 2022/2557 of the European Parliament and of the Council on December 14, 2022, on the resilience of critical entities and repealing Council Directive 2008/114/EC) defines critical infrastructure as "an asset, a facility, equipment, a network or a system, or a part of an asset, a facility, equipment, a network or a system, which is necessary for the provision of an essential service"[i]. The mentioned "essential service" was defined as "service which is crucial for the maintenance of vital societal functions, economic activities, public health and safety, or the environment." Worth mentioning is also the fact that this directive also defines "critical entities", as "public or private entity which has been identified by a Member State in accordance with Article 6 as belonging to one of the categories set out in the third column of the table in the Annex." Such entities belong to 11 categories (and multiple subcategories): energy, transport, banking, financial management infrastructure, health, drinking water, waste water, digital infrastructure, public administration, space, and production, processing, and distribution of food[ii].

Critical infrastructure - risk of physical attacks in the context of hybrid warfare

The aforementioned services may be disrupted in various ways, and the context of hybrid warfare is relevant. According to R. Seely, there are six broad categories composing the toolbox of Russian hybrid warfare: "governance (including religion, culture, and law), economics and energy, politics and political violence, military power, diplomacy and public outreach, and information and narrative warfare"[iii]. Another author, M. Galeotti, describes various forms of hybrid warfare as the weaponization of different issues from crime to law. Another analyst, D. Kilcullen, proposes term "liminal warfare" to describe modus operandi of a state actor employing variety of tools from clandestine activities (the existence of certain operation is unknown), through covert, ambiguous and finally open actions[iv]. This may include violent and nonviolent activities. All these hybrid warfare activities have been employed in various forms, including information and narrative

[i] *Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC*

[ii] *Ibidem*

[iii] Seely, R. (2017) 'Defining Contemporary Russian Warfare: Beyond the Hybrid Headline', The RUSI Journal, 162(1), pp. 50–59. doi: 10.1080/03071847.2017.1301634

[iv] Kilcullen D. The Dragons and The Snakes. How the Rest Learned to Fight West Hurst & Co. London 2022

campaigns, which include spreading disinformation to influence the targeted society. This may include campaigns directly aiming at critical infrastructure to slow down or cancel some projects in a similar manner to other propaganda campaigns from the past, such as anti-nuclear campaigns. However, these campaigns are slow and the results are difficult to measure[v].

There are other possible explanations for this. For example, large-scale Distributed Denial of Service attacks (DDoS) may be conducted against critical digital infrastructure, denying access to important services. This may lead to a significant disruption of societal functions and significant financial losses, as illustrated by the well-known case of the 2007 cyberattack in Estonia[vi]. However, DDoS usually does not damage the hardware and may be repulsed by the modification of software or network settings.

Physical attacks have several advantages from the perspective of attackers. First, they do have direct consequences because attacked facilities or systems are rendered unusable; therefore, critical services may be limited or not provided at all. This leads to another consequence: damage or destruction imposes additional costs on rebuilding lost capabilities. This means money, but can also be described in other ways. Some systems cannot be rebuilt or quickly restored. In short timeframe. The manufacturing and delivery of unique devices can take a long time. Therefore, time needs to be considered. In addition, professionals may be affected, forcing the operator to replace wounded or killed ones, although operating sophisticated facilities such as power grids, communications facilities, or data centers may require a uniquely qualified workforce. The replacement may be long and costly.

Finally, if critical infrastructure is successfully attacked, this will allow the attacker to create a narrative in which the targeted state is weak and unable to provide basic services. This can be used for further hybrid applications. This can be illustrated in a simple scenario. If a targeted country is dependent on imported energy resources such as oil or gas, an attack may disrupt existing import facilities such as pipelines or port terminals. In addition, physical attacks can be conducted in a disguised manner, suggesting that they are a result of domestic conflict. For example, attacks on the energy sector can be attributed to far-right groups. The report from 2023[vii] highlights the ideological interest of the American far-right in attacking targets such as power grids or communications networks, especially 5G telecommunications networks, owing to widespread conspiracy theories related to this system. State actors can easily conduct a double-stage campaign. In the first stage, conspiracy theories or other ideological justifications are used to mobilize potential supporters. Then, these persons and groups are used to conduct actual attacks, complicating the internal situation of an attacked country. Then attacker may come with "stabilization" offer of providing necessary deliveries, potentially combined with some political or economic concessions, offering to deploy military forces as a "stabilisation" or "antiterrorist" force.

The drone threat - general perspective

Aerial drones have been used in military roles since World War II, and were employed during the Cold War. However, their roles are mostly limited to training support (aerial targets) or reconnaissance. The number of cases of armed drones was limited and mostly comprised experiments. For example, the US Navy tried to use a remote-piloted helicopter QH-50 armed with anti-submarine torpedoes as an alternative to piloted machines but reverted to using conventional helicopters because, due to technological limits, the attrition rate was higher than that of crewed machines[viii]. This illustrates the challenges related to the use of drones. They require reliable autonomous or remote-control systems. While a simple reconnaissance mission may (at least in theory) be conducted using a preprogrammed route, its course should be corrected by some navigational systems (internal or external, especially radio navigational aids). During the Vietnam War, the widely used Ryan 147 drone (military designation: AQM-34) and its variants required modifications to conduct successful missions, including the ability to input manual course corrections during mid-flight. A more ambitious long-range D-21 supersonic strategic reconnaissance drone failed[ix]. Despite these issues, during the Cold War, both sides had some form of reconnaissance drone. For example, the Soviet Union developed Tu-141 and Tu-143 Rejs systems.

The use of armed drones has resulted in additional problems. To strike particular targets, accuracy was required, especially if the target was small or moving. However, these early issues were gradually resolved. While in typical military applications, more efforts have been focused on the development of guided missiles of various kinds, and the results of technological progress have had effects on drones. The challenges are essentially the same: a missile or drone must be able to fly to a certain location and conduct a strike with acceptable accuracy. The main difference is the fact that conventional missile, even if using aerodynamic lift to fly – otherwise called "wings"– is designed as a one-way weapon, required to fly and strike target, while drones usually are designed to be recovered after missions. However, this distinction may be blurred because there are differences in design, modes of employment, and ad hoc modifications of existing systems, including one-way attack drones called "loitering munitions." Special attention should be paid to the development of one-way attack systems. In addition, drones may be operated on purpose, assuming that they will be lost during certain missions. The most important aspect is the development of various precision navigational systems and guidance methods for the successful operational use of armed drones. The most notorious case was the use of armed MQ-1

[v] For more details. T. Rid Active Measures. The Secret History of Disinformation and Political Warfare Farrar, Straus and Giroux New York 2020

[vi] *2007 Cyber Attacks on Estonia* https://stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf

[vii] C. Clarke, M Sakrsjig *et at* The Targeting of Infrastructure by America's Violent Far-Right https://ctc.westpoint.edu/the-targeting-of-infrastructure-by-americas-violent-far-right/

[viii] For more detailed analysis see J.D Bloom *Unmanned Aerial Systems: A Historical Perspective. Occasional Paper 37* Combat Studies Institute Press US Army Combined Arms Centre Ft Leavenworth 2010

[ix] Ibidem

Predator and MQ-9 Reaper aircraft in the Global War on Terror by the American military forces. While a detailed description of technological developments is beyond the scope of this study, it is possible to mention, among others:

- Progress in computer technology has allowed for digitalization and miniaturization of sensors, control systems, and communication devices.

- Development of small, inexpensive, and reliable digital cameras that took place in analog photographic or video cameras.

- The development of digital electronic intelligence and warfare sensors allows the gathering of information on various types of radio emissions.

- Development of reliable digital command and control systems, including capabilities of transfer of digital data, still images, and video feeds.

- Developments in computer processing power, allowing for progress in digital data processing[x].

All of these factors have a significant influence on US capabilities and modes of employment. During the Cold War, imagery was gathered through analog photography. This would require the recovery of the drone with films, which would have to be developed and analyzed. Later, the drone could carry an analog video camera, which would allow information to be gathered in real time. As proven by the successful use of RQ-2 drones in Operation Desert Storm, when drones were used as spotters for naval gunfire[xi], the time between gathering information (e.g., detecting target) and taking action (e.g., engaging the target) would be reduced. Additionally, analog video systems have several limitations. At the end of these early developments, commercially available drones employed widely available components (including computer chips) and consumer-grade electronics. The same mechanism that led to the availability of digital cameras in smartphones or stand-alone devices such as GoPro led to the availability of digital camera-equipped drones such as the well-known and widely available DJI Phantom (in fact, the first model of this drone was equipped with a GoPro camera). This led to lowering the cost of drones, expanding their capabilities, and widespread civil use - in various applications, from pure recreational to highly professional, such as news gathering, movie production, and agricultural work.

Similar to other inventions (for example: cars allowed robbers for easier getaway and computers opened new spaces for malicious activities), the availability of drones led to their use in applications other than civilians. The use of weaponized drones in armed conflicts is well documented and discussed in the latter part of the article.

[x] for more general description see Ch. Miller Chip War: The Fight for the World's Most Critical technology

[xi] J. D Bloom *Unmanned Aerial Systems: A Historical Perspective. Occasional Paper 37* Combat Studies Institute Press US Army Combined Arms Centre Ft Leavenworth 2010

Drone threat - review of known cases

The 2016 report[xii] describes 15 cases of terrorist organizations, groups, and individual persons engaged in various forms or attempts to use drones. However, not all of these included actual uncrewed system use. Some were limited to the possession of systems and not using them or conducting experiments. Others have attempted to strike targets that can be identified as part of the critical infrastructure. Notable cases of actual drone use in intelligence gathering as well as in a weaponised form were by the Islamic state in Syria and Iraq (ISIS). This organization employed commercial drones such as the DJI Phantom quadrocopter. In a weaponized form, these devices were equipped with a crude but effective carrying and release mechanism for loads, such as grenades[xiii]. Earlier attempts include Rewzan Fedarus' 2011 plot to attack the pentagon – maybe one of the earliest attempts, while the feasibility of planning (using just off-the-shelf flying models) could be questioned[xiv]. It is notable that the person decided to conduct an attack in such an unusual manner at this time.

Other organizations, such as Hezbollah and Hamas, became more advanced and more successful in using drones. This is not surprising, considering their resources and the level of political ambitions. This group of actors was later joined by the Houti Movement in Yemen. Due to Iranian support, this group managed to build significant capabilities before the present (2023–2024) Red Sea crisis. The first sign of these capabilities was the use of Qasef-1 drones, capable of delivering a 30–45 kg explosive warhead with a range of up to 150 km. Later, the group used different drones from the Sambaed family, which had an estimated range of up to 1500 kilometres[xv]. These capabilities allowed Houtis to conduct attacks on the Saudi gas facilities in 2019[xvi]. Further cases illustrate their ability to attempt strikes on more distant targets, including Israel.

Other well-known cases are related to the large-scale Russian invasion of Ukraine. A campaign against Ukrainian critical infrastructure, especially the power grid, is widely conducted with a shared family of one-way drones, resulting in significant damage to the Ukrainian power system. In addition, Ukrainian forces have been engaged in strike operations against Russian targets, including military bases, the defence industry, and petroleum facilities. Ukrainian forces have used various types of devices, including converted Soviet era Tu-141 jet – powered reconnaissance, locally propelled UJ-22 Airborne and Bober planes, and commercially available Skyeye 4450 (made in

[xii] D. Rassler Remotely Piloted Innovation Terrorism, Drones and Supportive Technology Combating Terrorism Center, West Point 2016

[xiii] More detailed information: D. Rassler The Islamic State and Drones: Supply, Scale, and Future Threats. West Point 2018

[xiv] *Ibidem* pp 19–22

[xv] CAR Evolution of UAVs Employed by Houthi Forces in Yemen https://www.conflictarm.com/dispatches/evolution-of-uavs-employed-by-houthi-forces-in-yemen/

[xvi] https://www.iiss.org/online-analysis/online-analysis//2019/08/houthi-uav-strategy-in-yemen

China)[xvii]. In addition, there are known cases of conversion of piloted planes to uncrewed attack drones[xviii].

The use of drones against critical infrastructure is not only related to lone actors or war zones. For example, in 2019, a drone was found near an electrical substation in Pennsylvania, and the drone, a DJI Mavic, was modified with copper wire to disrupt the facility[xix]. Another known case was the sighting of drones of unknown origin flying over and around the Palo Verde Nuclear Generating Station in the United States[xx]. In 2022, suspicious drone activity was reported near the Norwegian Roar Gas Field in the North Sea[xxi]. Similar incidents have occurred in Norway[xxii] and Sweden[xxiii].

All these incidents, despite occurring in different places and under various conditions—from international war and terrorist activities to possible espionage—raise an important question. Is it possible to categorize threats to critical infrastructure in a way that offers a framework for planning security measures and provides insight into potential future threats?

Drone threat – possible scenarios

The analysis of the trends described above in the development of uncrewed systems allows the description of actual and potential methods for the employment of drones. In 2016, the West Point report divided these methods into five categories: surveillance, external commands, smuggle/courier, disrupt, and weapons[xxiv]. From the perspective of threats to critical infrastructure, it is possible to narrow this set to three groups: intelligence gathering, disruption, and kinetic attacks (destruction, damage, or disruption). Each of these groups provides a sketch of several scenarios. Here is a non-exhaustive set of scenarios that can, of course, be widened.

1. Intelligence gathering

The first and most common malicious use of drones is the gathering of intelligence that is useful to adversary actors. Depending on the nature of the requirements and context in which intelligence is gathered, this wide category may be divided into several narrower scenarios.

Scenario 1.1 Covert intelligence gathering

In this scenario, an adversary actor aims to gather information that allows for further decisions and actions, including attacks. Therefore, this information should be collected without alerting potential targets. The uncrewed systems offer particular advantages, especially allowing for the remote collection of intelligence, thus minimizing the risk of exposure of persons who may stay away from the target. Drones can be employed to gather the intelligence of a particular facility in order to gather information about buildings, installations, and entrances. This basic intelligence may be acquired during a quick overflight. Another method may be persistent surveillance if the drone is able to stay in the area of interest for several hours. This may allow noticing the movements of persons and vehicles in and around the facility and detect constant patterns (e.g., time when employees arrive and leave the facility, schedule of deliveries, or service works such as maintenance). Additionally, information on security systems and the behavior of security personnel may be collected in this manner. For example, drone surveillance may reveal that guards follow certain patrol patterns, making their actions predictable. Another option is to use drones to follow moving targets to gather intelligence regarding the movements of people and vehicles. This type of persistent surveillance was employed by US military forces during counterinsurgency and counterterrorist operations in Iraq. That "unblinking eye" allowed to create "patterns of life" of persons of interest, gather information on places and areas of interest[xxv]. While the US forces targeted terrorists and insurgents, owing to developments in technology, adversary actors may gather intelligence on possible targets in a similar manner, thus supporting their planning process. In addition, this method of using drones may include various modes of data-gathering. Commercially available drones, purchased off the shelf without any modifications, can provide daylight photos and video imagery. However, depending on the available resources, other sensors can be used. Drones may carry (or place) low-light, infrared, and thermal cameras, allowing for gathering imagery at night. Other possibilities include the use of acoustic sensors or electronic intelligence devices to intercept radio transmissions, which include GSM signals (cell phones) and Wi-Fi networks, as well as other devices. Aerial platforms, owing to their ability to overflight natural and artificial obstacles (e.g., fences), may offer particular use in that scenario. In addition, maritime and land platforms may be employed in a similar manner; for example, uncrewed submarine vessels may sneak into a port or gather intelligence on offshore platforms. Since this scenario assumes covert intelligence gathering, the exact number of such incidents is not known. This case is known only if a drone has been spotted. One of online accessible databases – "Drone

[xvii] A. Mladenov Bitting back Air Forces Monthly October 2023

[xviii] H. Altman Ukraine Appears to Be Using Light Planes Converted Into Reusable Bomber Drones https://www.twz.com/news-features/ukraine-appears-to-be-using-light-planes-converted-into-reusable-bomber-drones

[xix] Law enforcement discovers modified drone near electrical substation https://abcnews.go.com/GMA/News/video/law-enforcement-discovers-modified-drone-electrical-substation-80967575 29.02.2024. Also J. Trevithick Likely Drone Attack On U.S. Power Grid Revealed In New Intelligence Report https://www.twz.com/43015/likely-drone-attack-on-u-s-power-grid-revealed-in-new-intelligence-report. 29.02.204

[xx] T. Rogoway, J. Trevithick The Night A Mysterious Drone Swarm Descended On Palo Verde Nuclear Power Plant https://www.twz.com/34800/the-night-a-drone-swarm-descended-on-palo-verde-nuclear-power-plant

[xxi] https://www.reuters.com/business/energy/drone-activity-reported-near-north-sea-gas-field-danish-police-say-2022-10-04/

[xxii] https://www.euronews.com/2022/10/23/fears-grow-as-more-suspicious-drones-appear-above-norways-offshore-facilities

[xxiii] https://www.reuters.com/world/europe/swedish-security-service-investigates-drones-three-nuclear-plants-2022-01-17/

[xxiv] D. Rassler Remotely Piloted Innovation Terrorism, Drones and Supportive Technology Combating Terrorism Center, West Point 2016.

[xxv] S. Naylor Relentless Strike. The Secret History of Joint Special Operations Command St. Martin Press New York 2015

Attack & Incident Tracker" – of such incidents contains information about eleven cases[xxvi].

Scenario 1.2 Overt intelligence gathering

This scenario assumes that drones are employed voluntarily to trigger and gauge responses. This response may include the activation of emergency communication networks, crisis management plans, and deployment of additional security forces or systems. This may lead to gathering valuable intelligence, especially regarding communication systems that are used in emergency situations. It may allow the reconstruction of a chain of command and communication, measurement of response time, and detection of systems that are deployed to counter the drone. It was suggested that some of the mysterious sightings of flying objects in the US airspace were the result of such activities, aimed at gathering data on the US Army air defense systems[xxvii].

Scenario 1.3 Reconnaissance during kinetic attack and post-strike assessment

This scenario assumes that a drone is deployed as an asset to support other actions. This may include attacks conducted by persons, such as raids on a particular objective (facility), who may utilize intelligence-like live videos gathered by an uncrewed system to avoid detection by patrolling security personnel. In addition, after an attack, drones may be employed to conduct damage assessment, providing fast information about the results of the attack and the necessity of repetition of the attack against a particular target. Gathered footage can also be used for strategic communication (e.g., showing successful attacks in an attractive manner).

2. Disruption

This group of scenarios comprises two main proposals, assuming that drones are used not to destroy the target but to disrupt the operation of a given facility.

Scenario 2.1 Disruptive drone behaviour

This scenario assumes that drones are employed in a manner that has a direct effect on the attacked facility, system, or service by disrupting regular operations. This may result in the implementation of contingency, crisis response plans, or the activation of additional security assets. These actions interrupt operations, leading to suspension of critical services. One example is drones that penetrate the controlled airspace of major airports. The presence of an unauthorized aerial vehicle in such a space will result in major changes in the departures and arrivals of planes using this airport for security reasons. This scenario occurred in December 2018 at Gatwick airport when, twice in one week, unauthorized drone incursion resulted in hundreds of flights being delayed affecting 120 000 passengers, due to the inability to conduct normal operations[xxviii]. It is easy to notice that in this type of activity, passenger flights may be affected. Drones may be employed aggressively (a phenomenon called "buzzing") over heliports dedicated to emergency services (such as medical emergencies, police, or fire services), forcing helicopters to abort starting or landing attempts in fear of collision with a drone. This form of harassment is not limited to airspaces. Unauthorized operation of uncrewed maritime vehicles, operated in an unsafe manner, may disrupt traffic on shipping lines, especially in the proximity of ports (anchorages, roads, inland waterways), where it may be difficult to avoid dangerous areas. In addition, repeated cases of drone incursion may place additional strain on personnel, increasing work-related stress, and may lead to serious fatigue, resulting in a slowing response or threat neglect. The second option is particularly dangerous. If there are recurrent cases of drone activity, but limited only to "buzzing" or other form of disruption, but not resulting in more dangerous situations, personnel employed at the attacked facility may begin to consider this activity as irritating but benign, originating from merely irresponsible persons. This may lead to neglect of security procedures. This may, in turn, hamper detection and response to more advanced threats.

Scenario 2.2 Jamming

This scenario assumes that uncrewed systems are platforms for electronic warfare. Such systems may be employed to disrupt or deny radio communication or other radio-frequency emissions, such as navigation systems. This type of activity may make certain critical systems difficult or impossible to use. One possibility is the use of jamming satellite navigation systems (such as GPS or Galileo) or cellular networks (GSM). In addition, some systems such as transportation systems are particularly vulnerable to jamming. Planes, trains, and ships require reliable communication for safe operations. Another possibility is to use drone-borne jamming devices to send specific systems such as alert messages, causing the cessation of certain activities. For example, in Poland, the railway radio communication system has a built-in feature that allows sending an alert signal to remotely stop trains within the range of the signal. The malicious use of this system has caused significant delays. Drones may allow the placement of a jammer at a certain location or height, providing the optimal conditions for propagating jamming signals.

3. Kinetic attacks (destruction)

This employment of uncrewed systems can lead to several scenarios in which drones are employed to destroy targeted systems or facilities. Drones can only be used as weapons or in combination with other tools.

Scenario 3.1 Drone as weapon carrier

This scenario assumes that an unmanned system is a platform for weapons, potentially employed against the critical infrastructure systems, facilities, and persons employed at

[xxvi] https://d-fendsolutions.com/drone-incident-tracker/?from_date=20210101&until_date=20240313&sector=Critical Facilities and Infrastructure&incident_type=Espionage

[xxvii] https://www.twz.com/40054/adversary-drones-are-spying-on-the-u-s-and-the-pentagon-acts-like-theyre-ufos

[xxviii] https://www.bbc.com/news/uk-england-46654797

these facilities. Because a drone is used only as a carrier, its mission is to deliver the ordnance and recover it for future use. This makes this option particularly useful for repeated attacks or when the value of the drone (including its carrying capabilities) is much higher than the weapons carried. These can be divided into at least three subcategories. In the first, a drone carries weapons that are launched or dropped on target-like guided or unguided bombs or missiles. Maritime applications may involve launching the torpedoes. It is also possible to employ ground-uncrewed vehicles as missile or missile launching platforms. The armament may even include smaller drones[xxix]. This category of armament allows for conducting "standoff" attacks, and weapons carriers remain at a relative distance from the target, optimally beyond the range of defence systems. On the other hand, drones may carry armaments fixed to the vehicle, such as a machine gun or a grenade launcher. This may require getting close to the target in a manner similar to that when crewed vehicles are employed. In addition, drones may be used to carry mines or explosive devices that are placed in a covert manner and are activated at a later stage. Finally, drones can carry other devices designed to cause damage. This is the case with the already mentioned drones equipped with a copper wire to damage the electrical substation. There are a wide variety of such options, including the adoption of commercially available off-the-shelf drones as carriers of improvised explosive devices. This tactic was widely employed by Islamic State forces[xxx] and is used in other armed conflicts. They may use fully improvised devices, as well as depending on the available resources and scale of operations–standardization of purchased drones, equipment, and explosive devices–again, adapted (like hand grenades or other munitions), or purpose-built. The use of off-the-shelf drones has significant advantages, particularly low cost and high availability (including online sales). It is also possible to use "front" actors (persons or companies) to acquire them, thus maintaining an operational covert. One of the disadvantages is the limited choice of devices, the fact that they were built for peaceful purposes, or their range, endurance, or limited carrying capability. For example, the widely popular DJI Phantom Pro 4 can carry 800 g of payload under ideal conditions, and a bigger one, DJI Matrice, can carry up to 6 kg[xxxi]. More advanced and expensive devices, such as agricultural drones, may carry several dozens of kilograms of payload, such as DJI Argas T40, which can carry up to 50 kg[xxxii]. A more advanced method employs devices built for kinetic operation. A classic case is a military drone, for example, the already mentioned and well-known American MQ-1 Predator and MQ-9 Reaper, which can carry laser-guided missiles such as AGM-114 Hellfire and laser-guided bombs. There are other possibilities, depending on the capabilities available to the actor conducting the attack, and the availability of certain types of weapons and ammunition may be critical factors. For example, there are known cases of drones attached with firearms, made by amateurs and seemingly just an experiment[xxxiii], but there are also more professional solutions. Polish-made Perun ground uncrewed vehicles may be armed with machine guns in their dedicated weapon station (turret) or with guided anti-tank missiles[xxxiv]. Therefore, the only limits are strictly technical factors (especially drone parameters) and the availability of weapons.

Scenario 3.2 One way attack drones

This type of system is often referred to as "kamikaze drones" because they are built and employed in a manner that assumes that a drone is destroyed during an attack. Known examples in the aerial domain are systems described as "loitering munition", such as Polish Warmate[xxxv] or Israeli Harop[xxxvi]. In addition, FPV drones (First Person View), well-known from the Russia-Ukraine War, fall in this category; however, they are much more ad hoc constructed systems, for example, using warheads from locally available weapons. Another form of one-way weapons is systems used by Russia, including Iranian-designed Shahed 136 drones. There is also a documented attempt to convert large airplane models to one-way attack drones. It is also possible to convert conventional manned aircraft to uncrewed aircraft by exploiting their capabilities (range and payload) and availability (especially general aviation planes used for sports, recreational, and other purposes).

Ukrainian forces employ other solutions in the maritime domain in the form of uncrewed surface vehicles[xxxvii]. One-way attack drones can also be manufactured in the ground domain and designed to strike certain targets. One of the earliest examples is "Goliath" self-propelled, remote-controlled demolition device employed during World War II by the German Army. It is easy to assume that every ground vehicle that can be remotely controlled can be adapted to this role.

Impact of new technological developments

Norine MacDonald and George Howell's 2019 article "Killing Me Softly: Competition in Artificial Intelligence and Unmanned

[xxix] For example, Estonian Milrem company offers two types of combat uncrewed vehicles, one - TheMIS can be used in several variants, including armed, while other Type-X is essentially concept of uncrewed light tank https://milremrobotics.com/defence/

[xxx] D. Rassler Keep It Simple, Stupid! The Islamic State' s Tactical and Operational Drone Innovations. Combatting Terrorism Center at West Point (2018)

[xxxi] M. Piekarski, K. Wojtasik Protection of Polish critical infrastructure (CI) against air threats Security and Defence Quarterly 2022;39(3):76–87

[xxxii] https://www.dji.com/pl/t40

[xxxiii] https://www.youtube.com/watch?v=MBBC-xL_MTg The video footage illustrates serious issues, for example drone is not able to compensate recoil

[xxxiv] https://polska-zbrojna.pl/home/articleshow/36214?t=Jak-Perun-z-Piratem

[xxxv] https://www.wbgroup.pl/produkt/system-amunicji-krazacej-warmate/

[xxxvi] https://www.iai.co.il/p/harop

[xxxvii] http://www.hisutton.com/Ukraine-Maritime-Drones.html

Aerial Vehicles"[xxxviii] identified several fields of technological progress of Artificial Intelligence related to aerial uncrewed systems:

- Air combat algorithms: a set of capabilities allowing for the successful use of drones in air-to-air combat[xxxix].

- Machine vision: labeling (interpretation) of data received from visual sensors (cameras).

- Manned–unmanned teaming – a combination of crewed and uncrewed elements in one combat system.

- Automated missions – the ability to conduct independent mission planning using preapproved parameters (e.g., target selection).

- Swarming – the ability to use multiple drones in a cooperative manner.

- Autonomous flight – the ability to navigate independently from external support systems such as ground commands or GPS systems.

- Counter UAV systems – the use of AI in systems countering enemy drones.

- AI and electronic warfare: the employment of artificial intelligence applied to electronic warfare, such as jamming.

Developments in fields such as artificial intelligence, drone technology, and autonomous systems have a significant impact on threats to critical infrastructure. For instance, machine vision enables faster processing of data gathered by drones, which, while useful for security applications (such as detecting concealed threats), could also be exploited to identify targets for sabotage. This capability, when combined with other advancements, can be concerning. Manned-unmanned teaming, for example, allows military forces to deploy "loyal wingmen" that support helicopters or fighter planes. However, an autonomous drone could similarly act as a lookout for attackers targeting critical infrastructure, potentially detecting and attacking first responders.

Drone warfare, particularly as it has evolved during recent conflicts like the Russo-Ukrainian war, highlights another critical issue. Autonomous drones are reportedly used in these conflicts to strike designated targets even when command and control links are disrupted[xl]. This capability poses a challenge for protecting critical infrastructure, as soft-attack methods (such as jamming the command link to force drones to land) may be ineffective. Instead, more aggressive countermeasures, such as physically neutralizing or capturing drones, might be required. The rapid deployment of electronic warfare systems in the Russo-Ukrainian war, where countermeasures are implemented within weeks, underscores the adaptability required to counter evolving drone threats, including vulnerabilities in existing counter-drone systems[xli].

Considering these developments, a complex attack scenario could involve a combination of tactics. For instance, intelligence-gathering drones capable of signal interception might conduct preliminary surveillance, with repeated overflights designed to trigger security responses. Such tactics could expose weaknesses in protection systems, enabling a more precise kinetic attack. Consequently, current security systems may have a limited operational lifespan, emphasizing the need for rapid upgrades or modular designs that can quickly adapt to emerging threats.

The increasing role of low-cost, commercially available technologies in drone systems is another critical factor, as seen in the Russo-Ukrainian war. Consumer drones, including first-person-view (FPV) drones and uncrewed surface vessels, have become alternatives to traditional weapons, sparking a rapid evolution in drone capabilities[xlii]. This shift is particularly concerning for critical infrastructure, where inexpensive, custom-made drone swarms capable of autonomous operation could present significant threats. The proliferation of such technologies amplifies the risks associated with hybrid threats.

Russia, given the current geopolitical landscape, is one of the most prominent actors engaged in hybrid actions against EU member states. The country's extensive experience with uncrewed systems could inform future hybrid attacks conducted by Russian intelligence services or allied radical groups. Consequently, low-cost threats should not be underestimated. The influence of low-cost drone technology on critical infrastructure protection and risk mitigation requires further, in-depth research.

Ethics and consent

Ethical approval and consent were not required.

Data availability

No data associated with this article.

Data is not relevant to the research method, therefore no data are associated with it

[xxxviii] Norine MacDonald George Howell Killing Me Softly: Competition in Artificial Intelligence and Unmanned Aerial Vehicles PRISM, Vol. 8, No. 3 (2019), pp. 102–127

[xxxix] Due to dynamic nature of air to air engagements, especially in close range (within visual range, colloquially known as "dogfight") this type of drone use was particularly challenging. The beyond visual range engagement, based mostly on radar data and long - range missiles was much easier for any forms of automation.

[xl] https://www.twz.com/news-features/automated-terminal-attack-capability-appears-to-be-making-its-way-into-ukraines-fpv-drones

[xli] See J. Walting J Bronk Mass Precision Strike: Designing UAV Complexes for Land Forces https://www.rusi.org/explore-our-research/publications/occasional-papers/mass-precision-strike-designing-uav-complexes-land-forces

[xlii] See more O. Molloy Drones in Modern Warfare: Lessons Learnt from the War in Ukraine https://researchcentre.army.gov.au/sites/default/files/241022-Occasional-Paper-29-Lessons-Learnt-from-Ukraine_2.pdf

Open Peer Review

Current Peer Review Status: ✗ ✗ ✗ ✗ ? ✗ ✗

Version 2

Reviewer Report 04 September 2025

https://doi.org/10.21956/openreseurope.20744.r56835

© **2025 Rogers J et al.** This is an open access peer review report distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

✗ **James Patton Rogers**
Cornell University Department of Human Development, Ithaca, New York, USA
Elizabeth Redmond
Jeb E Brooks School of Public Policy, Cornell University, Ithaca, NY, USA

This article conducts a wide-ranging historical and contemporary survey of drone technology, discussing how recent advancements constitute an emerging threat to critical infrastructure. Its engaging scenario-based format illustrates how different drone technologies and methods of employment can threaten facilities and vital social systems. The article is strengthened by addressing not only kinetic attacks but also reconnaissance and disruption, as well as drawing examples from both state and non-state actors. Debates surrounding drones in the context of critical infrastructure and hybrid warfare are becoming increasingly salient, and this article has the potential to make a valuable contribution.

The article has a strong foundation, but there are areas that need to be improved.

First, although the paper emphasizes the unique threat posed by drone technology to critical infrastructure, the scenarios do not sufficiently center on critical infrastructure itself. Some scenarios primarily focus on general tactical and operational drone uses without clearly connecting these to unique threats to critical infrastructure. For example, Scenario 1.1 discusses drone use for general intelligence gathering by referencing U.S. military practices in Iraq. However, the authors do not distinguish why intelligence gathering in a critical infrastructure context - such as surveillance of a nuclear power plant or wastewater facility - is fundamentally different from traditional wartime imagery or measurement and signature intelligence.

Second, while the authors effectively highlight the importance of drones in a hybrid warfare context, the term “hybrid warfare” is underdefined in the paper. The authors present multiple, differing definitions of this contested term, which cause confusion. The authors also initially link hybrid warfare specifically to Russia through the quote by R. Seely, which further complicates the section.

In line with these points, we offer the following suggestions:
1. The scenario structure could be improved by organizing each category around specific types of critical infrastructure rather than drone capabilities. Instead of structuring scenarios around 1) Intelligence gathering, 2) Disruption, and 3) Kinetic attacks, the authors could consider focusing on the critical infrastructure sectors most at risk. This could look like 1) Energy, 2) Digital Infrastructure, and 3) Transportation, as mentioned earlier in the paper. This approach would allow existing examples, such as drone attacks on Ukraine's electrical grid, electronic warfare targeting cellular networks, and disruptions at airports, to clearly support the paper's primary subject while becoming more narrative. It would also necessitate more research on specific critical infrastructure/drone cases, allowing for recent (understudied) empirical examples to be analyzed.

2. In the "Critical infrastructure—risk of physical attacks in the context of hybrid warfare" section, the paper would benefit from delineating one definition of hybrid warfare that best applies to critical infrastructure threats. Such a definition could tie the tactical uses of drones, e.g. kamikaze/one-way attack (OWA) drones employed to destroy civil energy infrastructure, to the larger theory of hybrid warfare discussed later. The authors could then add a dedicated paragraph explicitly addressing Russian hybrid warfare doctrine. This would enable a deeper discussion of disinformation strategies consistent with the Russian understanding of hybrid warfare as a component of larger information campaigns and could serve as a throughline across the scenarios. The authors could then incorporate the final paragraph of the section into one of the scenarios, demonstrating how a disinformation campaign might follow a drone attack or disruption targeting critical infrastructure.

3. To make room for this more in-depth and cutting-edge research, the authors are encouraged to remove the history section. This section not only includes some inaccuracies but also lacks purpose, given that the history of drones has been covered by many other contributions to the field.

References
1. Bilal, Arsalan. "Hybrid Warfare – New Threats, Complexity, and 'Trust' as the Antidote." NATO Review (2021). https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html.
2. Clark, Mason. "Russian Hybrid Warfare," Institute for the Study of War (2020). https://www.understandingwar.org/report/russian-hybrid-warfare.
3. NATO. "Hybrid Threats and Hybrid Warfare: Reference Curriculum," (2024). https://www.nato.int/nato_static_fl2014/assets/pdf/2024/7/pdf/241007-hybrid-threats-and-hybrid-warfare.pdf.
4. Redmond, E. "The Entropic Age and 21st Century Regional Science: Renewed Relevance Through the Study of Hybrid Warfare Dynamics," (2025).http://dx.doi.org/10.13140/RG.2.2.33513.40809.
5. Rogers, J. "The Darkside of our Drone Future," The Bulletin of the Atomic Scientist (2019). https://thebulletin.org/2019/10/the-dark-side-of-our-drone-future/.

Is the work clearly and accurately presented and does it cite the current literature?
Partly

Is the study design appropriate and does the work have academic merit?
Partly

Are sufficient details of methods and analysis provided to allow replication by others?
Partly

If applicable, is the statistical analysis and its interpretation appropriate?
Not applicable

Are all the source data underlying the results available to ensure full reproducibility?
Partly

Are the conclusions drawn adequately supported by the results?
Partly

Competing Interests: No competing interests were disclosed.

Reviewer Expertise: drone warfare, emerging and disruptive technologies, hybrid warfare

We confirm that we have read this submission and believe that we have an appropriate level of expertise to state that we do not consider it to be of an acceptable scientific standard, for reasons outlined above.

Reviewer Report 08 March 2025

https://doi.org/10.21956/openreseurope.20744.r51584

© 2025 Estevez J. This is an open access peer review report distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Julian Estevez
University of the Basque Country, San Sebastian, Spain

The authors of this article primarily aim to communicate that the rapid evolution of uncrewed systems (drones) represents a growing and increasingly sophisticated threat to critical infrastructure, particularly when viewed through the lens of hybrid warfare. Their main contributions compared to the existing state of the art include:

1. **Structured scenario framework**: The authors develop a comprehensive framework that categorizes drone threats into three distinct groups (intelligence gathering, disruption, and kinetic attacks), with specific scenarios under each. This systematic approach provides security planners with a practical taxonomy for threat assessment.
2. **Integration of recent conflict Insights**: The research incorporates fresh observations from the Russia-Ukraine war, demonstrating how rapidly drone technology is evolving in actual conflict situations. This moves beyond theoretical concerns to document real-world applications of weaponized commercial drones.
3. **Analysis of technology convergence**: The authors highlight how the combination of artificial intelligence, autonomous capabilities, and commercially available hardware creates new threat vectors that traditional security frameworks may not adequately address.
4. **Hybrid warfare context**: By situating drone threats within the broader context of hybrid

warfare, the authors demonstrate how physical attacks on infrastructure can be coordinated with other elements (information warfare, economic pressure) to maximize societal impact.

5. **Critical infrastructure vulnerability assessment**: The research offers a detailed examination of how drones challenge conventional critical infrastructure protection paradigms, which have historically focused more on physical perimeter security and cyber defenses rather than aerial threats.

The authors' main conclusion is that the security community needs to rapidly adapt to this evolving threat landscape, as conventional countermeasures may have limited effectiveness against autonomous, AI-enhanced drone systems. They particularly emphasize that low-cost, commercially available technology can now pose significant threats to high-value infrastructure, creating an asymmetric advantage for potential attackers that requires further research and new defensive approaches.

The bibliography included in the article is a bit old-fashioned and authors should include newer references of the current state of art of the technique. Actually, the speed of technical evolution in this area is so high, that I consider that it has nothing to do to compare a UAV in 2016 to an UAV now. It is true that critical infrastructures might be in danger, and that responsible states should prepare countermeasures, but the authors don't mention any of those C-UAS countermeasures, or how could they been stopped if they were cable driven UAVs, for instance, as in the last months in Ukraine.

I consider that the article could be more focused solely on the presence and evolution of UAVs in the war of Ukraine, and how did these weapons develope along the years of war and how they were used to attack critical infrastructures. Otherwise, I think that there are thousands of similar articles in non-research media and journals. This article could have been in fashion when Nagorno Karabakh conflict happened.

Is the work clearly and accurately presented and does it cite the current literature?
No

Is the study design appropriate and does the work have academic merit?
Partly

Are sufficient details of methods and analysis provided to allow replication by others?
No

If applicable, is the statistical analysis and its interpretation appropriate?
Not applicable

Are all the source data underlying the results available to ensure full reproducibility?
No source data required

Are the conclusions drawn adequately supported by the results?
Partly

Competing Interests: No competing interests were disclosed.

Reviewer Expertise: UAVs; autonomous navigation; machine learning; collaborative robotics; warfare; ethics.

I confirm that I have read this submission and believe that I have an appropriate level of expertise to state that I do not consider it to be of an acceptable scientific standard, for reasons outlined above.

Reviewer Report 21 February 2025

https://doi.org/10.21956/openreseurope.20744.r50116

© 2025 Dung N. This is an open access peer review report distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

?

Nguyen Dinh Dung
Le Quy Don Technical University, Hanoi, Vietnam

This article provides valuable insights into the evolving role of uncrewed systems, particularly drones, in posing threats to critical infrastructure. Here are some comments to enhance the manuscript:

1. Introduction: Provide a more detailed introduction that sets the stage for the topic's significance. Clearly outline the specific security challenges posed by using uncrewed systems in attacks on critical infrastructure.
2. Methodology: While historical analysis and scenario-based analysis are valuable methods, consider incorporating quantitative data or statistical analysis to support the conclusions drawn. Additionally, provide more details on the selection criteria for the scenarios analyzed.
3. Results: Present the results of the scenario-based analysis in a structured manner, highlighting the key findings from each scenario. Discuss the specific technological advancements, such as artificial intelligence, that contribute to the increased threat to critical infrastructure.
4. In the conclusion section, provide specific recommendations for policymakers, security professionals, and researchers on addressing the emerging threats posed by uncrewed systems. Propose potential strategies for countering these threats effectively.

Is the work clearly and accurately presented and does it cite the current literature?
Partly

Is the study design appropriate and does the work have academic merit?
Partly

Are sufficient details of methods and analysis provided to allow replication by others?
Partly

If applicable, is the statistical analysis and its interpretation appropriate?

I cannot comment. A qualified statistician is required.

Are all the source data underlying the results available to ensure full reproducibility?
Yes

Are the conclusions drawn adequately supported by the results?
Partly

Competing Interests: No competing interests were disclosed.

Reviewer Expertise: Drone management; unmanned aerial vehicles, system design; control device integration of aircraft; numerical simulation; testing systems, and Intelligent transportation management systems; transportation system in smart city; urban planning and forecasting.

I confirm that I have read this submission and believe that I have an appropriate level of expertise to confirm that it is of an acceptable scientific standard, however I have significant reservations, as outlined above.

Reviewer Report 30 January 2025

https://doi.org/10.21956/openreseurope.20744.r49791

© 2025 Delleji T. This is an open access peer review report distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Tijeni Delleji
Military Research CenterScience and Technology for Defense Lab (STD), Aouina, Tunisia

General Overview:

The paper explores the evolving threat posed by uncrewed systems (drones) to critical infrastructure, particularly in the context of hybrid warfare. The authors provide a historical analysis of drone development, assess potential threats through scenario-based analysis, and discuss the implications of emerging technologies, such as artificial intelligence (AI), on these threats. The paper is well-structured and explores a timely and relevant topic, given the growing use of drones in both civilian and military contexts. While insightful, certain areas require refinement to improve clarity, consistency, and overall impact. Below are detailed recommendations:

1. **Lack of a Clear Thesis:** While the paper covers a broad range of topics related to drone threats, it lacks a clear, central thesis. The authors could have focused more sharply on a specific argument, such as how AI-enabled drones represent a qualitatively different threat compared to traditional drones.
2. **Limited Discussion of Countermeasures:** The paper briefly mentions the need for counter-drone technologies but does not delve deeply into existing or potential

countermeasures. A more detailed discussion of how to mitigate the threats posed by drones would have strengthened the paper.

3. **Insufficient Engagement with Recent Literature:** The paper could benefit from a more thorough engagement with recent academic and policy literature on drone threats, particularly in the context of critical infrastructure. For example, the authors could have referenced works by scholars like Zachary Kallenborn, who has written extensively on drone swarms and their implications for terrorism and warfare.
4. **Overemphasis on Historical Cases:** While the historical analysis is valuable, it sometimes overshadows the discussion of current and future threats. The paper could have placed more emphasis on recent developments, such as the use of drones in the Russo-Ukrainian war, and how these developments might inform future threats.
5. **Lack of Technical Depth:** The paper could have provided more technical details on how AI and autonomous systems enhance drone capabilities. For example, the authors could have discussed specific AI algorithms, machine learning techniques, or sensor technologies that enable drones to operate more effectively in contested environments.

Recommendation:
The authors should address the weaknesses outlined above, particularly the need for a clearer thesis, a more detailed discussion of countermeasures, and greater engagement with recent literature. Once these revisions are made, the paper will be a valuable contribution to the field.

Is the work clearly and accurately presented and does it cite the current literature?
Partly

Is the study design appropriate and does the work have academic merit?
Partly

Are sufficient details of methods and analysis provided to allow replication by others?
Partly

If applicable, is the statistical analysis and its interpretation appropriate?
Not applicable

Are all the source data underlying the results available to ensure full reproducibility?
No

Are the conclusions drawn adequately supported by the results?
Partly

Competing Interests: No competing interests were disclosed.

Reviewer Expertise: As a Full Imagery Analyst and Senior Engineering Project Manager, my research focuses on leveraging advanced technologies such as Machine Learning, Deep Learning, Computer Vision, Multi-spectral Imaging, Anti-drone Swarm Systems, and Thermography. These cutting-edge methodologies are aimed at enhancing threat detection, situational awareness, and mitigation strategies, with a strong emphasis on integrating innovative solutions to address emerging security challenges effectively.

I confirm that I have read this submission and believe that I have an appropriate level of expertise to state that I do not consider it to be of an acceptable scientific standard, for reasons outlined above.

Reviewer Report 23 January 2025

https://doi.org/10.21956/openreseurope.20744.r49737

© 2025 Scott B et al. This is an open access peer review report distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Benjamyn Scott
Universiteit Leiden Instituut voor Publiekrecht, Leiden, South Holland, The Netherlands
Oyku Kurtpinar
Law, Leiden University Leiden University College The Hague, The Hague, South Holland, The Netherlands

The term “uncrewed systems” is not widely used. The authors state they want to focus on illegal use, so the law is central to illegality. The law in Europe, ICAO documents, and many States (including EU's) use “unmanned aircraft systems”. It is, thus, unclear why “uncrewed systems” is used. This could suggest something else is meant, that the paper is wider than flying vehicles (“aircraft”), or that research is incomplete.

The introduction specifically mentions “artificial intelligence”, but the author response states that AI is omitted. AI is then mentioned a number of times, but in a limited way. The scope of the paper is not clear - is AI in or out?

Responding to the point about “uncrewed aerial systems (UAS), which are helicopters, planes, and other flying machines.” First, the term is wrong for 2 reasons: (1) unmanned aircraft systems is the standard legal term and (2) UAS is the aircraft and system, where as helicopter is just the aircraft. The two do not allign. Second, the use of "VTOL" in EU law has made a distinction between VTOL and other aircraft (rotorcraft and fixed wing). Rotorcraft and fixed-wing are aircraft types, whereas manned or unmanned is a category of the type (see ICAO Annex 2). There is a difference between rotorcraft and helicopter. The inconsistent use of terminology makes the paper confusing and lacking precision.

It is good to see the link to NIS II. This provides a better definition of critical infrastructure. Of course, this definition is specific to that directive, so caution in applying it generally.

There is a general omission of aviaton-specifc regulations. These rules govern access and use of airspace, and design of the aircraft. These are fundamental to how drones are used. Of course, illegal users may not care for these rules, but breaching them can lead to criminal or administrative sanctions. Without mentioning these, the discussion of the use of drones is descriptive and factual. There are many examples given in the article, but the value of numerous cases is limited as it does not link to a critical legal analysis. Rather, they just repeat the same point

– i.e., things are happening. This leads to a general point – there is a lot of description without much critical analysis.

Key documents are missing, such as all the regulatory and policy work on counter drones. This seems crucial for the topic. Further, standardisation work on C-UAS is missing, such as that by EUROCAE.

Competing Interests: No competing interests were disclosed.

Reviewer Expertise: Law, EU Law, Aviation Law, Drone Law, Defence and AI Law

We confirm that we have read this submission and believe that we have an appropriate level of expertise to state that we do not consider it to be of an acceptable scientific standard, for reasons outlined above.

Version 1

Reviewer Report 31 July 2024

https://doi.org/10.21956/openreseurope.19240.r41927

© 2024 Scott B et al. This is an open access peer review report distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.



Benjamyn Scott
Universiteit Leiden Instituut voor Publiekrecht, Leiden, South Holland, The Netherlands
Oyku Kurtpinar
Law, Leiden University Leiden University College The Hague, The Hague, South Holland, The Netherlands

The article delves into the topic of how uncrewed systems may pose threats to critical infrastructure. It first defines critical infrastructure and presents the historical development of uncrewed systems. Then, possible scenarios of drone use for attacks against critical infrastructure, and additional scenarios for AI and autonomous capabilities are provided. The author concludes with suggestions on the issue.

There are typos and grammatical mistakes in the text. The article would benefit from additional proof-reading.

The authors begin with highlighting the term “uncrewed system” (US), but later give emphasis to flying drones (UAS). It seemed that US was being used as a synonym for UAS, but then reference to land and sea were used. This could cause confusion, with the later focus on the air dimension.

The authors uses UAS for “uncrewed aerial systems”, however, most of the legal and technical

documents use UAS for “Unmanned Aircraft Systems”. Also, the sentence that it includes helicopters, planes, and other flying machines needs more explanation because normally, UAS are different than aeroplanes and helicopters/rotorcraft, but in a future scenario, it could be possible that these are helicopters or aeroplanes without a pilot onboard.

The justification for including the US definition in an article of this scope could have been clearer. It would be beneficial to explain that this inclusion is meant to show that the definition in context connotes broader implications and is relevant for comparison with other regional definitions. The paper focuses on Poland, so reference to other jurisdictions need to be substantiated. Additionally, the focus on Poland also needs to be substantiated. Poland, for example, is a member of the EU, NATO and UN. Therefore, there are specific rules at a regional level (eg drone safety regulations, AI Act, GDPR and EU Counter Drone rules,) and at an international level (eg ICAO, UN Charter and ITU). These are relevant, so it is not clear why Poland requires special attention, as opposed to any other jurisdiction.

For the paragraph beginning with “Therefore, the first part of this article aims to describe the definition of critical infrastructure as well as uncrewed systems in general,” it would enhance the flow and clarity of the article to include an overview of the entire article. This could be achieved by briefly outlining what will be discussed in the subsequent sections and the overall purpose of each part.

While there are citations for certain contextual information, they are insufficient in some areas. For instance, the second half of page 5 provides mostly contextual information rather than the authors’ opinion, yet it lacks proper references. There are a number of academic, legal and policy citatons missing from the paper. It makes one wonder if these were consulted by the authors. If not, then the paper’s quality is questionable. If yes, then why are they not referenced.

The statement, “In 2016, the West Point report divided these methods into five categories: surveillance, external commands, smuggle/courier, disrupt, and weaponsxix. From the perspective of threats to critical infrastructure, it is possible to narrow this set to three groups: intelligence gathering, disruption, and kinetic attacks (destruction, damage, or disruption),” appears inconsistent. The categories listed (intelligence gathering, disruption, and kinetic attacks) are not actually a narrowed-down version of the West Point report's list. However, these categories do provide a relevant framework for the context of critical infrastructure.

For the EU context, the author might consider referencing the EU publication, “Handbook on UAS protection of critical infrastructure and public space: a five-phase approach for C-UAS stakeholders” (available here: https://op.europa.eu/en/publication-detail/-/publication/e05f89e1-6bc9-11ee-9220-01aa75ed71a1/language-en).

Regarding the three types of unmanned vehicles (air, ground, and sea) mentioned by the author, it would be beneficial to elaborate on how different rules apply to each type. This could provide valuable insight.

On pages 10-11, further explanation on how AI and autonomous capabilities impact the specific case study is needed. Without this, the described attack scenario could equally be executed using a remote pilot. Drone rules typically differentiate remotely piloted and autonomous. The later is an absolute term, where there is no pilot involvement. This is not explored. Further, autonomous and

AI are not synonymous. The EU's AI Act focuses on AI-enabled technology, whereas the drone rules focus on autonomous operations. There are different focuses; operations v technology. This is also not explored.

The statement, "While there may be, in the future, attempts to regulate the use of artificial intelligence," requires updating. There are already significant legislative efforts in this area, such as the AI Act and the Artificial Intelligence Liability Directive. Further, human rights could be better discussed.

When discussing existing regulations on drones, especially in airspace, citing specific examples such as regulations 2019/945 and 2019/947 would be helpful.

The sentence, "For example, it may be necessary to have available solutions for intercepting or destroying drones that do not require external navigation systems," is unclear and could benefit from rephrasing for better understanding.

The originality of the article is limited. The recommendations lack focus – who are they targeted towards and how could they be realistically implemented.

References

1. Verzele P, Rodriguez CB, Bezerra MF, Lacerda LD: Regional differences in Hg contents in the liver and muscle of the green turtle (Chelonia mydas) from three foraging grounds in Northeast Brazil. *Environ Sci Pollut Res Int*. 2024; **31** (3): 3917-3925 PubMed Abstract | Publisher Full Text

Is the work clearly and accurately presented and does it cite the current literature?
Partly

Is the study design appropriate and does the work have academic merit?
Yes

Are sufficient details of methods and analysis provided to allow replication by others?
Yes

If applicable, is the statistical analysis and its interpretation appropriate?
Not applicable

Are all the source data underlying the results available to ensure full reproducibility?
No source data required

Are the conclusions drawn adequately supported by the results?
Partly

Competing Interests: No competing interests were disclosed.

Reviewer Expertise: Law, EU Law, Aviation Law, Drone Law, Defence and AI Law

We confirm that we have read this submission and believe that we have an appropriate level

of expertise to state that we do not consider it to be of an acceptable scientific standard, for reasons outlined above.

Author Response 11 Dec 2024

Malgorzata Wolbach

We unfortunately disagree with reviewers' claim that "The authors uses UAS for "uncrewed aerial systems", however, most of the legal and technical documents use UAS for "Unmanned Aircraft Systems". Also, the sentence that it includes helicopters, planes, and other flying machines needs more explanation because normally, UAS are different than aeroplanes and helicopters/rotorcraft, but in a future scenario, it could be possible that these are helicopters or aeroplanes without a pilot onboard."
UAS are (apart of some rare lighter-than-air examples) technically fixed – wing planes or rotorcrafts - just without crew onboard. They obey the same rules of aerodynamics, the propulsion is similar to crewed ones. While the fact that due to being remotely controlled or autonomous – not crewed has certain legal consequences for legal use, our text is focused on scenarios of malicious – so, often illegal use, therefore, number of important legal issues or human rights – were omitted.

Competing Interests: No competing interests were disclosed.

Reviewer Report 23 July 2024

https://doi.org/10.21956/openreseurope.19240.r41926

© 2024 Pascarella D et al. This is an open access peer review report distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Domenico Pascarella
Italian Aerospace Research Centre (CIRA), Capua, Italy
Raffaele Elia
Department of Engineering, University of Campania Luigi Vanvitelli, Aversa, Italy
Massimiliano Rak
Department of Engineering, University of Campania Luigi Vanvitelli, Aversa, Italy

The paper reports a scenario-based analysis of drone-based threats against critical infrastructures. The following shortcomings should be considered to improve the presentation of the work:

- Structuring the abstract in multiple sections is not a good practice. It should be a succinct and compact description of the main points of the articles to allow readers to have a clear and complete overview of the work.
- The article lacks a well-defined methodology. There is only a brief mention of the methodology in the abstract, which confuses readers and makes the goal of the work and the authors' contributions unclear. As a consequence, the article does not follow a

systematic approach: it leads to an incomplete work and makes its originality doubtful.
- In some points, the article does not cite the literature: it is not clear if they represent original contributions by the authors or references to existing works in the literature. We suggest to consider some papers (some are listed below) where an analysis of the state-of-art is available for drone threats.
- The conclusions drawn are not appropriately treated. The authors include them in the "Recommendations" section: it confuses readers because it makes unclear if the recommendations are the conclusions drawn or not. Recommendations are surely required to suggest to interested parties how to act to avoid the mentioned issues. However, they also require an independent section and a more detailed description to justify their implementation. Lastly, the conclusions should brief summarize the main points of the work also highlighting the authors' contributions.
- In the section about critical infrastructures, the article discusses only physical attacks against critical infrastructures. However, cyberattacks should be also analyzed since the work aims at discussing an hybrid warfare context.
- The article should report a brief classification of drones (e.g., the one adopted by NATO) to be linked with the different threat scenarios.
- Scenario 2.2 (jamming) may be extended to consider the cases wherein drones are used as generic attack vectors for cyberattacks, e.g., for WiFi network sniffing and spoofing, for WiFi DoS attacks, etc. The online article https://www.theregister.com/2022/10/12/drone-roof-attack/ reports an episode for these threat scenarios.
- For the influence of artificial intelligence on the drone threat, also "communication management and support" may be considered as a field wherein artificial intelligence may be used in conjunction with drones, e.g., for aerial mobile (drone-mounted) base stations within smart cities towards 6G (as illustrated in https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10059153). Moreover, a swarming-attack scenario (e.g., to saturate the protection of critical infrastructures) is missing.

References

1. Ficco M, Granata D, Palmieri F, Rak M: A systematic approach for threat and vulnerability analysis of unmanned aerial vehicles. *Internet of Things*. 2024; **26**. Publisher Full Text
2. Chamola V, Kotesh P, Agarwal A, Naren, et al.: A Comprehensive Review of Unmanned Aerial Vehicle Attacks and Neutralization Techniques.*Ad Hoc Netw*. 2021; **111**: 102324 PubMed Abstract | Publisher Full Text
3. Lykou G, Moustakas D, Gritzalis D: Defending Airports from UAS: A Survey on Cyber-Attacks and Counter-Drone Sensing Technologies.*Sensors (Basel)*. 2020; **20** (12). PubMed Abstract | Publisher Full Text

Is the work clearly and accurately presented and does it cite the current literature?

Partly

Is the study design appropriate and does the work have academic merit?

Partly

Are sufficient details of methods and analysis provided to allow replication by others?

No

If applicable, is the statistical analysis and its interpretation appropriate?
Not applicable

Are all the source data underlying the results available to ensure full reproducibility?
Partly

Are the conclusions drawn adequately supported by the results?
No

Competing Interests: No competing interests were disclosed.

Reviewer Expertise: Security of Aerospace Systems

We confirm that we have read this submission and believe that we have an appropriate level of expertise to state that we do not consider it to be of an acceptable scientific standard, for reasons outlined above.

Reviewer Report 23 July 2024

https://doi.org/10.21956/openreseurope.19240.r41928

© 2024 S Kallenborn Z. This is an open access peer review report distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.



Zachary S Kallenborn
[1] Unconventional Weapons and Technology Division, University of Maryland, College Park, Maryland, USA
[2] Schar School of Policy and Government,, George Mason University, Fairfax, Virginia, USA
[3] Center for Strategic and International Studies,, Washington DC, USA

Overall, the article describes the history of unmanned system use, potential threats to critical infrastructure, and future threats related to AI and autonomy. Although the topic is novel, has merit, and the authors raised some interesting issues, I do not recommend it for publication.

My primary critique is the lack of a strong thesis for the article supported by robust arguments or evidence. As far as I can tell, the primary argument of the piece is that AI-enabled drones pose a potential threat to critical infrastructure, but the authors did not spend enough effort showing how that threat is categorically or meaningfully different from existing drone threats. The primary analysis I see about how AI-enabled drones are different is largely relegated to a single paragraph in the “Influence of AI on the drone threat,” section with some additional details in the three scenarios. And in that paragraph, I see several questionable assertions.

First, the argument that AI meaningfully reduces human video analysis seems spurious in this context. If we’re talking about surveilling a single facility with a single drone over a short period of time, that seems quite unlikely to generate such huge amounts of data that human analysis would

be difficult. I'm also quite skeptical about the idea that humans could not quickly notice security guard uniforms, except perhaps in narrow cases like mass gathering attacks, which does not appear to be included in the definition of critical infrastructure. Identifying a security guard in a uniform patrolling the perimeter of a critical infrastructure facility does not seem to require special training or time.

Second, the author rightly notes that autonomy would allow jamming to be overcome; however, autonomy does not require any meaningful AI capability. Current DJI systems have autonomy based on simple GPS waypoint navigation.

Third, I do not agree with the claim that "machine vision can significantly increase the quantity and quality of information," though I am also not sure I understand it. I do not see how machine vision would have any meaningful effect on the quantity or quality of information. Machine vision is a method of *processing* not collecting information. The quantity and quality of information collected would be based on other factors like the quality of drone sensors, the amount of time spent surveilling, and prevailing weather conditions.

Fourth, I do not see analysis of the tradeoffs, requirements, or limits involved with developing, or fielding AI-enabled drones. Several of the issues discussed entail quite significant technical challenges, such as training the machine vision systems, and acquiring or developing swarms, which do not appear to have been addressed.

Fifth, there is a rapidly growing literature on these topics that does not appear to have been addressed, these include:

- Pietrek, G. (2022). Threats to critical infrastructure. The case of unmanned aerial vehicles. *Journal of Modern Science*, *49*(2), 120-133.
- Scott Crino and Conrad Dreby. "Drone Attacks Against Critical Infrastructure." *Atlantic Council,* May 2020
- Haugstvedt, H., & Jacobsen, J. O. (2020). Taking fourth-generation warfare to the skies? An empirical exploration of non-state actors' use of weaponized unmanned aerial vehicles (UAVs—'drones'). *Perspectives on terrorism*, *14*(5), 26-40.
- Haugstvedt, H. (2023). A Flying Reign of Terror? The Who, Where, When, What, and How of Non-state Actors and Armed Drones. *Journal of Human Security*, *19*(1), 1-7.
- Cronin, A. K. (2019). *Power to the people: How open technological innovation is arming tomorrow's terrorists*. Oxford University Press.
- Kallenborn, Z., Ackerman, G., & Bleek, P. C. (2023). A plague of locusts? A preliminary assessment of the threat of multi-drone terrorism. *Terrorism and political violence*, *35*(7), 1556-1585.
- Kallenborn, Z. The Plague Beckons: On the Proliferation of Drone Swarms. *Future Warfare and* Critical Technologies: Evolving Tactics and Strategies, 12.
- Zachary Kallenborn, "A cascading catastrophe: The drone threat to critical infrastructure," Bulletin of the Atomic Scientists, November 26, 2021
- https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/unoct_car_global_report_
- Scharre, P. (2018). *Army of none: Autonomous weapons and the future of war*. WW Norton & Company.

There are several others too.

Although these issues form my primary reasons for declining, for the authors benefit I will note

several other areas I feel could use improvement.

I did not understand what the take-away on the critical infrastructure definition analysis was intended to be, particularly what definition the authors were adopting or the strengths and limitations of that definition. The authors would benefit from focusing more on what, if any, implications the different definitions have for the analysis of related UAS risks. The authors also should be clear about which one they will be using for the analysis. Given that the focus is on UAS risks to critical infrastructure, without a strong adjustment to this section, I would suggest eliminating it and simply footnoting the relevant definition.

Similarly, I found the section on case study analysis of past drone events did not really add much beyond the scenarios above. Those scenarios included various examples of past events, so what is different about the case studies? I would suggest eliminating this section and incorporating relevant details into the previous section on scenarios.

References

1. Pietrek G: Threats to critical infrastructure. The case of unmanned aerial vehicles. *Journal of Modern Science*. 2022; **49** (2): 120-133 Publisher Full Text
2. Crino S: Drone Attacks Against Critical Infrastructure. *Atlantic Council*. 2020.
3. Haugstvedt H: Taking fourth-generation warfare to the skies? An empirical exploration of non-state actors' use of weaponized unmanned aerial vehicles (UAVs—'drones'). *Perspectives on terrorism*. 2020.
4. Haugstvedt H: A Flying Reign of Terror? The Who, Where, When, What, and How of Non-state Actors and Armed Drones. *Journal of Human Security*. 2023; **19** (1). Publisher Full Text
5. Cronin A.K: Power to the people: How open technological innovation is arming tomorrow's terrorists. *Oxford University Press*. 2019.
6. Kallenborn Z, Ackerman G, Bleek P: A Plague of Locusts? A Preliminary Assessment of the Threat of Multi-Drone Terrorism. *Terrorism and Political Violence*. 2023; **35** (7): 1556-1585 Publisher Full Text
7. Kallenborn Z: The Plague Beckons: On the Proliferation of Drone Swarms. *Future Warfare and Critical Technologies: Evolving Tactics and Strategies*. 2021.
8. Scharre P: Army of none. *Autonomous weapons and the future of war. WW Norton & Company*. 2018.

Is the work clearly and accurately presented and does it cite the current literature?
No

Is the study design appropriate and does the work have academic merit?
No

Are sufficient details of methods and analysis provided to allow replication by others?
Partly

If applicable, is the statistical analysis and its interpretation appropriate?
Not applicable

Are all the source data underlying the results available to ensure full reproducibility?

Partly

Are the conclusions drawn adequately supported by the results?
No

Competing Interests: No competing interests were disclosed.

Reviewer Expertise: I am the first author on several peer-reviewed studies concerning terrorism tactics in general, drone and terrorism specifically, and technical advances in drones in general.

I confirm that I have read this submission and believe that I have an appropriate level of expertise to state that I do not consider it to be of an acceptable scientific standard, for reasons outlined above.

Author Response 11 Dec 2024

Malgorzata Wolbach

The article has been rewritten, highlighting the part that we consider most important – the use of drones against critical infrastructure and early developments visible in recent cases, especially Russo-Ukraine armed conflict that may influence the way the drones may be employed in hybrid warfare scenarios.

Competing Interests: No competing interests were disclosed.