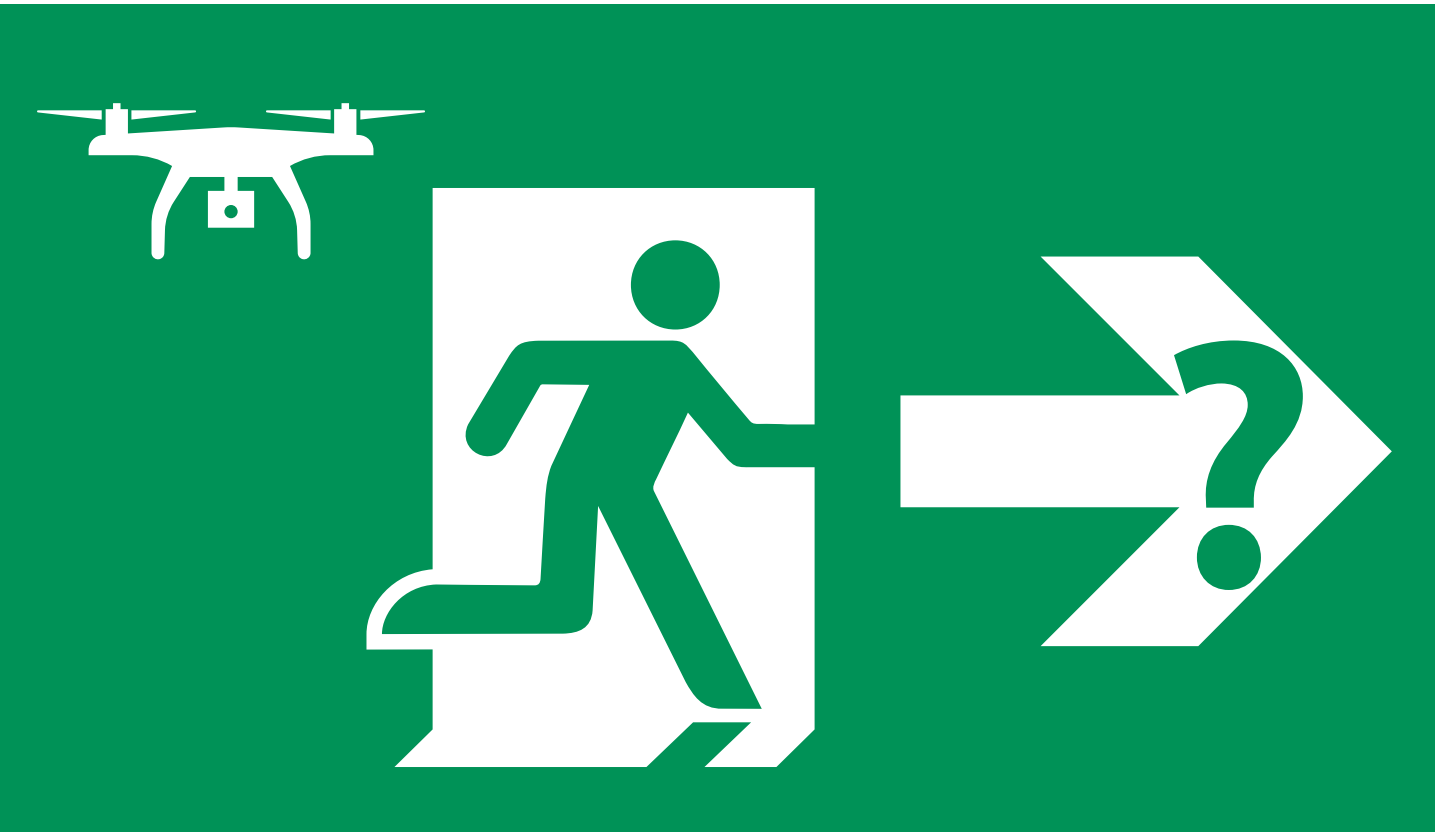


April 2024



Drone Drills

How to Prepare for a Drone Incident



© This work is copyrighted. All inquiries should be made to: The Editor, Joint Air Power Competence Centre (JAPCC), contact@japcc.org.

Author

Lieutenant Colonel André Haider, GE A

Acknowledgements

We extend our sincere gratitude to Lieutenant Colonel Kim Vogt (GE AF), Lieutenant Colonel Dennis Wartenberg (GE A), Lieutenant Colonel Eric Jodoin (CA AF), and Lieutenant Colonel Antonios Chochtoulas (GR AF) for their invaluable contributions and insights. Special thanks are also due to Mr Sascha Kranefeld for his exceptional work in conceptualizing and designing the drone evacuation point sign and information posters.

Disclaimer

This paper is a product of the JAPCC. It does not represent the opinions or policies of the North Atlantic Treaty Organization (NATO) and is designed to provide an independent overview, analysis and food for thought regarding possible ways ahead on this subject.

Terms of Use – Alteration, Notices

This White Paper may be reproduced for instruction, reference, or analysis under the following conditions:

1. You may not use this work for any commercial purposes, nor may it be used as supporting content for any commercial product or service.
2. You may not alter, transform, or build upon this work. Exception: Annexes A–C, F, G are accessible online and can be customized to meet the specific requirements of each organizational entity. These template annexes are intended to be used and modified as necessary to address individual organizational security concerns and potential threats. Download from the JAPCC website: <https://www.japcc.org/drone-drills>
3. All copies of this work must display the original copyright notice and website address.
4. A complete reference citing the original work must include the organization, author's name, and publication title.
5. Any online reproduction must also provide a link to the JAPCC website www.japcc.org, and the JAPCC requests a courtesy line.
6. This White Paper made use of other parties' intellectual property in compliance with their terms of use, taking reasonable care to include originator source and copyright information. The originator's terms of use guide the reuse of such material. To obtain permission to reproduce such material, please contact the copyright owner of such material rather than the JAPCC. In case of doubt, please contact us.

Copyright information contained within the White Paper made use of other parties' intellectual property in compliance with their terms of use, taking reasonable care to include the originator's copyright information. To obtain permission to reproduce, please contact the copyright owner of such material rather than the JAPCC. In case of doubt, please contact us.

Release

This document is approved for public release. This document is distributed to NATO Commands, Nations, Ministries of Defence, and relevant Organizations. Portions of the document may be quoted without permission, provided a standard source credit line, 'Courtesy of JAPCC' is included.

Published and distributed by:

The Joint Air Power Competence Centre
von-Seydlitz-Kaserne
Römerstraße 140
47546 Kalkar
Germany

Telephone: +49 (0) 2824 90 2201
Facsimile: +49 (0) 2824 90 2208
Email: contact@japcc.org
Website: www.japcc.org

 Denotes images digitally manipulated

Follow us on Social Media





From:

The Assistant Director of the Joint Air Power Competence Centre (JAPCC)

Subject:

Drone Drills – How to Prepare for a Drone Incident

Distribution:

All NATO Commands, Nations, Ministries of Defence and Relevant Organizations

The widespread availability and user-friendliness of drones, even without requiring significant investments or expertise, have raised concerns regarding potential misuse. Drones possess the capability to effortlessly breach physical security boundaries, capture high-definition imagery, transport explosives, chemicals, and other hazardous substances, or even launch attacks against wireless networks.

Identification of an unauthorized drone and determining whether its payload poses a potential threat to safety and well-being of personnel is a challenging task for an untrained observer. In such uncertain situations, it is crucial to exercise utmost caution until experts can assess the circumstances and grant clearance. The effective management of drone intrusions requires the establishment of well-trained and practiced immediate response procedures. Just as we prioritize first aid, fire safety, and bomb threat protocols, it is imperative to develop comprehensive strategies to address this growing concern.

This paper proposes a set of immediate actions that individuals should take in the first few minutes of a drone incident, prior to the arrival of security personnel such as the guard force or the police.

It is important to note that this paper intentionally does not delve into technically advanced countermeasures delivered by professional drone defence systems. Instead, its purpose is to provide guidance to individuals on how to respond to a drone incident in a safe and effective manner. This can be likened to administering first aid measures before the arrival of an ambulance or implementing evacuation measures before the arrival of a bomb squad.

I invite you and your staff to read this paper and use its content, and the online material provided at www.japcc.org/drone-drills to bolster your organization's drone response. We highly appreciate and encourage insightful comments and feedback from our readers. Should you have any queries or wish to share your thoughts, please do not hesitate to contact our Combat Air Branch via email at CombatAir@japcc.org.

Paul Herber

Air Commodore, NE AF
Assistant Director, JAPCC

JOINT AIR POWER COMPETENCE CENTRE

Joint Air Power Competence Centre | von-Seydlitz-Kaserne | Römerstraße 140 | 47546 Kalkar | Germany
Phone: +49 (0) 2824 90 2201 | Email: contact@japcc.org | www.japcc.org

Table of Contents

Executive Summary

Threats Originating from Drones.....	1
Drone Capabilities.....	1
Immediate Response Options.....	3
Preparatory Mitigation Options.....	3
Post Incident Measures.....	3
Conclusion.....	3

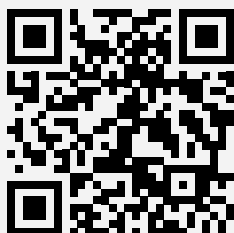
Chapters

1 Introduction.....	4
1.1 Background.....	4
1.2 Aim.....	5
1.3 Constraints and Limitations.....	6
1.4 Terminology and Definitions.....	6
2 Drone Threats – An Overview.....	8
2.1 Terrorism.....	9
2.2 Espionage.....	10
2.3 Sabotage.....	11
2.4 Subversion.....	12
3 Drone Imaging.....	13
3.1 Relevant Technical Specifications.....	13
3.2 Sensor Capabilities.....	14
3.3 Sensor Limitations.....	16
3.4 Assessment.....	16
3.5 Mitigation Options.....	16
4 Delivery of Explosives and Other Hazardous Materials.....	20
4.1 Airborne Improvised Explosive Devices.....	20
4.2 Hazardous Materials.....	25
4.3 Assessment.....	25
4.4 Mitigation Options.....	25

5	Cyber Attacks	27
5.1	Cyber Capabilities	27
5.2	Assessment	28
5.3	Mitigation Options	28
6	Drone Reporting	32
6.1	Drone Sighting and Classification.....	32
6.2	Immediate Warning Options	33
6.3	Centralized Alerts through Guards and Security Personnel.....	33
6.4	After Action Reporting and Incident Documentation.....	34
7	Conclusion and Recommendations	35
7.1	Conclusion.....	35
7.2	Recommendations.....	36

Annexes

A	Drone Sighting Report Sheet	37
B	Drone Incident After Action Report	38
C	Guidelines for Conducting a Drone Drill	42
D	Acronyms and Abbreviations	46
E	About the Author	48
F	Information Poster ‘Immediate Drone Response Measures’	49
G	Information Poster ‘Preparatory Measures Against Drone Threats’	51



Please visit

www.japcc.org/drone-drills

to download customizable templates for the annexes included in this paper, as well as additional educational references and materials.



 Drone: © AdobeStock, 260694458 (10 November 2023)

Run a drill!

***You don't have to have a flying object
to run a drill any more than you have to have
a fire to have a fire drill.***

Richard Lusk, Director, UAS Research Center,
Oak Ridge National Laboratory



Executive Summary

Well-established emergency procedures are vital for swift and efficient crisis management across military, civil, and public sectors. These protocols encompass first aid, fire, and bomb threat calls, aiming to save lives, prevent harm, and minimize destruction. Regular drills ensure that all stakeholders are well-versed in these procedures, contributing to effective crisis handling and safety.

While established protocols exist for common emergencies, organizations often lack specific plans for drone incidents, which are becoming more prevalent due to increased drone usage. Responses to drone incidents require tailored plans covering threat assessment, protection measures, and implementation of immediate procedures. Regular drills are essential to ensure readiness and proficiency.

Effective response to drone incidents might be delayed as Counter-Unmanned Aircraft System (C-UAS) technology is not yet widely available. Therefore, immediate actions upon detection are crucial to minimizing harm, damage, and potential casualties.

Threats Originating from Drones

The proliferation of drones and Unmanned Aircraft Systems (UAS) has brought opportunities and potential threats to various sectors. Drones with cameras raise concerns about privacy violations and breaching security as well as illegal monitoring of restricted areas and government facilities. Additionally, drone collisions and malfunctions pose physical hazards. The weaponization of drones and their potential for cyber-attacks add further dimensions to these concerns.

The accessibility of drones and their user-friendly controls make potential abuses feasible even without advanced expertise. The second chapter highlights recent incidents and the pressing need to address drone-related threats comprehensively, with tailored response plans, education, and countermeasures to ensure the health and safety of personnel.

Drone Capabilities

Even in their most affordable variants, drones can capture high-definition images and identify objects and individuals from substantial distances. The level



Figure 1: DJI Showroom in Katowice, Poland.

of detail varies, but a general guideline is that larger drones offer better imaging capabilities. Larger drones positioned a few metres away from a window can capture enough detail to read documents and computer screens inside a room. Moreover, larger fonts used in presentations, diagrams, headlines, and whiteboard notes are even more susceptible to drone capture.

The potential dangers posed by drones are magnified when considering their possible use as delivery systems for explosives. Small amounts of explosives can cause significant harm to the human body and easily break glass surfaces and windows. Common public and office buildings are often not designed to withstand explosions, focusing more on protection against burglary and intrusion. Detecting explosives within drones, especially when concealed, is exceptionally challenging for an untrained eye. Therefore, encountering an unauthorized drone requires extreme caution, treating the drone as a possible Improvised Explosive Device (IED) until professionals can assess the situation and provide clearance.

Chemical, biological, radiological, and nuclear substances have varying effects, with even minor quantities and brief contact times posing severe health risks. Dedicated equipment, such as liquid tanks with

spray nozzles or specialized containers, is needed to apply these substances. Caution is essential, especially if attached tanks or containers are visible. Professionals should always be consulted to respond in such situations, and individuals should refrain from employing their own measures to prevent being contaminated.

The evolution of cyberattacks has introduced new challenges. Previously, attackers had to approach target networks physically, risking detection and arrest. However, contemporary methods enable attackers to employ drones to breach physical security boundaries. Equipped with tools like the 'WiFi Pineapple'¹, an altered version of the Raspberry Pi², drones can infiltrate protected areas without the attacker's physical presence. Paired with local cellular connectivity, drones can launch substantial attacks against wireless networks, which can pose a significant threat, from compromising intellectual property and exploiting system vulnerabilities to breaching personal data. The potential for sabotage, including data deletion and destruction of computer-controlled equipment, is a reality. This merging of technology and tactics emphasizes the urgency of implementing comprehensive security measures in the rapidly evolving digital landscape.

Immediate Response Options

Any initial action should eliminate the drone's ability to cause harm or capture footage and images. Stand-off and staying clear of a drone are the best protection until trained professionals can take countermeasures. Recommended measures that can be handled easily and swiftly are locking the computer screen and leaving the room. Depending on the situation and available time, curtains and shutters can be closed, and sensitive documents can be covered or stored away. Doors should be closed, and staff should stay clear of glass surfaces and windows. Wireless connections should be turned off or at least checked if they are still connected to the network they are supposed to be on.

Preparatory Mitigation Options

Preventive safety measures can significantly minimize the required time or even eliminate the need for the immediate actions described above, thus saving critical time for a rapid evacuation. Recommended options include arranging workspaces not to be observed from the outside, installing window shutters, placing desks at a distance from windows, and establishing designated evacuation points for drone incidents. Educating staff on cyber security, providing best practices for handling mobile devices, and investing in enterprise-level wireless network security mitigates drone-delivered cyber threats.

Post Incident Measures

After a drone incident, the threat may not be over. Drones may have landed, left something behind, or even crashed. Until first responders arrive, personnel must keep clear of a landed or crashed drone and any unexpected objects found after a drone sighting, as it may carry explosives or other hazardous materials.

Conclusion

The widespread availability of drones has introduced a spectrum of security challenges. Drones can capture

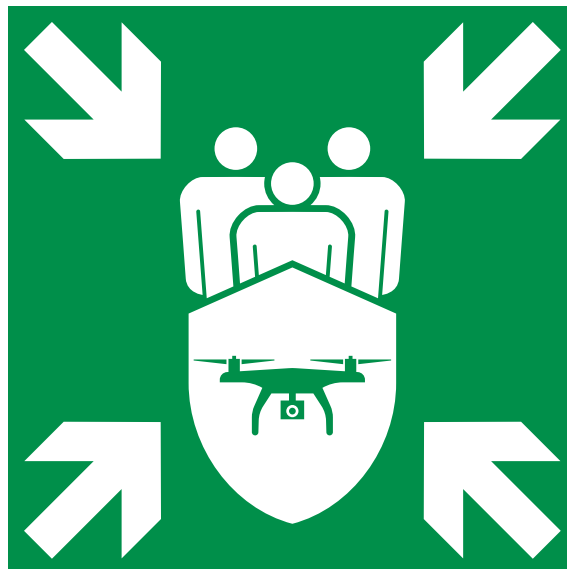


Figure 2: Unlike traditional safety measures like fire alarms, it is important to note that in the event of a drone incident, leaving the building may actually put you at risk of danger from the drone. As a result, designated assembly points should be established inside the building for this specific scenario. The illustration provided displays a recommended sign that should be placed in these designated locations. For easy access, the sign can be downloaded from the JAPCC website.

high-resolution images, detect objects, and even transport explosives. Privacy concerns arise as advanced drones can decode documents and screens, potentially exposing sensitive information. Safety risks are heightened when explosives are involved, as small amounts can cause significant damage and injuries due to the lack of blast-resistant structures and difficulties in detecting hidden charges. Additionally, even minimal quantities of hazardous materials carried by drones can cause severe health effects. The evolving landscape of cyberattacks adds another layer of complexity, with drones equipped with tools like the Raspberry Pi bypassing physical security to compromise networks and sensitive data. Education and training are vital to address these issues, enabling personnel to recognize threats, understand drone risks, and implement appropriate protocols.

1. Hak5 LLC, 'WiFi Pineapple', [online store], <https://shop.hak5.org/products/wifi-pineapple>, (accessed 7 November 2023).
2. Raspberry Pi is a series of small single-board computers originally leaned toward the promotion of teaching basic computer science in schools but can be easily turned into serious Wi-Fi hacking tools. Technical specifications and purchase options for the most recent model can be found at the Raspberry Pi Foundation's homepage at <https://www.raspberrypi.com/products>.



Chapter 1

Introduction

1.1 Background

Established and rehearsed procedures are essential for military, civil, and public organizations to respond quickly and efficiently to any emergency. So far, this typically includes having clear and well-rehearsed response plans and drills for first aid, fire, and bomb threat calls. These plans and exercises help to save lives, prevent injuries, and minimize damage. Moreover, regular drills ensure that everyone is familiar with the procedures and well-trained to handle emergencies, which is crucial for ensuring the safety of everyone involved.

Immediate measures for first aid typically include essential life support such as CPR (Cardiopulmonary Resuscitation), controlling bleeding, and stabilizing fractures or dislocations. Trained first responders may also be able to use an Automated External Defibrillator (AED) to assist someone in cardiac arrest. First aid kits, AED equipment, and related signs are also often required by law in public buildings and industrial facilities.

Immediate measures for fire typically include activating the fire alarm, calling the fire department, and evacuating the building. Trained individuals may also use fire extinguishers to try and control small fires. Similar to first aid, emergency equipment and related signs are often required by law, such as fire extinguishers, smoke detectors, or automatically closing doors to contain the propagation of a fire.



Immediate measures for bomb threat calls typically include evacuating the affected area, calling the police, and notifying the bomb squad. Trained individuals may also be able to recognize and report suspicious behaviour or packages.

While response plans for the above emergencies are standard, the same is rarely valid for drone incidents. The unwanted presence of drones is a relatively new phenomenon, and many organizations still need to develop specific plans to address this type of emergency. However, it is essential to note that with the increasing use of drones in both civilian and military contexts, the need for response plans and drills for drone incidents is becoming more pressing. Organizations need to develop and implement response plans that cover the time from incident detection to the arrival of first responders, including procedures for identifying and assessing the threat posed by the drone, as well as measures for protecting individuals and property. Regular drills are also essential to ensure everyone is familiar with the procedures and well-trained to handle drone incidents.

It is also important to note that the arrival of trained and equipped first responders to a drone incident may take a significant amount of time. Many military

and public facilities do not yet have or are not authorized to employ C-UAS equipment in peacetime, nor has it been widely introduced into the common police or guard force. This lack of availability and implementation again highlights the importance of immediate action after incident detection to minimize negative consequences and damage, prevent injuries, and save lives.

1.2 Aim

This paper aims to provide actionable drone response measures that one can quickly and easily implement to cover the timeframe from drone detection to the arrival of emergency responders or until a dedicated C-UAS system can intervene. Furthermore, examples of an immediate drone response warning sign, a preparatory measures info sheet, and a drone sighting report sheet are provided in the annexes. Customizable templates are also available as a digital download on the JAPCC website. Finally, this paper recommends preventive, cost-effective and easy-to-implement structural, organizational, and educational measures to complement and support the recommended immediate actions.



Figure 3: A Comprehensive Approach to Countering Unmanned Aircraft Systems.

1.3 Constraints and Limitations

This paper aims at both military and civilian target audiences. All information provided is unclassified and open to the public to maximize its utility. The templates provided can and should be customized to the individual needs of organizations that would like to use them and incorporate them into their security policy or emergency response plan.

This paper provides recommendations for preventive and immediate actions to protect human lives and health in the event of drone incidents in peacetime and crisis. It explicitly does not address military C-UAS operations in wartime or mission scenarios, as the JAPCC’s book on ‘A Comprehensive Approach to Countering Unmanned Aircraft Systems’, published in 2021, already covers these aspects in extensive detail.¹

1.4 Terminology and Definitions

Unmanned Aircraft (UA), Unmanned Aircraft System (UAS) and drone are terms often used interchange-

ably. For clarity, this paper uses these terms as described below.

Unmanned Aircraft System. A UAS is a system whose components include the UA, the supporting network, and all equipment and personnel necessary to control the UA.² NATO classifies UAS into three categories, ranging from Class I for the small and most miniature systems to Class III for the larger medium and high altitude UAS.³ For this paper, UAS indicates any military-grade unmanned systems covered by the NATO UAS Classification Table (*cf. Table 1*).

Drone. The term drone is predominantly used in the civilian domain and typically refers to UAS categorized as Class I by NATO. For this paper, the term drone refers to any non-military grade unmanned system, ranging from commercially available products for hobbyist and recreational use to customized airborne improvised explosive devices assembled in a terrorist workshop.

Counter-Unmanned Aircraft System (C-UAS)⁴ systems are purpose-built professional systems for de-

Category	Normal Employment	Normal Operating Altitude	Normal Mission Radius	Primary Supported Commander	Example Platform
Class III (> 600 kg)					
Strike/Combat	Strategic/ National	Up to 65,000ft MSL	Unlimited (BLOS)	Theatre	Reaper
HALE	Strategic/ National	Up to 65,000ft MSL	Unlimited (BLOS)	Theatre	Global Hawk
MALE	Operational/ Theatre	Up to 45,000ft MSL	Unlimited (BLOS)	JTF	Heron
Class II (150 kg–600 kg)					
Tactical	Tactical Formation	Up to 18,000ft AGL	200 km (LOS)	Division, Brigade	Watchkeeper
Class I (< 150 kg)					
Small (> 15 kg)	Tactical Unit	Up to 5,000ft AGL	50 km (LOS)	Battalion, Regiment	Scan Eagle
Mini (< 15 kg)	Tactical Sub-unit (manual or hand launch)	Up to 3,000ft AGL	Up to 25 km (LOS)	Company, Platoon, Squad	Skylark
Micro (< 66J)	Tactical Sub-unit (manual or hand launch)	Up to 200ft AGL	Up to 5 km (LOS)	Platoon, Squad	Black Widow

© NATO

Table 1: NATO UAS Classification Table.⁵

tecting, tracking, and engaging non-cooperative UAS or drones. Many companies also refer to their C-UAS solutions as drone defence systems as a way to market these systems to their civilian customers. For this paper, drone defence systems are included in the generic terms C-UAS and C-UAS systems, which range from portable solutions, such as anti-drone rifles, to stationary systems with specialized weaponry.

1. Joint Air Power Competence Centre (JAPCC), *A Comprehensive Approach to Countering Unmanned Aircraft Systems*, Kalkar, JAPCC, 2021, <https://www.japcc.org/books/a-comprehensive-approach-to-countering-unmanned-aircraft-systems>, (accessed 7 November 2023).
2. North Atlantic Treaty Organization (NATO), *NATO Term – The official NATO Terminology Database*, [website], n.d., <https://nso.nato.int/natoterm/Web.mvc>, (accessed 7 November 2023).
3. NATO, Allied Tactical Publication (ATP) 3.3.8.1, *Minimum Training Requirements for Unmanned Aircraft Systems (UAS) Operators and Pilots*, Edition B, Version 1, 2019.
4. NATO defines Counter-UAS as 'a counter-air operation conducted to prevent mission accomplishment of an enemy unmanned aircraft system, which could include attacking the aircraft itself, its data links, or the control station', *Ibid.* 2.
5. *Ibid.* 3, p. 2-2.



© DeawSS/Shutterstock.com

Chapter 2

Drone Threats – An Overview

Drones and UAS have become increasingly popular in recent years for military operations and various private and commercial uses, such as delivery, aerial photography, drone racing contests, etc.¹ Their common availability and, thus, widespread proliferation entail potential threats associated with the use of drones, including:

Privacy and Security Violations. Drones equipped with cameras can be used to spy on individuals and organizations without their knowledge or consent.

Physical Hazards. Drones can pose a risk to infrastructure, material and personnel on the ground if they – intentionally or accidentally – collide or malfunction.

Weaponization. Drones can be outfitted with weapons or explosives and used to attack infrastructure, material, and personnel.

Cybersecurity. Drones equipped with wireless communication capabilities or the ability to deliver portable hacking equipment can be used to hack into and compromise the confidentiality, integrity, or availability of Wi-Fi networks.

None of the potential drone abuses mentioned above require sophisticated knowledge or advanced piloting and engineering skills. Controlling drones has become nearly effortless thanks to the introduction of hobbyist-friendly cell phone or tablet computer applications that make flying a drone as simple as pointing and clicking on a digital map.² Blueprints and instructions for building a custom drone,³ disabling geo-fencing restrictions,⁴ or converting an off-the-shelf product into a hazardous device are readily available and can be found with a simple Google search.

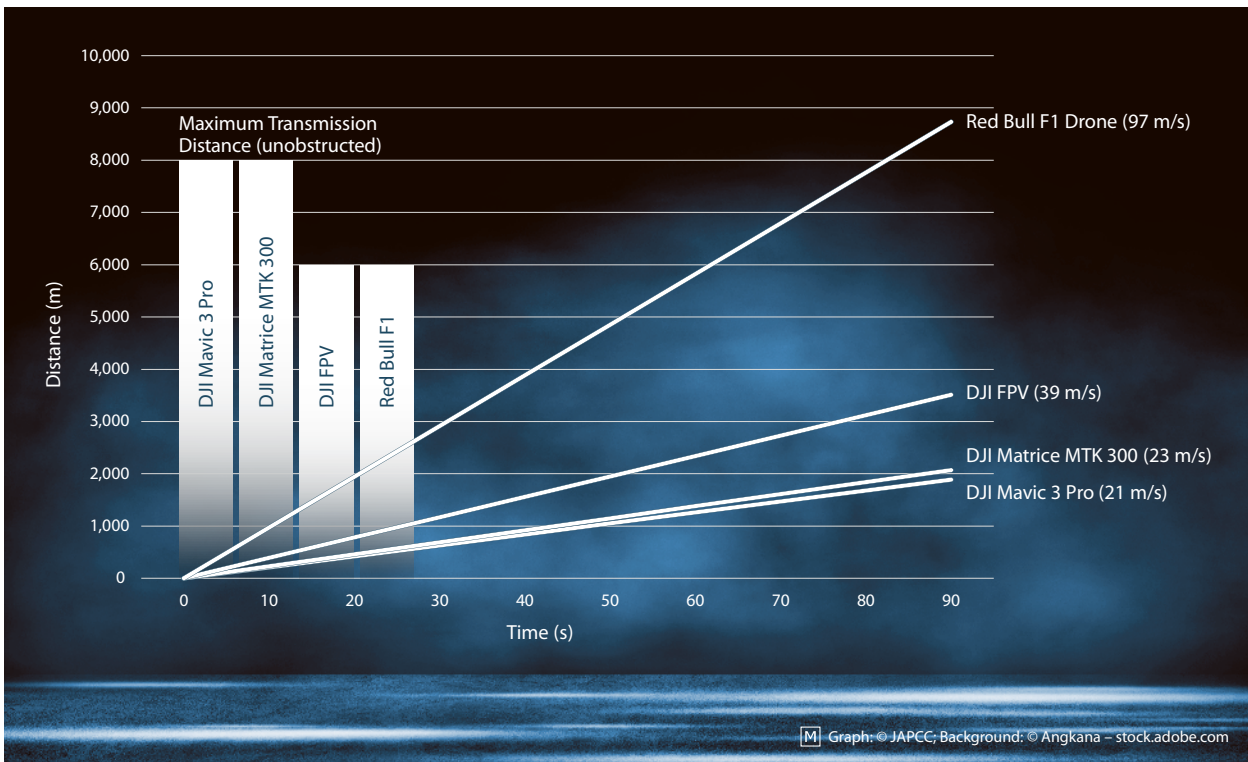


Figure 4: Drones are fast, leaving little reaction time for countermeasures when an unauthorized drone is detected.

NATO categorizes threats as Terrorism, Espionage, Sabotage, and Subversion (TESS), and drones can be used in all of these threat cases. Following this structure, the following sections briefly describe the potential dangers of drone misuse and provide examples of recent drone-related incidents.

2.1 Terrorism

Terrorism is the *'unlawful use or threatened use of force or violence, instilling fear and terror against individuals or property in an attempt to coerce or intimidate governments or societies or gain control over a population to achieve political, religious, or ideological objectives.'*⁵

In this context, drones can deliver explosives and other hazardous materials into traditionally protected areas due to their ability to fly over or bypass physical security measures. Due to their ability to carry dangerous payloads, drones are a potent tool for malicious actors

and can pose a significant threat to public safety and military security.

In several instances, drones operated close to or inside protected areas, including critical infrastructure, sports venues, and political event locations.

Germany. In 2013, a small quadcopter appeared before the German Chancellor and the defence minister during a public campaign rally. It hovered in front of the leaders before crashing into the stage and landing at the Chancellor's feet when the operator was forced to do a quick landing.⁶ Had the drone been equipped with even a small explosive, a detonation in front of the two politicians would have been fatal. For many, this event first exposed the severe security issues of small drones and sparked the initial ideas and concepts for countering them.

Japan. In 2015, a drone carrying a camera and a bottle of unidentified liquid that bore a sticker with the

universal symbol for radioactivity was found on the roof of the Japanese Prime Minister's official residence in Tokyo. Traces of radioactivity were detected on the roof near the drone and prompted concern about whether the drone might have been part of a terrorist attack. There was also speculation that it could have been a protest related to the Fukushima accident. The discovery prompted the government to review its antiterrorism measures as Japan prepared for the 2020 Olympic Games in Tokyo.⁷

France. In 2018, Greenpeace intentionally crashed a drone into a French nuclear power plant to reveal its security vulnerability. Though the drone was harmless, the activists stated that this action proved that the airspace around nuclear power plants is easily accessible and highly exposed to outside attacks.⁸

United States. In 2022, the US Federal Bureau of Investigations (FBI) stated in a Senate Homeland Security Committee hearing on domestic threats that they were investigating several cases in which people sought to fly drones equipped with homemade bombs within the United States.⁹

It should be noted here that due to repeated and widely reported drone incidents, the general population may already be alarmed when a drone hovers above them, even if it is unarmed. According to the definition of terrorism, this pattern may be abused to spread fear and panic or cause anxiety among the population.

2.2 Espionage

Espionage is an *'activity directed towards the acquisition of information through clandestine means and forbidden by the law of the country against which it is committed.'*¹⁰ Another definition describes espionage as the *'process of obtaining military, political, commercial, or other classified information by means of spies, secret agents, or illegal monitoring devices.'*¹¹

In either case, drones with cameras or other sensing devices can illegally monitor activities in restricted areas, such as government facilities, critical infrastructure, or

military installations. This includes infrared and multi-spectral sensing in addition to ordinary electro-optical imagery.¹²

Drones can also be used as delivery mechanisms to hack into wireless networks. A drone could deliver a smartphone or other portable device onto the roof of a target building. The attacker could remotely control the device using the local cellular service and the device's built-in Wi-Fi equipment to compromise the wireless network. This method allows the attacker to penetrate the network and exfiltrate data surreptitiously.^{13,14}

In a broader context, drones can also capture images or footage of private individuals, homes, or businesses without consent. Collecting information about the movements, behaviour, and private lives of high-profile individuals, such as military or business leaders, may also raise security concerns, such as planning a more conventional attack, or capturing compromising information.

The internet is littered with reported incidents where drones were used – or at least suspected of being used – to collect information illegally. Here are some most recent examples:

Germany. In 2022, the German Ministry of Defence experienced frequent overhead drone flights, including at night. Drones were also seen flying over areas where the German Army had conducted training exercises for Ukrainian soldiers. A German magazine reported 'indications' that Russian intelligence services tried to spy on the Ukrainian soldiers receiving the training, though no official source could confirm this.¹⁵

United States. In 2022, federal officials and drone industry experts reportedly delivered classified briefings to the Senate's Homeland Security, Commerce, and Intelligence committees on hundreds of drone intrusions over the White House, Capitol, and Pentagon.¹⁶ While these incidents may have just been innocent data collection or curiosity, they demonstrated that malicious actors could readily obtain information about the organization and operation of a government facility.



[M] Drone: © Adobe; Sky: ParinPIX – stock.adobe.com;
Text Classified: theerakit – stock.adobe.com

2.3 Sabotage

Sabotage acts intend *‘to injure, interfere with, or cause physical damage to assist an adversary or to further a subversive political objective.’*¹⁷ Unlike terrorism, the objective of sabotage is often to disrupt operations or production rather than to spread fear and terror among the general population.

In this context, similar to terrorist threats, drones can drop and detonate explosives on critical infrastructure and equipment, causing significant damage and disruption. The key difference is that the primary target will likely be material and property, not personnel.

As described in the last section, drones equipped with hacking tools can do far more than exfiltrate data once they have compromised a target network. They can also inject malicious code, destroy data, or disrupt communication systems, compromising the ability to carry out regular military, industrial, or commercial operations at a critical time for the victim.

Drones can also fly into or over restricted airspace and areas, causing a disturbance or even disruptions of military, industrial, or commercial operations. These

adverse effects may include, for example, temporary shutdowns, activation of emergency protocols, or deployment of security personnel to investigate the threat.

Some examples of recent sabotage or suspected sabotage attempts are listed below.

United Kingdom. In recent years, drones have disrupted airport operations by flying into restricted airspace and interfering with air traffic and runway operations. In December 2018, London’s Gatwick Airport was forced to shut down for several days due to multiple drone sightings, causing widespread flight cancellations and delays.¹⁸

Saudi Arabia. In 2019, drones attacked two major oil refineries in Saudi Arabia, causing significant damage and temporarily disrupting oil production of almost 5.7 million barrels a day, about 5 percent of the world’s daily oil production at that time. Though Yemen’s Houthi rebels claimed the attack, the United States accused Iran of an ‘unprecedented attack on the world’s energy supply.’¹⁹ After this well-known incident, several other drone attacks occurred on Saudi Arabian oil facilities in the following years.²⁰

United States. In 2020, a drone approached a power substation carrying a thick copper wire beneath it to potentially disrupt operations by creating a short circuit. However, the drone crashed before it could reach its target. According to a joint security bulletin released by the Department of Homeland Security, the Federal Bureau of Investigation, and the National Counterterrorism Center, this incident constituted the first known instance of a modified drone being used to target US energy infrastructure.²¹

2.4 Subversion

Subversion consists of *'action or a coordinated set of actions of any nature intended to weaken the military, economic or political strength of an established authority by undermining the morale, loyalty, or reliability of its members.'*²²

In this context, drones can decrease military and civilian personnel's enthusiasm, spirit, and morale to serve and carry out their duties. This can be achieved by conducting regular drone attacks or simply the recurring presence of drones overhead, creating a feeling of vulnerability and fear among the affected personnel. Constant disruption of military, industrial, and commercial operations by drones can lead to growing frustration and undermine morale and confidence in the military or civilian chain of command and the effectiveness of security measures in place. This can result in decreased efficiency, effectiveness, and cohesiveness among personnel, potentially impacting the success of military operations or business revenues.

The most recent example of an attempt to undermine the morale of a population through drone strikes is Russia's use of Class II UAS (*cf. Table 1, p. 7*) against Ukraine's civilian infrastructure, particularly its power supply. By disrupting the power grid and other essential services, Russia attempts to force the population into a difficult decision to either stay in the country despite the harsh conditions inflicted by Russian actions or flee or surrender, thereby creating feelings of helplessness and breaking the morale of the Ukrainian population.²³

1. The global drone market is anticipated to grow from 26.3 billion US dollars in 2021 to 41.3 billion US dollars by 2026. Drone Industry Insights, 'Drone Market Analysis 2022–2030', [website], 7 September 2022, <https://droneii.com/project/drone-market-analysis-2022-2030-infographic>, (accessed 13 November 2023).
2. The Google Play Store lists multiple applications for 'Drone Remote Control' that enable mobile phones to remotely control different types of commercial drone models. Google, 'Google Play', [website], 2023, <https://play.google.com/store/search?q=Drone%20Remote%20Control&c=apps>, (accessed 13 November 2023).
3. Drone Nodes, 'How to Build a Drone – Step by Step Guide', [website], 14 October 2023, <https://dronenodes.com/how-to-build-a-drone>, (accessed 13 November 2023).
4. UAV Coach, 'How to Unlock DJI Geofencing and Warning Zones in 2023', [online video], 21 June 2023, https://www.youtube.com/watch?v=U_pGbc9xWdw, (accessed 13 November 2023).
5. North Atlantic Treaty Organization (NATO), 'NATO Term – The official NATO Terminology Database', [website], n.d., <https://nso.nato.int/natoterm/Web.mvc>, (accessed 7 November 2023).
6. Friederike Heine, 'Merkel Buzzed by Mini-Drone at Campaign Event', Spiegel International, 16 September 2013, <https://www.spiegel.de/international/germany/merkel-campaign-event-visited-by-mini-drone-a-922495.html>, (accessed 13 November 2023).
7. Martin Fackler, 'Drone, Possibly Radioactive, Is Found at Office of Japan's Prime Minister', The New York Times, 22 April 2015, <https://www.nytimes.com/2015/04/23/world/asia/drone-possibly-radioactive-is-found-at-office-of-japans-prime-minister.html>, (accessed 13 November 2023).
8. Anastasia Gliadkovskaya, 'Greenpeace activists pilot and crash drone into French nuclear plant's no-fly zone', Euronews, 3 July 2018, <https://www.euronews.com/2018/07/03/greenpeace-activists-pilot-and-crash-drone-into-french-nuclear-plant-s-no-fly-zone>, (accessed 13 November 2023).
9. Christopher Wray, Director Federal Bureau of Investigations 'Senate Homeland Security Hearing on National Security Threats', C-SPAN, [online video], 17 November 2022, 00:46:53–00:47:31, <https://www.c-span.org/video/?524139-1/senate-homeland-security-hearing-national-security-threats>, (accessed 13 November 2023).
10. Ibid. 5.
11. 'Espionage', Britannica, [website], 23 October 2023, <https://www.britannica.com/topic/espionage>, (accessed 13 November 2023).
12. DJI, 'P4 Multispectral – Plant Intelligence for Targeted Action', [website], n.d., <https://www.dji.com/p4-multispectral>, (accessed 13 November 2023).
13. Cal Jeffrey, 'Wi-Fi drones were used by hackers to penetrate a financial firm's network remotely', TechSpot, 14 October 2022, <https://www.techspot.com/news/96321-drones-helped-hackers-penetrate-financial-firm-network-remotely.html>, (accessed 13 November 2023).
14. Sai Ram, 'Drones for Wi-Fi Hacking? A new attack vector? What next?', [online blog], 16 October 2022, <https://www.linkedin.com/pulse/drones-wi-fi-hacking-new-attack-vector-what-next-sai-ram>, (accessed 13 November 2023).
15. Jörg Diehl and Matthias Gebauer, 'Verteidigungsministerium soll gegen verdächtige Drohnenflüge geschützt werden', Der Spiegel, 4 November 2022, <https://www.spiegel.de/politik/deutschland/bundeswehr-verteidigungsministerium-soll-gegen-verdaechtige-drohnenfluegen-geschuetzt-werden-a-6a562796-b009-4c1f-ad42-fca6f3cc753d>, (accessed 13 November 2023).
16. Bryan Bender and Andrew Desiderio, 'Senators alarmed over potential Chinese drone spy threat', Politico, 23 November 2022, <https://www.politico.com/news/2022/11/23/drones-chinese-spy-threat-senate-00070591>, (accessed 13 November 2023).
17. Ibid. 5.
18. Samantha Masunaga, 'Gatwick Airport incident shows the threat of rogue drones in commercial airspace', Los Angeles Times, 20 December 2018, <https://www.latimes.com/business/la-fi-gatwick-drones-20181220-story.html>, (accessed 13 November 2023).
19. Ben Hubbard, Palko Karasz, and Stanley Reed, 'Two Major Saudi Oil Installations Hit by Drone Strike, and U.S. Blames Iran', The New York Times, 14 September 2019, <https://www.nytimes.com/2019/09/14/world/middleeast/saudi-arabia-refineries-drone-attack.html>, (accessed 13 November 2023).
20. Ben Hubbard, 'Yemeni Rebel Attack Sets Saudi Oil Facility Ablaze', The New York Times, 25 March 2022, <https://www.nytimes.com/2022/03/25/world/middleeast/yemen-attack-saudi-arabia.html>, (accessed 13 November 2023).
21. Sean Lyngaas, 'Drone at Pennsylvania electric substation was first to "specifically target energy infrastructure", according to federal law enforcement bulletin', CNN, 4 November 2021, <https://edition.cnn.com/2021/11/04/politics/drone-pennsylvania-electric-substation/index.html>, (accessed 13 November 2023).
22. Ibid. 5.
23. Michael N. Schmitt, 'Ukraine Symposium – Attacking Power Infrastructure Under International Humanitarian Law', Lieber Institute West Point, 20 October 2022, <https://lieber.westpoint.edu/attacking-power-infrastructure-under-international-humanitarian-law>, (accessed 13 November 2023).



© Lukas Gojda/Shutterstock.com

Chapter 3

Drone Imaging

Typically, any consumer drone comes with at least one camera for aerial photography and video. In recent years, high-quality models have become quite affordable, compact, and versatile, allowing drones to capture stunning aerial footage and images that were once impossible for non-professionals and hobbyists.

3.1 Relevant Technical Specifications

The quality of a camera is mainly defined by the number of megapixels, the quality of the lens and its focal length. Other specifications, usually considered by professionals, such as the digital sensor size and sensitivity, the shutter speed of the camera and more, are

not addressed in this paper because they are beyond the scope of our discussion.

3.1.1 Megapixels

The number of megapixels refers to the resolution of the camera sensor and determines the level of detail it can capture in an image. Generally, a higher megapixel count results in larger images and more detail. The average consumer drone with a price tag under 500 Euros typically provides high-definition video and imagery with 12 to 20 megapixels resolution. More expensive models offer resolutions of up to 48 megapixels and higher.

3.1.2 Focal Length

The focal length determines the camera's angle of view and zoom capabilities. Like mobile phones, consumer drone cameras typically have wide-angle lenses

with a focal length between 20 mm and 35 mm, which is essential for situational awareness and wide-area aerial photography. However, semi-professional drones starting at around 2,000 Euros come with longer focal lengths going up to 160 mm and more, allowing for closer shots of distant objects. Dedicated professional drone cameras provide even longer focal lengths of up to 1,200 mm, which comes at around 5,000 to 12,000 Euros for the camera alone.

Table 2 overviews commonly available drone models and their camera specifications, ranging from entry-level to professional drones.

3.2 Sensor Capabilities

To illustrate the imaging capabilities of consumer drones under optimal conditions, the images on the right page were taken with a professional photo camera configured according to the respective drones' maximum focal length and number of megapixels.

The test image (cf. Figure 5) is a 7.5 cm x 7.5 cm square with text in 12-point Arial font, which is a common

standard for business and military documents. The photos were taken from 2, 4, and 6 metres away to reflect the estimated distances of a drone hovering outside a window and shooting into the room (cf. Figures 5–10).

3.2.1 Entry-Level Drones

Cheap drone models start below 100 Euros and are usually aimed at a young customer audience or as entry-level gadgets for the drone flying hobby. These drones are generally very limited in their capabilities and come with a very basic camera, typically without optical zoom, which is even inferior to what a mobile phone camera would offer (cf. Figure 8). Figure 6 shows that cheap drone models hardly capture details, even from short distances.

3.2.2 Consumer and Hobbyist Drones

Drones starting at around 500 Euros typically include better cameras than their entry-level counterparts. Often, these cameras provide higher focal lengths and at least a double optical zoom, allowing them to depict more detail. These specifications are comparable

	Ryze Tech Tello	DJI Mavic 2 Zoom	DJI Mavic 3	DJI Zenmuse H20
Megapixel	5 MP	12 MP	12 MP	20 MP
Resolution	2,592 x 1,936	4,000 x 3,000	4,000 x 3,000	5,184 x 3,888
Focal Length	24 mm	48 mm	162 mm	556 mm
Price	120 €	850 €	2,000 €	4,650 €
Drone Weight	80 g	905 g	958 g	~7,200 g
Drone Size (l/w)	~10 x 9 cm	~32 x 24 cm	~35 x 29 cm	~81 x 67 cm
Max. Flight Time	13 min.	30 min.	43 min.	55 min.

Table 2: Commercial drone models and their technical specifications.^{1,2,3,4}

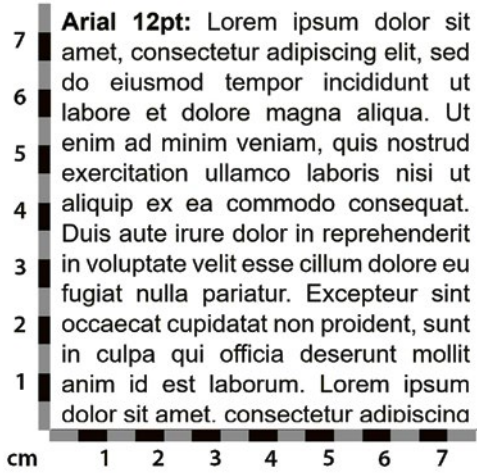


Figure 5: Original Image with 12 pt Arial Font.

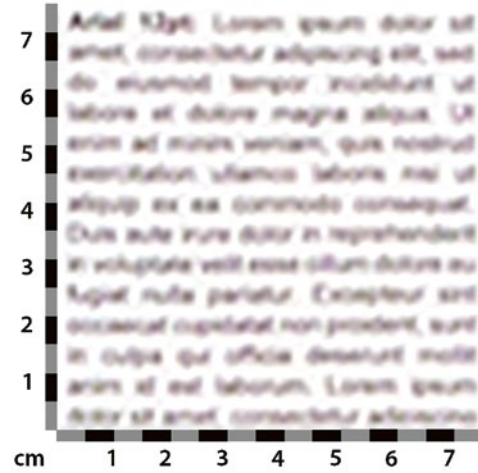


Figure 6: Image Taken with the Ryze Tech Tello Specifications from a Distance of 2 m.

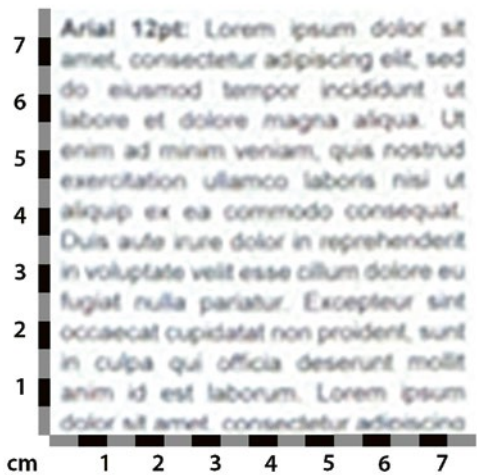


Figure 7: Image Taken with the DJI Mavic 2 Zoom Specifications from a Distance of 4 m.



Figure 8: Image Taken with an iPhone 12 Pro with Double Optical Zoom at a Distance of 2 m.

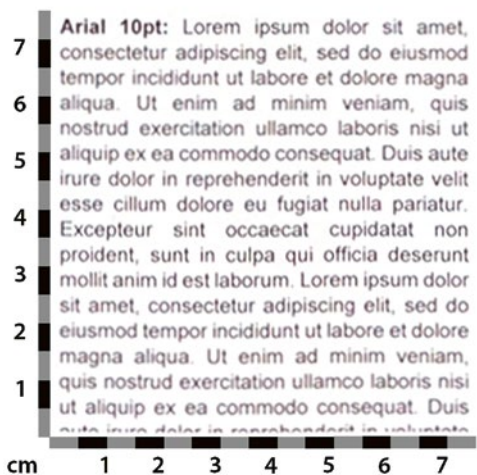


Figure 9: Image Taken with the DJI Mavic 3 Specifications from a Distance of 6 m.

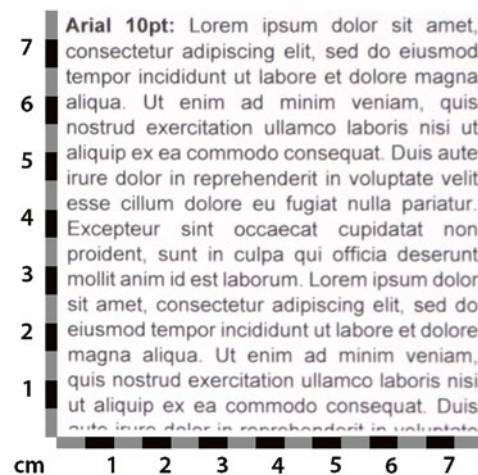


Figure 10: Image Taken with the DJI Zenmuse H20 Specifications with 400 mm Focal Length from a Distance of 6 m.

to a modern mobile phone's camera. *Figure 7* and *Figure 8* on the previous page illustrate the level of detail a double optical zoom would provide, though, at distances of more than four metres, details become blurred and difficult to read.

3.2.3 Semi-Professional Drones

Affordable for dedicated hobbyists and small businesses, semi-professional drones offer excellent imaging capabilities that can compete with traditional photo cameras at a comparable price range. With significantly longer focal lengths and multiple times the zoom of the drones discussed earlier, *Figure 9* and *Figure 10* were taken from a greater distance and with a smaller 10-point font to illustrate the leap in imaging capabilities of drone models starting at about 2,000 Euros.

3.3 Sensor Limitations

Several limiting factors affect the quality of drone imagery, including the drone's movement, adverse lighting conditions, and window reflections.

3.3.1 Drone Movement

As drones move, they experience vibration, which leads to blurry images if not technically compensated. Hence, most drone cameras have built-in stabilization features that can help mitigate this issue. However, the drone must still hover mid-air with as much stability as possible and avoid movement for best results.

3.3.2 Adverse Lighting Conditions

Lighting may be either too low or too bright. In low light conditions, the sensor's ability to capture light is reduced, leading to increased noise, graininess, reduced sharpness, and, eventually, loss of detail in the image. Conversely, too bright light creates strong contrasts and can cause overexposure in parts of the image that are directly hit by, for example, the sun. Stark contrast results in a loss of image detail, whereas the overexposed parts appear plain white.

3.3.3 Window Reflections

Window reflections are caused by various factors, including bright sunlight, the properties of the glass itself, and the camera's angle. Entry-level and cheaper consumer drones typically use an autofocus mechanism that can be distracted by the reflections and then focus on the glass rather than the objects behind it. Professional cameras can compensate for reflections by using a polarizing filter or manual focusing, though this requires some experience on the operator's part and may be challenging for hobbyists.

3.4 Assessment

Drones in even the cheapest price ranges can capture high-definition imagery and identify objects and persons at considerable distances, though the level of detail differs greatly. As a rule of thumb, the larger a drone, the better its potential imaging capabilities (*cf. Figure 11*). Larger drones hovering a couple of metres in front of a window can be expected to capture enough detail so that documents and computer screens inside the respective room can be read. Larger fonts, such as those typically used for presentation slides and diagrams, as well as for headlines and notes on whiteboards, are even more susceptible to drone imagery.

3.5 Mitigation Options

Mitigating exposure to drone cameras does not require a large investment; in fact, a high level of mitigation can already be achieved with simple and easy-to-implement action plans and little organizational changes, which can optionally be accompanied by some low-budget purchases for even better protection.

3.5.1 Immediate Measures

Any initial action should immediately eliminate the drone's ability to capture footage and images of the targeted workplace. Some recommended measures that can be taken easily and swiftly are listed on the next page.

3.5.1.1 Lock Your Computer Screen. All common desktop computer operating systems, such as Microsoft Windows, Apple iOS, or all Unix-based systems, offer the possibility to lock the computer and screen. This function is usually bound to a specific combination of keys that need to be pressed simultaneously, and all users should know the combination for their respective systems by heart. After detecting a drone, the first action should be to lock the computer immediately and deny access to the screen content.

3.5.1.2 Lower and Close Curtains and Shutters. Most offices have curtains or shutters to prevent sunlight reflections on computer screens and protect the room from heat. In addition, closed curtains or shutters perfectly deny outside observation. If both are fitted, the curtains should be shut, or the shutters should be lowered and closed, whichever is faster. It should be noted that a drone may pose additional hazards, such as an explosive charge, so it is strongly recommended to leave the room as fast as possible and not spend excessive time closing the shutters (*cf. Chapter 4.4.1 f.*).

3.5.1.3 Cover Whiteboards, Flip Charts, and Documents. If curtains or blinds are not fitted, it is suggested

to cover, for example, whiteboards, flip charts, and documents, which are in the window's line of sight, depending on available time and threat level. As mentioned above, a drone may be equipped with an explosive charge, so it is strongly recommended to leave the room as fast as possible and not spend excessive time covering visible information (*cf. Chapter 4.4.1 f.*).

3.5.2 Preparatory Measures

Properly prepared safety measures can significantly minimize the time required or even eliminate the need for the immediate actions described above, thus saving critical time for a rapid evacuation.

3.5.2.1 Computer Screens and Keyboards. The workplaces inside an office should be arranged so that computer screens and keyboards are tilted away from direct lines of sight and face away from the window. If such a setup is not feasible for a workplace, screens can be fitted with privacy screen filters for a small investment, between 20 and 50 Euros each, depending on the screen size.

3.5.2.2 Whiteboards are usually attached to the wall, and so inevitably face the window in most cases.



Figure 11: Different Sizes of DJI Drone Models. From left to right: DJI Mini 2, Mavic Air 2, Mavic 2 Pro, Mavic 3.



Figure 12: Avoiding the Line of Sight between Window and Screens.

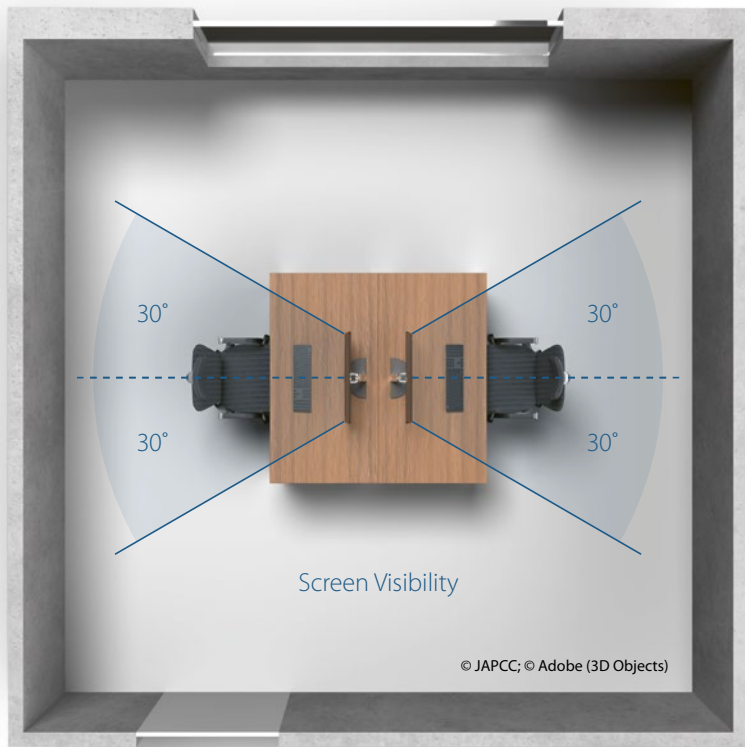


Figure 13: Limiting Viewing Angle to 30° Relative to the Main Axis with Privacy Screen Filter Applied.

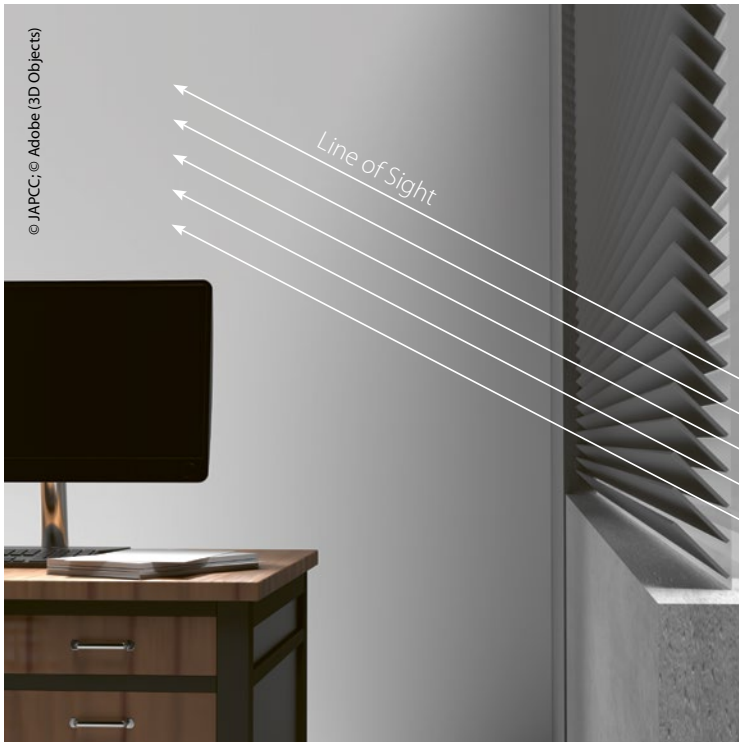


Figure 14: Window Shades Forcing an Upwards Viewing Angle.

It should be best practice to only note unclassified and non-proprietary information on a whiteboard and always clean it after meetings. If information needs to stay on the whiteboard regularly, applying a cover should be considered when the board is not in use. Such a cover can be self-made from cardboard, a company wall poster, fabric, or other makeshift materials. Professional solutions can be purchased starting at around 250 Euros.

3.5.2.3 Flipcharts. Like computer screens, flipcharts should not face the window. However, if this is not feasible and information is kept on the flipchart, it is recommended to leave the first/top page blank and fold it back over the others after the meeting to cover all those below it.

3.5.2.4 Documents. When not being used, documents should be kept away in drawers, folders, or at least covered with a blank top page, cardboard, or similar, if piled on the desk, to protect the information on them. Rules for handling classified and proprietary

documents are usually in place, so adhering to them should provide sufficient mitigation against drone imagery. A clean desk policy is always a good practice (i.e., to clean up the desk after business hours and not leave any documents in plain sight).

3.5.2.5 Window Blinds. For ergonomic reasons, many offices already have blinds or shades with horizontal slats fitted to reduce sunlight reflections on computer screens while keeping the heat out. Fully lowered blinds provide excellent protection from drone images, as they completely obstruct the view from the outside.

Even if not fully closed but properly adjusted, they provide solid protection from drone images by forcing an upward viewing angle that blocks the line of sight to anything below the height of the window-sill. Inexpensive models start at 15 to 20 euros and should be considered a worthwhile investment.

3.5.2.6 Reflective, Mirror, and Glazing Films. Though the main application of these films is sun protection, they work very well as privacy films during the day since they reflect light and act like a mirror. However, it is essential to note that this visual effect is not present when it is dark outside with the office lights on. It should also be considered that equipping only individual areas with these films could visually indicate specially protected areas and draw unwanted attention to the ones so equipped.

1. RyzeTech, 'Tello Specs' [website], n.d., <https://www.ryzerobotics.com/tello/specs>, (accessed 13 November 2023).
2. DJI, 'Mavic 2 Specs' [website], n.d., <https://www.dji.com/mavic-2/info#specs>, (accessed 13 November 2023).
3. DJI, 'DJI Mavic 3 Specs' [website], n.d., <https://www.dji.com/mavic-3/specs>, (accessed 13 November 2023).
4. DJI, 'Zenmuse H20 Series' [website], n.d., <https://enterprise.dji.com/zenmuse-h20-series/specs>, (accessed 13 November 2023).



© Zysko Sergii/Shutterstock.com

Chapter 4

Delivery of Explosives and Other Hazardous Materials

Drones can deliver explosives and other hazardous materials into traditionally protected areas due to their ability to fly over or bypass physical security measures.

4.1 Airborne Improvised Explosive Devices

Drones can be used as an airborne delivery means for an explosive payload.¹ Depending on their take-off capacity, the explosive yield that can be transported can range from a few grams to multiple kilograms with larger models. In this context, it should be noted that explosives can also be stored inside the drone, for example, in parts of the battery compartment, and are not necessarily apparent as a regular, externally mounted payload. Therefore, any drone

intrusion should be treated with extreme caution, and the possibility that an explosive charge has been attached or hidden inside should always be considered with any action taken.

4.1.1 Relevant Factors

The effect of a detonating explosive charge depends on several factors, such as the type of explosives used, the explosive yield, the distance of the target from the point of detonation, as well as the type and durability of the target.

4.1.1.1 Types of Explosives. Various reliable and tested explosives are used in civilian and military applications. In addition, Homemade Explosives (HMEs) are improvised mixtures made by individuals without adherence to safety standards or regulatory requirements. Homemade explosives typically lack the stability, reliability, and predictable performance of military explosives, making them inherently unsafe to handle. For this paper, Trinitrotoluene, more commonly known as TNT,

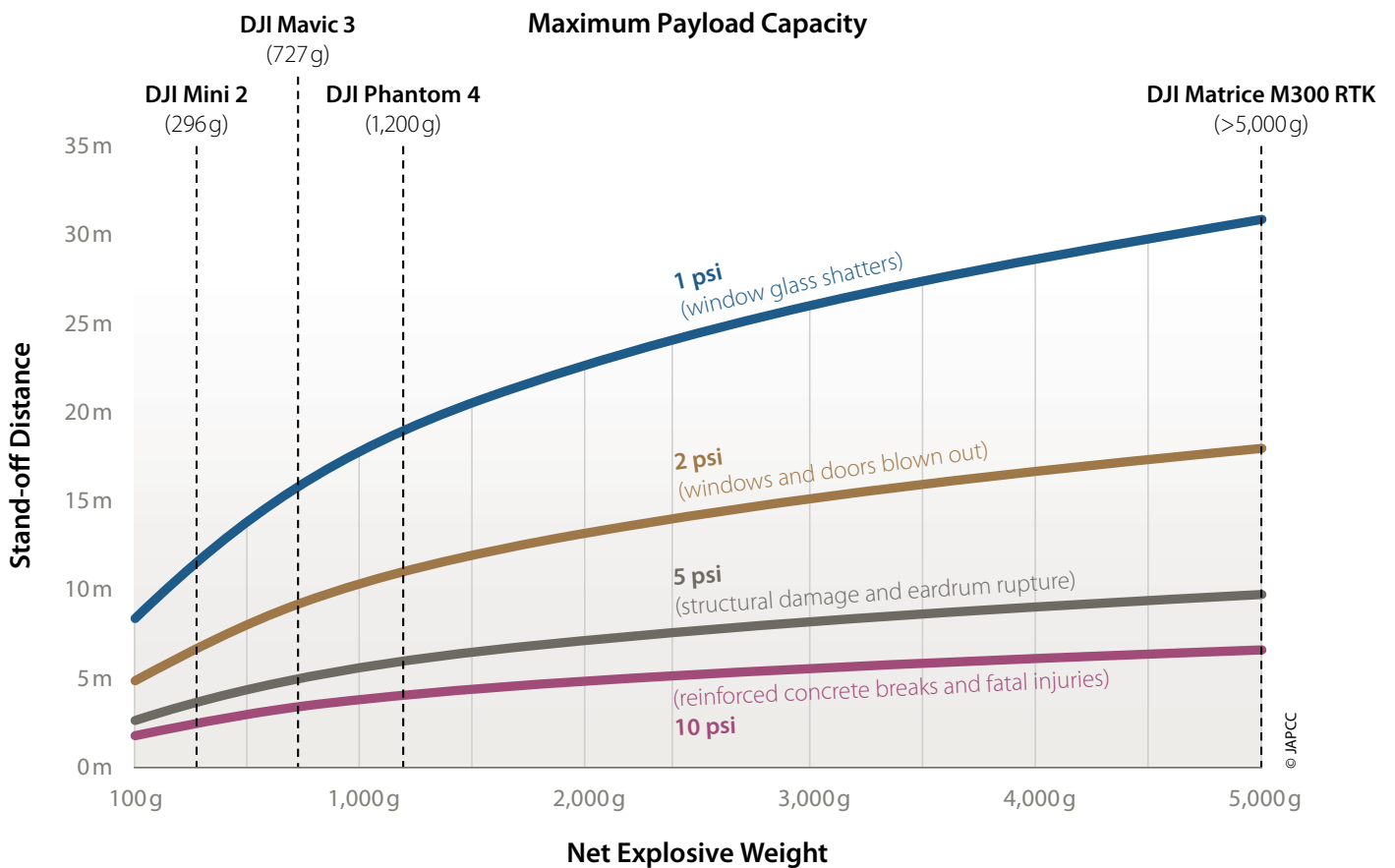


Figure 15: Incident overpressure measured in pounds per square inch (psi), as a function of stand-off distance and net explosive weight of TNT in relation to potential drone payload capabilities.^{2,3} Depicted maximum payload capacities are based on actual weightlifting tests and exceed the official drone models' specifications.^{4,5,6,7}

is used as the standard explosive for calculating blast effects and safety distances, as its detonation velocity is a good baseline for most cases discussed and includes a safety buffer since drones with HMEs could be expected to be less effective than if they were fitted with TNT.

4.1.1.2 Explosive Mass and Distance to the Point of Detonation. In addition to the type, the quantity of explosives used determines the magnitude of the detonation. The resulting pressure wave causes an immediate spike in air overpressure, which affects buildings, windows, and the human body. This excessive air pressure decreases exponentially with distance from the explosion's centre, i.e., at twice the distance from the detonation, the air pressure already drops to a quarter of its original value, meaning that stand-off by itself is an essential safeguard against blast.

4.1.1.3 Type and Durability of the Target. The weakest target that can be exposed to the blast wave of a detonation is the human body itself. Depending on the intensity of the blast, severe injuries such as

ruptured eardrums and lungs, collapsed lungs, organ perforations, traumatic brain injury, or internal bleeding may occur. The weakest points in physical infrastructures are the windows and other glass elements since, due to the very nature of their material, they are far more susceptible to a sudden blast wave than the walls surrounding them.

4.1.2 Effects Originating from Blast

The type of casing used for the explosive charge, any shrapnel load additions, and possible containment of the charge to provide a directional effect can significantly increase the impact of the detonation. However, for easier comprehension, this paper limits itself to examining only the results of blast and air overpressure, as the additional factors mentioned above would involve too many variables, some unpredictable and well beyond the scope of this discussion. Nevertheless, the effects of the blast alone are sufficient to formulate general guidelines for protecting human lives and health in the event of a drone incident.

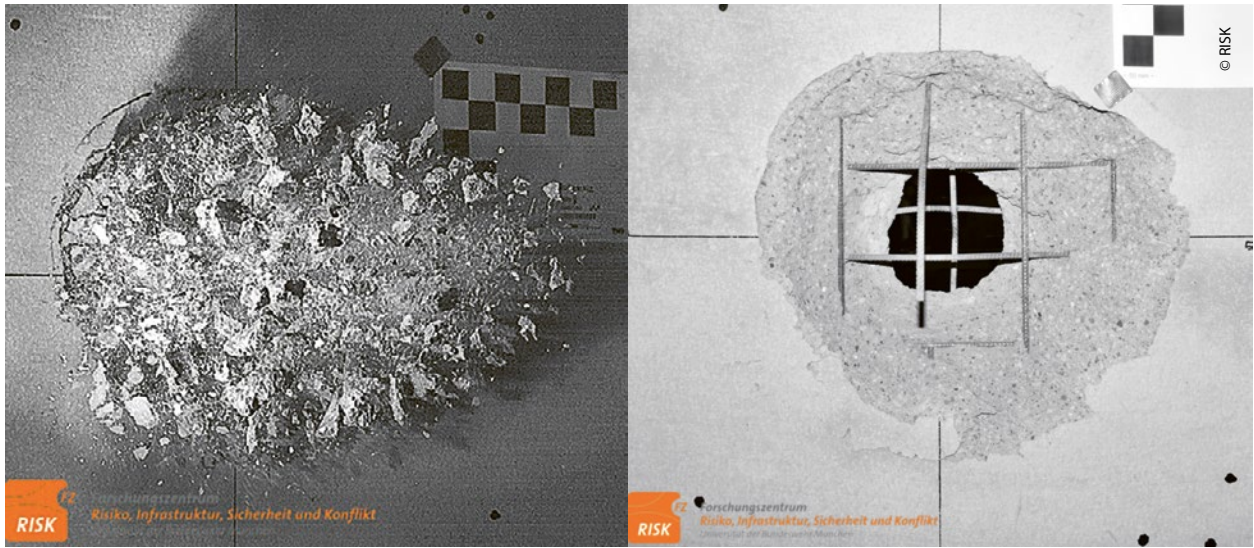






Figure 16: Contact Detonation of 1,000 g SEMTEX10 against 20 cm Reinforced Concrete. Fragment Velocity up to 70 Metres per Second (m/s).⁸

Table 3: Recommended Safety Distances from Explosions.¹⁵

				
THREAT DESCRIPTION	Small Package/ Letter	Pipe Bomb	FedEx Package	Vest/ Container Bombs
EXPLOSIVE CAPACITY	1 lb	5 lb	10 lb	20 lb
BUILDING EVACUATION DISTANCE	40 ft	70 ft	90 ft	110 ft
OUTDOOR EVACUATION DISTANCE	900 ft	1,200 ft	1,080 ft	1,700 ft






4.1.2.1 Walls. The brick or concrete walls of an office building offer decent protection against blast and fragmentation; however, small amounts of explosives can also damage solid walls at close range, with debris being propelled into the room, which can seriously injure any persons inside it. Figure 15 shows the explosive mass and minimal distance required to damage buildings and structures.^{2,3} Additionally, Figure 16 illustrates the effects of a small explosive yield against a reinforced concrete wall.⁸

4.1.2.2 Windows. Standard office windows typically consist of two or three layers of glass with air between them to provide insulation. Protected areas usually have more sturdy windows installed that include at least one outer layer of security glass, which sandwiches a strong rip-proof foil between two or more layers of

glass. However, this window type only aims to delay the time necessary to break them, such as from blunt force. However, they are not immune to breakage or designed to withstand blast. Blast-resistant and bullet-proof windows are usually only installed in highly sensitive areas, for example, guard buildings, but rarely in regular office buildings. Figure 15 illustrates the minimum distance from the point of detonation and the explosive mass required to shatter glass.^{9,10} Single pane annealed glass windows will likely break at less than 1 pound per square inch (psi) air overpressure,¹¹ though it should be noted that tempered and laminated glass windows have a 4–5 times higher resistance.¹²

4.1.2.3 Human Body. The human lungs and inner ear function is adapted to an average atmospheric pressure of 1 bar. Sudden strong changes in atmospheric

[M] Concept of Table: © JAPCC; 3D Objects, from left to right – 1–5: © Adobe; 6–7: © 'Generic passenger car pack' (<https://skfb.ly/6sUFy>) by Comrade1280 is licensed under Creative Commons Attribution (<http://creativecommons.org/licenses/by/4.0/>); 8: © adobestock3d – stock.adobe.com; 9: © 'UN Truck 1' (<https://skfb.ly/oKtNM>) by RGB is licensed under Creative Commons Attribution-NonCommercial (<http://creativecommons.org/licenses/by-nc/4.0/>). Source data extracted from US Department of Homeland Security, *1ED Attack – Improvised Explosive Devices*, 2009.¹⁵

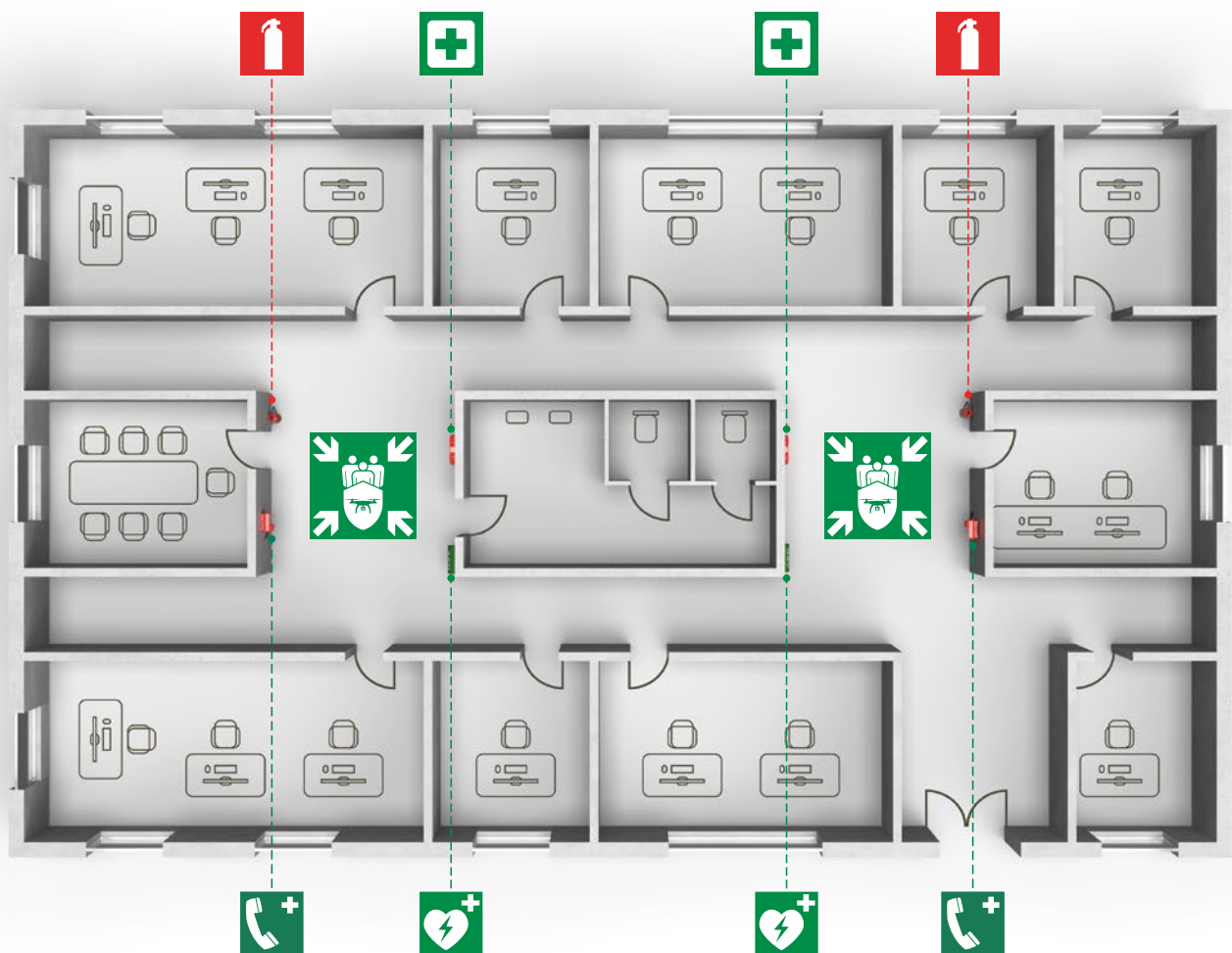
				
Parcel Package	Compact Car	Full-Size Car/Minivan	Van/SUV/Pickup Truck	Delivery Truck
50 lb	500 lb	1,000 lb	4,000 lb	10,000 lb
150 ft	320 ft	400 ft	640 ft	860 ft
1,850 ft	1,900 ft	2,400 ft	3,800 ft	5,100 ft

pressure, as they occur during a detonation, can cause irreversible damage, which, if severe enough, can be fatal. The inner ear, particularly the eardrum, is most sensitive to pressure and can rupture even with little explosive mass and relatively far from the detonation site. The lungs can also rupture or collapse at lower distances and with higher amounts of explosives. At very close distances and very high amounts of explosive mass, the explosion pressure can cause

severe or fatal internal injuries. Figure 15 shows the relationship between explosive mass and distance with the probability of injury to the human body.^{13,14} It is important to note, however, that these calculations do not consider the fragmentation that usually occurs and that the distances given are by no means to be considered safe unless the person took cover. Table 3 shows recommended safety distances from the centre of an explosion.¹⁵

Figure 17: Example Evacuation Plan with Designated Drone Incident Assembly Points.

Assembly Points for Drone Incidents



[M] Floor Plan: © JAPCC; Textures/3D Objects: © Adobe; Floor Plan Surrounding Signs: © Copyrighted
 Sign 'Drone Evacuation Point' – Drone: © AdobeStock, 260694458 (10 November 2023); Shield: © Copyrighted; Group: FourLeafLover – stock.adobe.com; Arrows: © Copyrighted

4.2 Hazardous Materials

Drones could disperse hazardous agents or substances across the Chemical, Biological, Radiological, and Nuclear (CBRN) spectrum that severely threaten the health and safety of affected individuals. These may include nerve agents, toxic gases, pathogens, bacteria, viruses, or radioactive materials. Improvised CBRN attacks can be conducted by spraying pesticides and herbicides or disseminating finely powdered rat poison or other freely available toxins. It should be noted that the effects of contact with or

be visible if hidden within the drone's casing. Consequently, if an unauthorized presence of a drone is encountered, extreme caution is advised, and the drone ought to be treated as a possible explosive device until called-in professionals can give an all-clear.

4.3.2 Hazardous Materials

The effects of the various CBRN substances are diverse. At worst, it can be assumed that even the most minor quantities and the shortest contact times are sufficient to cause severe harm to a person's health.

'Unlike fire or bomb threat calls, do not leave the building and expose yourself to the drone. Remain inside and seek shelter!'

inhalation of hazardous materials may not occur immediately after ingestion but may take hours or days to show symptoms indicative of poisoning.

Discussion of the various effects of all possible CBRN payloads is beyond the scope of this paper. However, since the hazardous substances mentioned all have in common that they pose a severe risk to the health of exposed individuals, the following sections provide generally applicable recommendations to avoid or minimize the effects of the substances addressed.

4.3 Assessment

4.3.1 Explosives

Even small amounts of explosives can cause severe injuries to the human body and break glass surfaces and windows. To further aggravate the situation, most common public and office buildings have been constructed without considering protection against explosions, and physical security measures are typically aimed against burglary and intrusion. In addition, identifying a drone, especially its payload, is extremely difficult for the untrained eye, and explosives may not

An appropriate device, such as an agricultural drone, is required to apply the substances mentioned, for example, a liquid tank and spray nozzles or a container designed for emptying. As mentioned in the last paragraph on explosives, extreme caution should be exercised, especially if attached tanks or containers can be identified. Always wait for professionals to respond, and refrain from taking any action against the drone yourself to avoid contamination.

4.4 Mitigation Options

Since blast strength decreases exponentially with distance, stand-off is the best method to minimize the risk. It is also advisable to seek shelter to avoid being hit by potential fragments. Staying well clear of a drone and seeking shelter is also advisable to minimize the effects of hazardous substances that it may carry.

4.4.1 Immediate Measures

4.4.1.1 Leave the Room. To mitigate the effects of the blast and avoid injury from shattered glass in the event of a detonation, immediately exit any room or part of the building from which the drone can be

observed. Close doors and try to get at least two walls between you and the drone. Refrain from being inquisitive and stay well clear of glass surfaces and windows. Standard windows can shatter a considerable distance from a detonation. Although mostly non-fatal, broken glass is statistically the most common cause of injury after an explosion. Leaving the room and closing the door behind is also advisable to mitigate the propagation of hazardous substances.

4.4.1.2 Seek Shelter. If in the open, get indoors to avoid exposure to fragmentation and hazardous materials. If this is not feasible, keep yourself as far as possible from the drone. Take cover behind solid objects to mitigate the impact of fragments that may occur in the event of a detonation.

4.4.2 Preparatory Measures

4.4.2.1 Establish a Designated Evacuation Point.

In the event of a fire or bomb threat, the standard procedure is to evacuate the building. However, in the case of a drone incident, the danger is outside the building, and it is, therefore, safer not to leave the structure. Thus, a designated evacuation point for drone incidents should be established within the building (cf. Figure 17). This point could be the hallway between offices or a room inside the building without exterior walls. It could also be a dedicated shelter in the basement. However, employees on the upper floors may need more time to reach it, and, if applicable, the longer duration must be considered when developing the appropriate evacuation plans.

4.4.2.2 Place Desks at Some Distance to Windows.

As mentioned, the best protection against explosions is distance from the detonation. If room conditions permit, place employees' work areas as far away from the window as possible. Since explosion pressure decreases exponentially with distance, just a few more metres of space can make the difference between life and death.

4.4.2.3 Reinforce Windows. Not every office or workplace can be evacuated in the event of a threat. For example, command and control or emergency operations centres may have to remain staffed even in an emergency. Larger spaces like dining halls may not be evacuated quickly enough. In these specific cases, reinforcement of windows should be considered so that personnel can remain in place with reasonable protection. Applying a protective blast film may be sufficient to withstand smaller explosive masses instead of completely upgrading the windows with blast-proof frames and glass. However, this is always a case-by-case consideration and requires appropriate on-site consultation.

1. Volodymyr Rykhlitskiy, 'Production that cannot be destroyed by missiles – kamikaze drones made in Ivano-Frankivsk for use on the front', *Ukrainska Pravda*, 7 August 2023, <https://www.pravda.com.ua/eng/articles/2023/08/17/7414480>, (accessed 13 November 2023).
2. UN SaferGuard, International Ammunition Technical Guidelines, 'Kingery-Bulmash Blast Parameter Calculator', UN Office for Disarmament Affairs, [website], n.d., <https://unsafeguard.org/un-safeguard/kingery-bulmash>, (accessed 13 November 2023).
3. R. Karl Zipf, Jr., Ph.D., P.E., and Kenneth L. Cashdollar, 'Effects of blast pressure on structures and the human body', Centers for Disease Control and Prevention (CDC), July 2010, <https://www.cdc.gov/niosh/docket/archive/pdfs/NIOSH-125/125-ExplosionsandRefugeChambers.pdf>, (accessed 13 November 2023).
4. Drone Surf, 'DJI Mini 2 maximum weight lift test', [online video], 24 November 2020, <https://www.youtube.com/watch?v=y13yY2k3dvl>, (accessed 22 March 2024).
5. Drone Surf, 'Mavic 3 – Lifting weight test', [online video], 2 December 2021, <https://www.youtube.com/watch?v=bYyGcN-bhZE>, (accessed 22 March 2024).
6. Gannet Drone Fishing, 'Phantom 4 Max lift and drop testing with Gannet', [online video], 23 May 2018, <https://www.youtube.com/watch?v=roFoMkESXmI>, (accessed 22 March 2024).
7. Aerial Media Gladstone, 'DJI Matrice M300 RTK Maximum Payload Weight Lift Test', [online video], 4 December 2020, <https://www.youtube.com/watch?v=6sln44hDr1A>, (accessed 22 March 2024).
8. Norbert Gebbeken and Moritz Hupfaut, 'Behavior of reinforced concrete structures under high dynamic loads with focus on the distribution of secondary debris and residual load bearing capacity of pre-damaged reinforced concrete slabs', University of the German Armed Forces, Munich, October 2023.
9. Ibid. 2.
10. Ibid. 3.
11. 'Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings', FEMA 426, Federal Emergency Management Agency (FEMA), December 2003, p. 4–19., https://www.fema.gov/sites/default/files/documents/fema_426_reference_manual.zip, (accessed 13 November 2023).
12. UN Department of Safety and Security (UNDSS), Division of Specialized Operational Support, Physical Security Unit (PSU), PSU Information Bulletin, 'Blast Protection for Windows (draft)', 16 December 2020, www.unicef.org/jordan/media/5951/file/LRFP-2021-9166373-Annex_4-Blast_Protection_for_Windows.pdf, (accessed 15 November 2023).
13. Ibid. 2.
14. Ibid. 3.
15. US Department of Homeland Security, 'IED Attack – Improvised Explosive Devices', 2009, https://www.dhs.gov/xlibrary/assets/prep_ied_fact_sheet.pdf, (accessed 15 November 2023).



Chapter 5

Cyber Attacks

Drones can be utilized to conduct cyber-operations when carrying dedicated payloads, enabling them to exploit or attack wireless and cell phone networks or other radio-controlled equipment in their vicinity. The miniaturization of electronics and computers allows for integrating sophisticated network sniffing and hacking tools into small, lightweight payloads that most consumer drone models can easily carry. Commercially available and inexpensive hacking tools such as the Wi-Fi Pineapple¹ (cf. Figure 18) have been legally available for many years, can be purchased online, and are easy to use, making the barrier of entry surprisingly low thanks to the numerous YouTube videos and online tutorials explaining how to operate them. Therefore, it is increasingly urgent to improve employees' awareness and mindset on cybersecurity. Furthermore, investing in robust enterprise-level cybersecurity solutions to defend wireless networks is

critical as drones provide a new avenue of attack that is inexpensive and significantly reduces the risks to the attacker.

5.1 Cyber Capabilities

The following sections briefly describe the potential cyber capabilities of drone payloads that can be easily purchased online and are available for anyone starting at as little as 35 Euros.

5.1.1 Rogue Wireless Network Hotspot

A wireless network (often also referred to as a Wi-Fi) hotspot is a device that provides wireless internet access and is commonly found in public places, for example, cafes, airports, hotels, or libraries. Mobile phones, tablets, or laptops are usually configured to store known Wi-Fi network details so they can automatically connect to them when in range. For this purpose, mobile devices actively seek Wi-Fi signals in the area and try to find a match against their stored list of known

networks. Unencrypted networks, where usually no password is required, are of particular concern as drones with specialized hacking payloads can listen to the cell phone's search broadcasts and fake the Wi-Fi the device is looking for (cf. Figure 19).² A mobile device will recognize the rogue hotspot's fake network as a known Wi-Fi and connect to it. Once connectivity is established, all network traffic can be intercepted and monitored by the operator of the rogue hotspot.

5.1.2 Wireless Access Point Password Theft

A drone with specialized hacking payloads can track the login transmissions from mobile devices to a secured wireless network. When a mobile device wants to connect to a secured Wi-Fi, encrypted messages are exchanged between the Wi-Fi's hotspot and the device for authentication. This initial communication between a hotspot and a mobile device is called a handshake. A drone can exploit the wireless communication standard and send de-authentication messages to the mobile device and the hotspot, forcing them to disconnect and initiate a new handshake with a new encrypted message sequence. Catching multiple handshakes with enough variations is sufficient to breach the encryption and reveal the password. Although this cannot (yet) be done in real-time on-site, modern processing units can decrypt a handshake in a few hours. An attacker may also subscribe to one of the dedicated Dark Web tools that offer decryption services for just a few Euros. Fortunately, this type of attack can be detected, provided appropriate countermeasures are in place. Otherwise, the stolen passwords could be used in a subsequent attack to gain unauthorized access to the network using the compromised credentials.

5.1.3 Electromagnetic Intelligence

Drones can also be equipped with payloads that scan frequencies other than Wi-Fi bands, enabling them to map the use of the electromagnetic spectrum in a particular area, also known as 'wardriving'.³ This data can then be exploited to determine activities and vulnerabilities by identifying signals such as radio frequencies used by the guard force, remote control frequencies used for barriers and road-blocking mechanisms (if

radio-controlled), frequencies of radio-controlled fire alerts, and more.⁴ The gathered intelligence can then be used later for other malicious activities.

5.1.4 Exploit Unprotected Wireless Networks

A drone may connect to an existing Wi-Fi offered publicly for the organization's guests and members, such as at the dining facility or meeting rooms. Access to such unprotected networks can be exploited to gather information about the network's users, for example, the brand and type of the devices connected, their IP addresses, operating systems, and activated network services that have known 'zero-day' vulnerabilities and are not yet updated.⁵ Furthermore, unencrypted web traffic, emails, login credentials, or other sensitive information may be captured.

5.2 Assessment

While cyberattacks are not new, the methods and techniques are constantly evolving. In the past, attackers had to approach a target network physically and thus risk detection and arrest. In contrast, today, they can utilize drones to penetrate physical security perimeters. Armed with lightweight and drone-transportable network tools such as the WiFi Pineapple, drones can enter protected areas without the need for the attacker to be physically present. When paired with local cellular connectivity, the capabilities that can be brought to bear against a wireless network are considerable. The potential impact is significant, from compromising intellectual property and exploiting system vulnerabilities to breaching personal data. The possibility of sabotage through the deletion of data and even the physical destruction of computer-controlled equipment is no longer fiction. This convergence of technology and tactics underscores the urgency of implementing more comprehensive security measures in this ever-changing digital landscape.

5.3 Mitigation Options

Organizational and individual security measures are required to minimize potential cyber threats. These



Figure 18: The WiFi Pineapple mounted below a small customized drone.

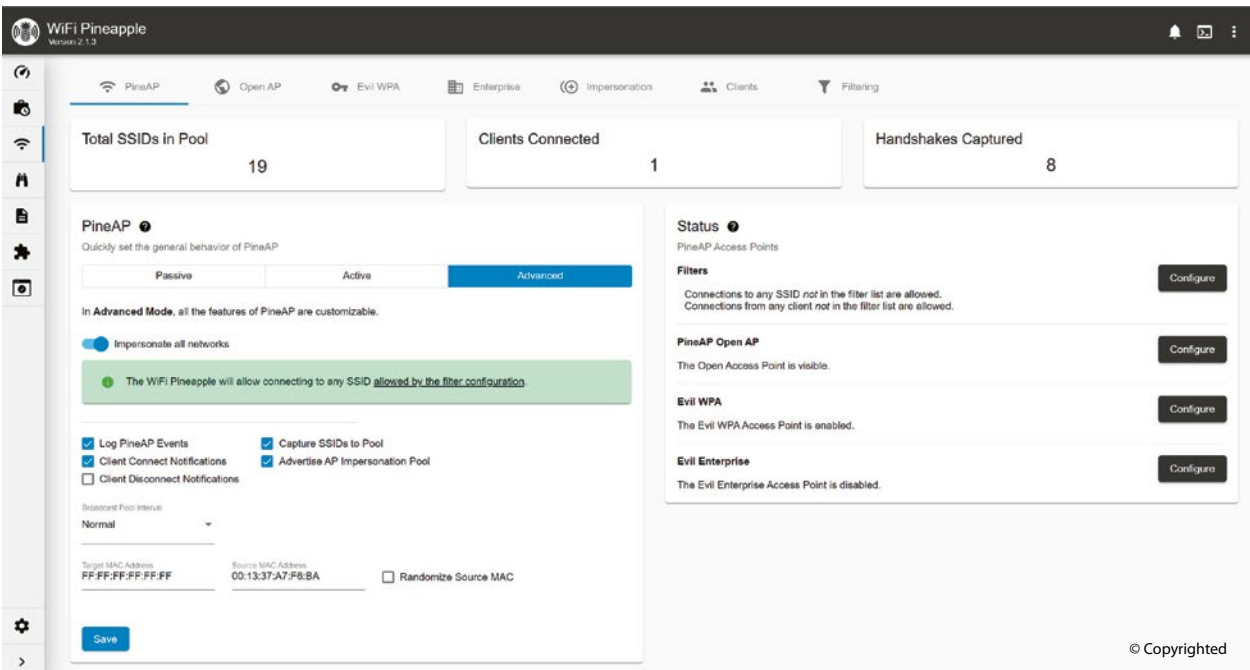


Figure 19: Screenshot of the WiFi Pineapple's Web Interface during a Live Testing at the JAPCC's Premises.

measures should address the official computer equipment used at work and the private hardware brought into the workplace by employees.

5.3.1 Immediate Measures

5.3.1.1 Check Your Wi-Fi Connection. Ensure your mobile device is still connected to the network it is supposed to be on. Disable the option to auto-connect to known Wi-Fi networks (cf. 5.3.3.2). Disconnect your mobile device immediately if you recognize wireless networks that should not exist, for example, if your favourite restaurant's Wi-Fi suddenly appears at your office location. Also, be suspicious if there is an unusual abundance of wireless networks offered, as they might be fake and tapped from your colleagues' mobile devices.

5.3.1.2 If in Doubt, Turn off Your Wi-Fi. If you recognize any unusual or suspicious activity, turn off your mobile device's wireless connection completely. Even if you are not actively using your device, emails, notifications, and other processes run in the background and transmit and receive information. Furthermore, you can remain connected through your cellular data plan, so Wi-Fi connectivity is unnecessary.

5.3.2 Post Incident Measures

5.3.2.1 Check if a Drone Has Landed or Left Something Behind. Usually, cyber-attacks, as described above, benefit from the device (not necessarily the drone) staying in place for some hours or even days. If equipped with additional battery packs or a small solar panel, a drone or hacking payload could be powered significantly longer. Hence, a covert landing or payload delivery is likely a preferred option for the attacker. Remember to keep clear of a landed drone or unexpected objects found after a drone sighting, as it may carry explosives or other hazardous materials.

5.3.3 Preparatory Measures

For Personnel

5.3.3.1 Clean Your Wi-Fi List. Routinely check the list of wireless networks stored on your device and remove any entries you do not use regularly. Delete all

entries of unsecured networks and adopt the routine of either not using them in general or removing them from the list after use.

5.3.3.2 Check Your Mobile Device Settings. Most mobile devices are set to connect to known networks automatically. Configure your mobile device to either confirm each connection attempt or manually establish every connection. Consider having Wi-Fi connectivity off as default and turning it on only when needed.

5.3.3.3 Use a Virtual Private Network (VPN). When using a VPN, all internet traffic between your device and the VPN provider is encrypted and thus prevents eavesdropping by anyone else on the network. The consistent use of a VPN is always a sound security practice and will significantly increase the difficulty of an attacker trying to compromise mobile devices through a drone impersonating a fake Wi-Fi.

For the Organization

5.3.3.4 Upgrade from Wi-Fi to WLAN. WLAN (Wireless Local Area Networks) are enterprise-level Wi-Fi solutions equipped with enterprise-level security solutions to facilitate the management and securing of networks important to an enterprise.

5.3.3.5 Secure Your WLAN. Though convenient and offering easy access to staff and guests, unsecured wireless networks must be discouraged due to the associated security issues. Consistently implement robust enterprise-level authentication that uses individual usernames and passwords to contain network intrusion and limit the damage of password theft.

5.3.3.6 Offer a VPN for Your Staff. In line with section 5.3.3.3, set up a VPN and encourage your staff to use it for an additional layer of cyber security.

5.3.3.7 Sanitize Your Wi-Fi. Ensure no sensitive data is transmitted via open or insufficiently encrypted Wi-Fi. If local conditions do not permit physical network connections, use WLAN (cf. 5.3.3.4 f.) or additional end-to-end encryption with adequate strength independent of the Wi-Fi's encryption method, adding a second layer of protection.

5.3.3.8 Separate Your Guest Wi-Fi from Your WLAN.

To maintain the integrity of your organization's WLAN, it is crucial to restrict its usage solely to your staff. However, in situations where guests require Wi-Fi access, especially within a meeting room, it is advisable to create a dedicated and secure guest network. By providing guests with a password, they can enjoy internet connectivity without compromising the security of your primary network. It is essential to change this password immediately after each event and periodically to ensure maximum protection.

5.3.3.9 Bolster Your Network Intrusion Prevention and Detection.


Turn off your Wi-Fi access points outside regular working hours when no one is expected to be in the office. Also, Wireless Intrusion Prevention Systems (WIPS) can detect de-authentication attacks, as described in section 5.1.2. This practice will give your Incident Response Team (IRT) enough time to reset the passwords for affected individuals and prompt your IRT to look for the hacking hardware, even if the drone used to deliver it was never sighted. Furthermore, WIPS can detect many other intrusion attempts, such as a user logging in at unusual hours, from multiple locations at once, or from unauthorized access points.

5.3.3.10 Issue a Mobile Device Policy.

Educate employees about the cybersecurity issues with unprotected wireless networks and recommend best practices for configuring their mobile devices. Generally, only permit business-issued devices on the WLAN. Allow only personal devices loaded with an enterprise Mobile Device Management (MDM) software suite that would allow the enterprise to limit and monitor the device's activity on the enterprise network. Consider a general no-mobile device policy for classified and sensitive areas.

1. 'Wi-Fi Pineapple', Hak5 LLC, [website], n.d., <https://shop.hak5.org/products/wifi-pineapple>, (accessed 15 November 2023).
2. 'Setting up your WiFi Pineapple', Hak5 LLC, [website], 22 September 2022, <https://docs.hak5.org/wifi-pineapple/setup/setting-up-your-wifi-pineapple>, (accessed 15 November 2023).
3. Moving around a physical space and cataloguing Wi-Fi networks, ostensibly for future exploit. Bradley Wilson et al., 'Small Unmanned Aerial System Adversary Capabilities', Homeland Security Operational Analysis Center operated by the RAND Corporation, 2020, https://www.rand.org/pubs/research_reports/RR3023.html, (accessed 15 November 2023).
4. Dedicated professional drone platforms provide a spectrum measurement capability with direction finding from 20 MHz to 50 GHz. Wireless Innovation Forum, 'Overview of the Use of Drones for Spectrum Monitoring Applications', WINNF-TR-2009, Version 1.0.0, 1 November 2021, p. 10 f., <https://www.wirelessinnovation.org/reports>, (accessed 15 November 2023).
5. A zero-day vulnerability is a software vulnerability discovered by attackers before the vendor has become aware of it. Because the vendors are unaware, no patch exists for zero-day vulnerabilities, making attacks likely to succeed. 'What is a Zero-day Attack? – Definition and Explanation', Kaspersky Lab, [website], 2023, <https://www.kaspersky.com/resource-center/definitions/zero-day-exploit>, (accessed 15 November 2023).



 Background and Red Alert Light: © zef art – stock.adobe.com; Megaphone: © Adobe

Chapter 6

Drone Reporting

The previous three chapters have explained the main threats of small drones and highlighted immediate and preventive countermeasures. However, an essential pre-condition for the successful implementation of the measures recommended is the timely warning that a threat exists if the presence of a potentially dangerous drone has not been personally detected or observed.

6.1 Drone Sighting and Classification

Commercial drones are comparatively small flying objects with a relatively high speed given their size, which makes early detection difficult; often, the

presence of a drone is first acoustically perceived before it is visually recognized, or the acoustic cue enables visual orientation towards the drone in the first place. If the drone is in motion and not hovering in place, the time it can be observed may also be relatively short, and limited to gaps between structures or vegetation. These factors will almost certainly overwhelm an inexperienced observer to such an extent that valuable time is lost when assessing a potential threat.

Recognition and classification of commercially available drone types should be an integral part of drone awareness training. Personnel should be able to recognize at least the shape and size of the drone as well as the number of rotors to draw initial conclusions about the possible payload and the associated potential danger. Where possible, live demonstrations of drone flights should also be offered as part of the training to provide participants with the typical acoustic

and visual sensations as realistically as possible so that they can recall their personal experience in an emergency and gain time when classifying the observed drone characteristics.

6.2 Immediate Warning Options

Ensuring personal safety should always be the top priority. It serves no purpose to put oneself at risk in an attempt to warn others. This practice is analogous to the established procedures for accidents, fire, and first aid. Therefore, it is strongly recommended to get oneself to safety first and only then perform any subsequent warning measures once safely positioned. Regular drills help build confidence and reduce the time between protecting oneself and alerting others to a minimum.

6.2.1 Warning Shout

The quickest and most straightforward measure is to warn people within audible range with a loud call. This warning shout can be made immediately and in parallel with personal self-protection measures and should, therefore, always be used as the first measure to warn others. The warning call should be simple, pre-defined and well-known, for example 'Drone! Drone! Get to safety!'

6.2.2 Emergency Call

After taking personal protective measures, the incident must be reported immediately to the police, and, if applicable, security personnel. The latter can then alert all areas of the organization centrally and request protective measures to be taken. In this context, essential information on the incident must be communicated quickly and precisely.

The so-called '9-Liner' has proven effective in military operations in medical emergencies. Similarly, you will find a reporting scheme adapted for drone emergency reports in Annex A. It is recommended to display this reporting scheme, adapted to local conditions and pre-filled with the relevant emergency numbers, at the drone evacuation point. Ideally, a landline tele-

phone for emergency calls is also installed at this location. It is also advisable to coordinate the reporting scheme with the authorities to be alerted.

6.3 Centralized Alerts through Guards and Security Personnel

The larger the organization, particularly its infrastructure and spatial footprint, the more critical it is for all relevant areas to be alerted. Military facilities and larger commercial and industrial areas usually have a guard or security centre that can centrally initiate and coordinate all alarm measures after notification of drone detection. Below are some options for centralized alerting.

6.3.1 Message Alert

6.3.1.1 Email. In office buildings, staff usually work at workstations connected to a computer network. There are several ways of warning personnel on their computers using electronic messages in such a network. For example, this alerting can be done by utilizing an

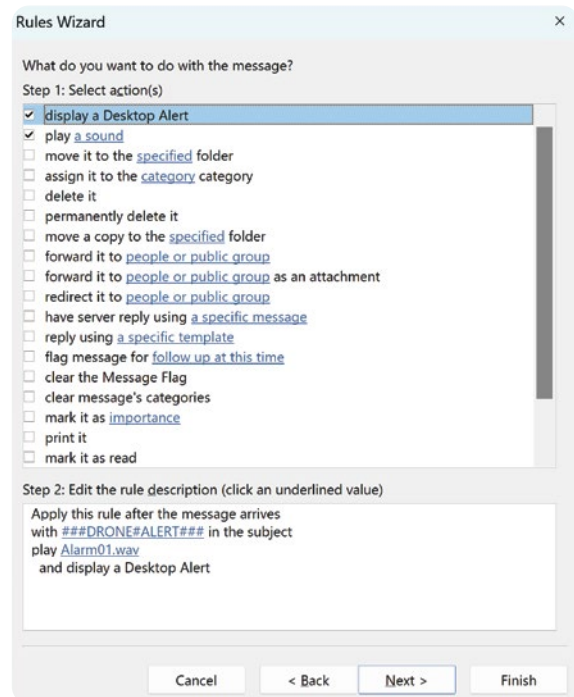


Figure 20: Configuring an Email Rule to Alert Staff at Their Workplaces.

email rule configured uniformly for all, which prominently highlights a corresponding alarm email in the inbox and triggers an individual acoustic signal on the computer. To carry out this procedure without delay, the guard or security centre requires corresponding email templates and email distribution lists.

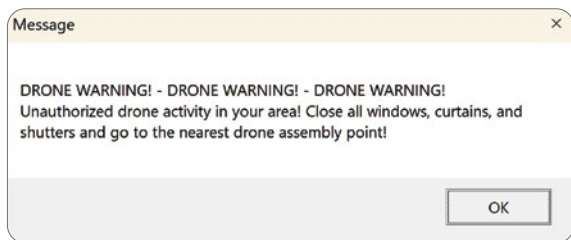


Figure 21: Broadcast Alert Message to All Workstations on the Local Network.

6.3.1.2 Network Broadcast. Another option is to use pre-configured broadcast messages to all computers connected to a network. An administrator usually sends these broadcasts via the command line. However, they can also be prepared and placed as a shortcut icon on the desktop of all computers in the security centre so that they only need to be clicked when an alarm is triggered.

6.3.2 Acoustic Alert

6.3.2.1 Sirens. Siren signals are a tried and tested means of alerting military and civilian personnel. Many military barracks, public buildings and even larger industrial facilities still have sirens installed to warn the population in the event of danger. Siren signals are usually standardized but can vary from country to country. In most nations, an ascending and descending wailing tone is the generic warning signal and prompts people to seek shelter. Siren alerts have an immense range and are highly effective, but their use needs careful consideration. Particularly in the case of low-level threat situations, a siren alarm may cause more uncertainty than benefit, whereas, in the case of a confirmed terror warning, its use may be justified and advisable.

6.3.2.2 Loudspeakers. Another means of acoustic alerting is loudspeaker announcements. Public buildings, shopping centres, or production facilities often have loudspeakers to inform staff or customers. The advantage of raising an alarm using loudspeakers is the ability to communicate specific instructions, such as directions and locations where people need to go. This capability is beneficial for visitors unfamiliar with the alarm measures and premises.

6.3.3 Visual Alert

6.3.3.1 Warning Lights. Warning lights are particularly well suited for areas that need to be vacated or may no longer be entered in the event of a drone alarm to avert danger to life and limb if an explosion occurs. These can be, for example, fuel depots, ammunition sites, or stored chemicals. Central control of the warning lights from the security control centre enables the concerned area to be alerted without delay if necessary. Even if on-site personnel are alerted by other means, a locally activated warning light is still helpful in indicating the evacuation notice to outside personnel and preventing them from entering the area.

6.4 After Action Reporting and Incident Documentation

Once an all-clear has been given, all information and testimonies should be gathered to support further police investigations and any resulting prosecution. However, even if no other police action is required, the data collected about the drone incident can be used to review and, if necessary, improve the alert measures. Last but not least, they can be used by the authorities dealing with drone incidents for statistical recording and evaluation and contribute to the broader risk assessment. A reference for an After-Action Report is attached in Annex D. It can be downloaded online at www.japcc.org/drone-drills for further customization.



Chapter 7

Conclusion and Recommendations

7.1 Conclusion

The alarmingly unrestricted accessibility to drones opens a wide range of security implications. Drones can capture high-resolution images and detect objects and people at great distances. Higher quality, more expensive, and, in turn, often larger models are capable of capturing minute details and deciphering documents and computer screens, raising concerns about privacy and the disclosure of sensitive information.

The potential safety risks become even more significant when drones transport explosives. Even small amounts of detonating explosives can shatter windows and glass surfaces, causing severe injury to

people. The lack of explosive-resistant structures in public and office buildings and the difficulty of detecting hidden explosive charges increase that risk. In addition, even small amounts of toxic or hazardous materials can lead to profound health implications even with short exposure times. Aggravatingly, these may not be apparent immediately and only become evident after hours or days. Therefore, extreme caution and professional response are required to avoid contamination, injury, or death when encountering trespassing drones.

The evolution of cyberattacks introduces another layer of security challenges. Previously, attackers would require physical proximity to target networks. However, drones with tools like a Raspberry Pi can circumvent physical security barriers, allowing them to exploit vulnerabilities in wireless networks and, in turn, compromise intellectual property and sensitive data, which highlights the urgency of implementing comprehensive security measures in the constantly evolving digital landscape.

Education and training play a crucial role in effectively addressing these security challenges. Organizations must invest in training programmes to equip personnel with the knowledge and skills to identify, respond to, and mitigate drone threats. This training should include recognizing potential threats, understanding drone risks, and implementing appropriate protocols.

7.2 Recommendations

7.2.1 Educate

To successfully respond to threats presented by drones and to minimize the risk of harm to personnel and property, it is imperative that all potentially concerned personnel receive comprehensive and thorough education. As with the established routines for fire protection and first aid, the dangers posed by drones must be conveyed and refreshed regularly with the same level of emphasis.

Therefore, alongside this white paper, the JAPCC offers frequently updated training materials about drone awareness and countering drone threats for download on its website.

7.2.2 Train

Drones can appear unexpectedly at any time and in any situation. Therefore, the theoretical knowledge conveyed must be verified in practice and converted into actual action. For a very low budget of less than

100 euros, a beginner's drone can be purchased and used for demonstrations, but this is not essential. After all, there is no need for an actual fire to exercise a fire alarm.

For training purposes, one can just show the photo of a drone and use it to initiate the emergency procedures. A drone sighting report can also be practiced based on a printout alone. All other emergency measures recommended in this paper do also not require a real drone to be practiced.

The annexes to this White Paper provide templates of information signs like those displayed for fire and first aid measures. These are also suitable and can be used as a checklist of the immediate drone response measures to be reviewed, in addition to their use as a general information media for the staff.

All annexes to this White Paper are also available online as digital downloads on the JAPCC website to allow for customization to the needs of the organization that wishes to use them.

***Run a drill.
You don't have to have a flying object to
run a drill any more than you have to have a fire
to have a fire drill.***

**Richard Lusk, Director, UAS Research Center,
Oak Ridge National Laboratory**



Please visit
www.japcc.org/drone-drills
to download customizable templates for the annexes included in this paper,
as well as additional educational references and materials.



Drone: © AdobeStock, 260694458 (10 November 2023)

Annex A

Drone Sighting Report Sheet

☎ Police:
☎ Guards:
☎ Ambulance:
📍 Your Location:
<i>Fill in before posting.</i>

<input type="checkbox"/> Drone Found <input type="checkbox"/> Drone Sighting <input type="checkbox"/> Drone Attack		When reporting, read only applicable items.					
1	Who is reporting?	A	Name	B	Unit	C	Own Location
2	Injuries or Fatalities	D	<input type="checkbox"/> YES <input type="checkbox"/> NO First Responders Required	E	_____ persons injured		
3	Date and Time	F	Date	G	Time		
4	Observations						
	Activity	H	<input type="checkbox"/> In Flight <input type="checkbox"/> Hovering <input type="checkbox"/> Landed <input type="checkbox"/> Crashed <input type="checkbox"/> Exploded		I	Heading	
	Drone Size	K	<input type="checkbox"/> Mini (<10 cm) <input type="checkbox"/> Small (<50 cm) <input type="checkbox"/> Medium (<100 cm) <input type="checkbox"/> Large (>100 cm)		J	Location	
	Type and Number	L	<input type="checkbox"/> Multi-Rotor _____ Number of Rotors	<input type="checkbox"/> Fixed-Wing	M	Number of Drones	
	Payload	N	<input type="checkbox"/> visible <input type="checkbox"/> not visible	O	Suspected Type		
	Other	P	<input type="checkbox"/> Colour _____ <input type="checkbox"/> Lights _____ Number and Colour of Lights				
5	Action Taken	Q	<input type="checkbox"/> Taken Cover <input type="checkbox"/> Observing* <input type="checkbox"/> Engaging* <input type="checkbox"/> Providing First Aid *If not trained in drone defence, refrain from observing or engaging.				

Annex B

Drone Incident After Action Report

Type of Drone Incident

<input type="checkbox"/> Drone found Suspected <input type="checkbox"/> Accident/Crash <input type="checkbox"/> Intentional Landing	<input type="checkbox"/> Illegal Flight Activity Suspected Intent <input type="checkbox"/> Unintentional Overflight <input type="checkbox"/> Espionage <input type="checkbox"/> Disruption <input type="checkbox"/> Subversion	<input type="checkbox"/> Drone Attack Damage occurred to <input type="checkbox"/> Personnel <input type="checkbox"/> Equipment <input type="checkbox"/> Infrastructure
---	--	---

Brief Summary of Incident

Date	Time	Duration	Location	Drone Count
dd/mm/yyyy	hh:mm	hh:mm	UTM	

Summary

Short description of the incident

Contact Details

	Reporter	Witness	Witness
Name, First Name			
Title or Rank			
Organization or Unit			
Email			
Phone			

Drone Specifications

Observation Method

Technical Sensing Radar Optical Acoustic

Human Sensing Optical Acoustic

Type	Dimensions	Payload
If recognized <input type="checkbox"/> Single Rotor <input type="checkbox"/> Quadcopter <input type="checkbox"/> Multicopter <input type="checkbox"/> Fixed-Wing <input type="checkbox"/> Biomimetic	Estimated <input type="checkbox"/> Airframe <input type="checkbox"/> Wingspan <input type="checkbox"/> Miniature (< 10 cm) <input type="checkbox"/> Small (10–50 cm) <input type="checkbox"/> Medium (50–100 cm) <input type="checkbox"/> Large (> 100 cm)	If recognized <input type="checkbox"/> Camera (built-in) <input type="checkbox"/> Camera (attached) <input type="checkbox"/> Other (specify below)
Speed	Altitude	Other
Estimated Maximum Speed _____ <input type="checkbox"/> m/s <input type="checkbox"/> km/h	Estimated Min _____ (m) Max _____ (m)	Additional details observed, for example, colour

Drone Behaviour

<input type="checkbox"/> Has hovered	<input type="checkbox"/> Has crashed	<input type="checkbox"/> Has landed	<input type="checkbox"/> Has dropped sth.
Number of Stops/Duration _____ / _____ _____ / _____ _____ / _____ _____ / _____ _____ / _____ <input type="checkbox"/> Additional Hovers in Annex	Suspected Reason <input type="checkbox"/> Accident <input type="checkbox"/> On Purpose <input type="checkbox"/> Other (specify below)	Number of Landings/Duration _____ / _____ _____ / _____ _____ / _____ _____ / _____ <input type="checkbox"/> Additional Landings in Annex	If unsure treat as IED <input type="checkbox"/> Solid Object <input type="checkbox"/> Liquid/Chemicals <input type="checkbox"/> Powdery Substance <input type="checkbox"/> Technical Device <input type="checkbox"/> Other (specify below) <input type="checkbox"/> Forensic Report in Annex

Annex C

Guidelines for Conducting a Drone Drill

Proper education and regular training on drone incident procedures are essential for effectively responding to threats. This is crucial for protecting personnel, material, intellectual property, and sensitive data. The following guidelines are designed to help you plan a drone drill. It is important to note that these guidelines are not universally applicable and should be adjusted to fit local conditions. Please be aware that this checklist focuses on immediate drone response measures and does not cover planning considerations for dedicated drone defence systems and their deployment. To customize this document, please visit www.japcc.org/drone-drills to download the editable file.

Mission Analysis/Assessment

1. Critical Infrastructure

1.1 Identifying Mission-Critical Infrastructure and Equipment

- What is the crucial aspect of the organization's mission or production?
- Which infrastructure and equipment are indispensable for sustaining it?
- What personnel are essential for operating that infrastructure and equipment?
- What is the potential financial loss if production is interrupted?
- What is the potential impact if intellectual property is compromised?
- What is the potential impact if the mission is interrupted?

(It is highly advisable to assess the estimated loss/impact in comparison to an investment in professional drone defence systems that could aid in maintaining mission-critical processes.)

1.2 Vulnerability of Critical Infrastructure and High-Value Equipment

(e.g., weapon systems, communications, power generators, water supply)

- Can high value equipment be securely stored or quickly sheltered in the event of a threat?
- Is there redundancy built into critical systems to ensure continued operation in the face of damage or loss?
- Is it possible to disguise critical infrastructure to prevent observation or deceive drone threats?
- Can critical infrastructure be hardened to withstand smaller yields of explosive?
- Is there a way to keep drones at a safe distance to minimize potential blast damage?

If critical infrastructure or equipment is deemed mission essential and the answer to these questions above are negative, it is strongly advised to explore options for implementing professional drone defence systems.

1.3 Considerations for Areas that Contain Hazards

(e.g., ammunition storage sites, fuel tanks, chemicals)

- Has the minimum safety distance been assessed?
- Are there nearby protective structures or shelters available?
- Have designated evacuation points been established and clearly marked?
- Are special hazard-related First-Aid kits available for emergencies?

2. Regular Infrastructure

2.1 Vulnerability to Drone Observation

- Are computer screens positioned away from windows to prevent observation?
- Are whiteboards and flipcharts covered when not in use to protect sensitive information?
- Are there guidelines for handling classified materials?
- Have window blinds been installed to enhance privacy?
- Have additional measures been implemented to prevent unauthorized observation?

2.2 Vulnerability to Explosive Drone Payloads

- Are workplaces located at a safe distance from windows?
- Do office windows have blast-resistant capabilities?
- Are the inner walls sturdy enough to provide adequate protection against blasts and fragmentation?

3. IT Infrastructure

3.1 Vulnerability of Wireless Computer Networks

- How many wireless networks are broadcasting in the area?
(It is recommended to map all wireless networks in the area, not just your own.)
- Are your wireless networks sufficiently encrypted?
- Are intrusion detection systems in place to monitor and respond to potential security breaches on the wireless networks?
- If other wireless networks are identified as insecure, can the provider be contacted?
(Other networks that are not secured could be exploited, potentially compromising the devices of your own personnel as well.)

3.2 Vulnerability of Mobile Devices

- Are private devices with wireless connectivity permitted in the designated area?
- Are company-issued devices consistently updated and configured to adhere to the most current security protocols?
- Has a comprehensive mobile device policy been established for both employees and visitors?

4. Personnel

4.1 Vulnerability of Personnel Exposed Outside of Buildings

(e.g., sports fields, maintenance areas, designated smoking areas)

- Are there any protective structures or shelters nearby?
- Have evacuation points been established and clearly marked in the vicinity?
- What is the estimated time needed to reach the nearest shelter?
- Are there any obstacles blocking the way to the evacuation points?

4.2 Vulnerability of Personnel Inside Buildings

- Have evacuation points been established and clearly identified?
- Can personnel reach the evacuation points quickly and efficiently?
- Are there any obstacles (e.g., furniture) blocking the path to the evacuation points?

4.3 Considerations for Crowds of People

(e.g., meeting rooms, conferences, exhibitions, dining halls, sports events)

- Are the evacuation routes and emergency exits sufficiently large to allow for a quick and efficient evacuation in case of an emergency?
- Are evacuation points, emergency exits, and evacuation routes clearly marked and easily identifiable?
- Are the designated evacuation points capable of accommodating the entire crowd in case of an emergency?
- Have evacuation procedures been adequately trained and tested to ensure that panic is minimized during an emergency?

If the answer to any of the above questions is no, it is strongly advised to consider enhancing the infrastructure to protect against potential threats, such as small explosives. Another option to consider is the implementation of professional drone defence systems.

Drone Drill Planning and Execution

5. Emergency Procedures

5.1 Education and Training

- Is there a drone threat awareness curriculum (see below) in place and regularly delivered?

Suggested Curriculum Contents

- Types, classes, and key visual characteristics of drones;
- Potential threats originating from drones (espionage, terrorism, sabotage);
- Preparatory measures to mitigate the above threats;
- Drone incident procedures, warning signs, and drone evacuation points;
- Warning and reporting procedures, including emergency points of contact;
- All-clear procedures.

Furthermore, a live demonstration offers a unique opportunity to witness firsthand the acoustic and visual cues of drones in action.

5.2 Drone Incident and Reaction Plan

- Do the organization's safety, security, and emergency procedures account for drone incidents?

Preparatory Measures in Support of Safety and Security

- Protection against espionage (refer to chapter 3.5.2)
- Defence against terrorism and sabotage (refer to chapters 4.4.2 and 5.3.3)

Immediate Actions in Support of Emergency Procedures

- Implementing measures against espionage (refer chapter 3.5.1)
- Taking steps against terrorism and sabotage (refer to chapters 4.4.1, 5.3.1, and 5.3.2)

- Are dedicated drone incident evacuation points incorporated into all evacuation plans?
 - Are warning and information signs prominently displayed? (refer to annexes F and G)
 - Are drone reporting formats coordinated with first responders? (refer to annex A)
 - Are central drone warning procedures in place? (refer to chapter 6.3)
-

5.3 Exercise Preparation

- Clearly define the exercise objective.
(review of preparatory measures, observation and reporting, evacuation drill, full exercise?)
 - Determine the scope of the exercise.
(full base/organization or dedicated buildings/areas/staff elements)
 - Review existing emergency plans.
(are there any overlaps, synergies, or conflicts with existing procedures that can be used or need to be deconflicted?)
 - Prepare, distribute, and promote exercise materials.
(updated emergency procedures, evacuation plans, drone report sheets, warning and information signs, etc.)
 - Conduct a site survey.
(are evacuation plans, drone report sheets, warning and information signs in place?)
 - Issue exercise instructions, a warning order, or an announcement.
(An initial announcement for a drone exercise is essential to allow personnel to become acquainted with the newly implemented measures beforehand. Subsequent drone exercises can then be conducted regularly without prior notification.)
 - Communicate, collaborate with, and/or involve external authorities.
(Depending on the objective and scope, external authorities such as the military police, the local police or the security staff may need to be informed/involved. Live drone flights, if applicable, should always be coordinated with external authorities, as the drone can trigger unplanned reports outside of the actual exercise.)
 - Assign an evaluation team and provide them with a checklist of expected measures to assess the exercise's effectiveness.
-

5.4 Run the Drill

- Initiate a drone sighting.
(You don't have to have a flying object to run a drill any more than you have to have a fire to have a fire drill.)

Alternatives to a Live Drone Flight

- Use a photo of a drone and show it to your exercise participants.
(Photos taken at various distances are effective in training observation and reporting skills.)
 - Showcase a real drone in a fixed position.
(This can initiate a drone sighting report, similar to a bomb threat caused by unattended luggage.)
 - Activate one of the established drone warnings.
(While only a few staff members may observe the drone, the majority of staff will need to react based on the warning.)
-

5.5 Evaluation

- Review the checklists used by the evaluation team.
- Interview participants to collect their self-assessments of the implemented measures.
- Distribute an after-action report to all participants.
- Make necessary adjustments to your drone incident and reaction plan.

Annex D

Acronyms and Abbreviations

AED	Automated External Defibrillator	J	Joule
AGL	Above Ground Level	JAPCC	Joint Air Power Competence Centre
BLOS	Beyond-Line-of-Sight	JTF	Joint Task Force
CBRN	Chemical, Biological, Radiological, and Nuclear	kg	Kilogram
CDC	Centers for Disease Control and Prevention	km	Kilometre
cf.	confer (Latin), meaning 'compare'	l/w	Length/Width
cm	Centimetre	lb	Pound(s)
CPR	Cardiopulmonary Resuscitation	LOS	Line-of-Sight
C-UAS	Counter-Unmanned Aircraft System	m	Metre
et al.	et alia (Latin), meaning 'and others'	MALE	Medium-Altitude, Long-Endurance
f.	folium (Latin), meaning 'on the next page'	MDM	Mobile Device Management
FBI	Federal Bureau of Investigations	min	Minute
ff.	folio (Latin), meaning 'and the following pages'	mm	Millimetre
ft	Foot/Feet	MoD	Ministry of Defence
g	Gram	MP	Megapixel
HALE	High-Altitude, Long-Endurance	MSL	Mean Sea Level
HME	Homemade Explosives	n.d.	no date
ibid.	ibīdem (Latin), meaning 'in the same place'	NATO	North Atlantic Treaty Organization
IED	Improvised Explosive Device	p.	Page
IRT	Incident Response Team	psi	pound per square inch

PSU	Physical Security Unit (of the United Nations Department of Safety and Security)	UNDSS	United Nations Department of Safety and Security
TESS	Terrorism, Espionage, Sabotage, and Subversion	US	United States
UA	Unmanned Aircraft	VPN	Virtual Private Network
UAS	Unmanned Aircraft System	Wi-Fi	Wireless Fidelity
UK	United Kingdom	WIPS	Wireless Intrusion Prevention System
UN	United Nations	WLAN	Wireless Local Area Network

Annex E

About the Author

André Haider

Lieutenant Colonel, GE Army, NATO OF-4
JAPCC, Combat Air Branch
Unmanned Aircraft Systems,
Countering Unmanned Aircraft Systems



Lieutenant Colonel Haider began his military career with the German Armed Forces in April 1992. He initially served as a Personnel NCO in the 150th Rocket Artillery Battalion HQ. Following his promotion to Lieutenant in 1998, he took on the role of platoon leader within the same battalion. After three years, he transitioned to the position of CIS Branch Head at the 150th Rocket Artillery Battalion HQ.

Subsequently, Lieutenant Colonel Haider was assigned to the 325th Tank Artillery Battalion in Munster, where he served as a battery commander before assuming command of the maintenance and supply battery.

In 2008, he was appointed as the commander of a maintenance and supply company within the 284th Signal Battalion in Wesel. His responsibilities expanded in 2010 when he became the Deputy Commander of the German support staff for the 1st NATO Signal Battalion in Wesel.

As a follow-on assignment he served as the Deputy Battalion Commander of the 132nd Rocket Artillery Battalion in Sondershausen.

Notably, in 2004/2005, Lieutenant Colonel Haider led the resettlement efforts for Serbian refugees following the March 2004 riots in Prizren, Kosovo. In 2011, he oversaw the rapid deployment of NATO's German Operational Reserve Forces Battalion to Kosovo.

Since 2012, Lieutenant Colonel Haider has been a Subject Matter Expert for Unmanned Aircraft Systems and Countering Unmanned Aircraft Systems within the JAPCC Combat Air Branch. He has authored books, white papers, and articles on various topics, including the operations of 'Remotely Piloted Aircraft Systems in Contested Environments', the establishment of a 'NATO/Multinational Joint Intelligence, Surveillance, and Reconnaissance Unit', the 'Legal and Ethical Implications of Increasing Unmanned System Automation', and 'A Comprehensive Approach to Countering Unmanned Aircraft Systems'.

Lieutenant Colonel Haider represents the JAPCC in and contributes to several key NATO groups, including the NATO Joint Capability Group Unmanned Aircraft Systems, the NATO Counter-UAS Working Group, and the NATO Joint Capability Group Maritime Unmanned Systems.

Drone Warning



Avoid Drone Observation

Close curtains and lower shutters
Cover documents
Lock computer screens



Prevent Cyber Attacks

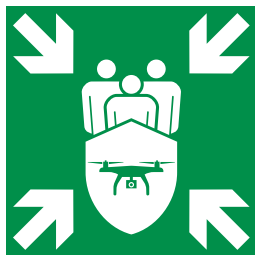
Turn off Wi-Fi connection on all mobile devices

Drone Alarm



Stay Calm

Do not be inquisitive
Stay away from windows



Get to Safety

Leave the room and seek shelter
Do not leave the building



Report Drone Sighting _____

Medical Emergency _____



Please visit

www.japcc.org/drone-drills

*to download customizable templates for the annexes included in this paper,
as well as additional educational references and materials.*



Drone: © AdobeStock, 260694458 (10 November 2023)

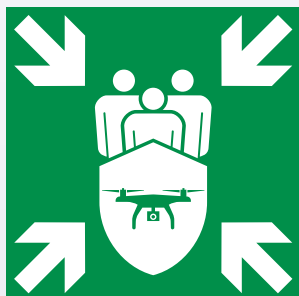
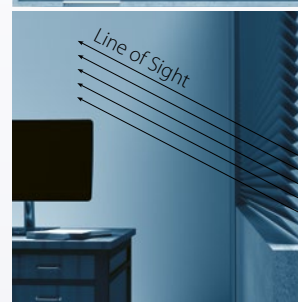
Prepare for Drones



Prevent Drone Observation

Drones always have cameras!

- Turn your screen away from your window.
- Lower shutters and adjust them at an upward angle.
- Cover whiteboards and flipcharts after use.
- Handle classified and proprietary documents with care, stow them away or cover them if not in use.



Mitigate Blast Effects

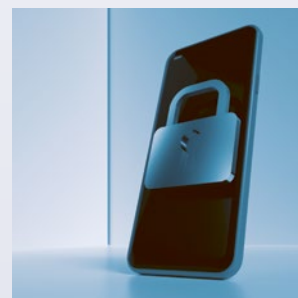
Drones may carry explosives!

- Arrange your workplace at a distance to windows. Blast decreases exponentially with distance, just a little space can make the difference.
- Make yourself familiar with the drone assembly points. The drone is outside – stay inside.

Prepare against Cyber Attacks

Drones may fake your wireless network!

- Clean your Wi-Fi List and delete all unsecured networks.
- Configure your mobile device so you have to confirm each connection attempt.



Visit www.japcc.org/drone-drills to learn more about drone threats and how to prepare for them.





Please visit

www.japcc.org/drone-drills

*to download customizable templates for the annexes included in this paper,
as well as additional educational references and materials.*



Drone: © AdobeStock, 260694458 (10 November 2023)

Imagery Front Page

Drone Evacuation Point Sign – Drone: © AdobeStock, 260694458 (10 November 2023); Shield: © Copyrighted; Group: FourLeafLover – stock.adobe.com; Arrows: © Copyrighted
Prevent Drone Observation (top/front view): © JAPCC; © Adobe (3D Objects)

Logo Headline – Shield: © Copyrighted; Drone Parts Next to Shield: © 1arts – stock.adobe.com
Lock/Mobile Arrangement: © Adobe

Do you know what to do when you spot a drone flying above you or outside your office window? Are you aware of the potential threats and hazards that drones can pose? Do you know the appropriate actions to take when encountering one? Furthermore, do you know how to protect yourself and what steps you can take to ensure the safety of those around you?

We recommend reading this paper if you find yourself seeking answers to these questions. It delves into the immediate actions individuals should take in the first few minutes of a drone incident before the arrival of the guard force, police, or other first responders. It's important to note that this paper does not focus on technically advanced countermeasures provided by professional C-UAS systems. Instead, its emphasis lies in guiding individuals on how to respond to a drone incident safely and effectively, much like administering first aid measures before the arrival of an ambulance or implementing evacuation measures before the appearance of a bomb squad.



Joint Air Power Competence Centre

von-Seydlitz-Kaserne

Römerstraße 140 | 47546 Kalkar (Germany) | www.japcc.org