ISSN 1831-9424

European Commission

Protection against Unmanned Aircraft Systems

Handbook on UAS risk assessment and principles for physical hardening of buildings and sites

JRC technical report

Karlos, V. | Larcher, M.

EUR 31458 EN

Joint Research Centre

Contact information

Name: Vasilis KARLOS
Address: European Commission
Joint Research Centre
Via Enrico Fermi, 2749
21027 Ispra (VA)
ITALY

Tel.: +39 03 32 78 59 34
Email: vasileios.karlos@ec.europa.eu
jrc-public-spaces@ec.europa.eu

EU Science Hub

https://joint-research-centre.ec.europa.eu

Data and Tools to Counter Terrorism

https://counterterrorism.ec.europa.eu

JRC132967
EUR 31458 EN

Print	ISBN 978-92-68-06615-7	ISSN 1018-5593	doi:10.2760/758582	KJ-NA-31-458-EN-C
PDF	ISBN 978-92-68-01267-3	ISSN 1831-9424	doi:10.2760/969680	KJ-NA-31-458-EN-N

Luxembourg: Publications Office of the European Union, 2023

How to cite this report: Karlos, V. and Larcher, M., Protection Against Unmanned Aircraft Systems – Handbook on UAS risk assessment and principles for physical hardening of buildings and sites, Joint Research Centre, Publications Office of the European Union, Luxembourg, 2023, doi:10.2760/969680, JRC132967.

Protection against Unmanned Aircraft Systems

Handbook on UAS risk assessment and principles for physical hardening of buildings and sites

JRC technical report

Karlos, V. | Larcher, M.

Contents

Abstract

The purpose of the current handbook is to provide guidance to security and law enforcement officials, building/site owners, venue organisers, state organisations, engineers and other stakeholders in charge of securing infrastructure and public spaces against the growing international threat posed by the malicious use of unmanned aircraft systems (UAS), commonly referred to as drones. The focus narrows down into recommendations for a robust and usable approach for the physical hardening of non-military infrastructures and public spaces against this borderless phenomenon. It addresses shortcomings encountered in the design of such security solutions and aims at producing a simple, self-contained guide to help select appropriate measures that are able to mitigate and/or deter potential attacks.

To help assess the relevant risk, a detailed analytical procedure is illustrated to identify the weaknesses of the potential targets and calculate the parameters that influence the likelihood of a UAS-driven attack taking place and its consequences. Despite the fact that intentional malicious use of drones is infrequent in Europe, the direct (e.g. injuries, fatalities, disruptions) and indirect (e.g. psychological, economic, political) consequences can be disproportionally high. As a result, a methodological approach is proposed that facilitates the development of attack scenarios depending on the vulnerabilities of the examined asset, assisting their comparison in terms of severity and probability of occurrence.

Advice is provided for the introduction of physical hardening measures that may effectively treat the evaluated threat. These measures range from physical protective measures to concealment or disguising efforts to make the target less attractive. Such an approach overcomes many of the legal and operational shortcomings of counter-UAS (C-UAS) technologies and provides a variety of methods for securing a site in an efficient, inexpensive, simple and multifunctional mode.

This handbook is a key component of the European Commission's C-UAS package initiative, announced as a flagship action under the Commission communication 'A drone strategy 2.0 for a smart and sustainable unmanned aircraft eco-system in Europe' [1]. This package includes a dedicated C-UAS communication (COM) outlining the main ideas for the EU's future policy on how to address the potential threats posed by UAS. As part of the COM's recurrent drive to provide continuous practical support to EU Member States and private stakeholders, JRC has produced two handbooks; the first concerns a five phase approach to evaluate the needs of a C-UAS solution and how to start, define risks, design, implement and operate it, while the second (current handbook) contains a series of recommendations for assessing the risk stemming from the malicious use of UAS complemented with advice regarding the physical hardening of non-military infrastructures against such threats.

1 'Flagship action 17: The Commission intends to adopt a counter-drone (C-UAS) package' in Commission communication – A drone strategy 2.0 for a smart and sustainable unmanned aircraft eco-system in Europe, COM(2022) 652 final.

Introduction

An unmanned aircraft system (UAS), commonly referred to as a 'drone', involves an aircraft that can operate in an automated manner or be piloted remotely without human presence on or in the aircraft, and also includes the ground control system and the system of data transfer that allows communication to take place between the remotely located operator and the drone. Even though drones were initially developed to be operated within a military context, they have gained popularity in the industry, business and consumer sectors due to their versatility, technological advancement and decreasing purchase cost. Their presence in the European skies has increased almost exponentially in the last years as they are used by industries for various activities, including topographical mapping, courier services, inspections, catering, surveillance, emergency response and marketing. Moreover, the sales of recreational UAS have been increasing rapidly, as the public has direct accessibility to a great number of affordable and reliable solutions that are marketed by producers as great tools for taking aerial photographs and video footage. Several new technologies have been expanding to the drone sector, such as the roll out of 5G networks, which allows faster and more robust communication to take place between the ground control systems and the drones, and the introduction of artificial intelligence, which enables UAS to process their surroundings, make real-time decisions while flying and provide instant feedback to the pilot. However, with the increasing number of UAS and the proliferation of technology, concerns have also risen regarding security-related threats.

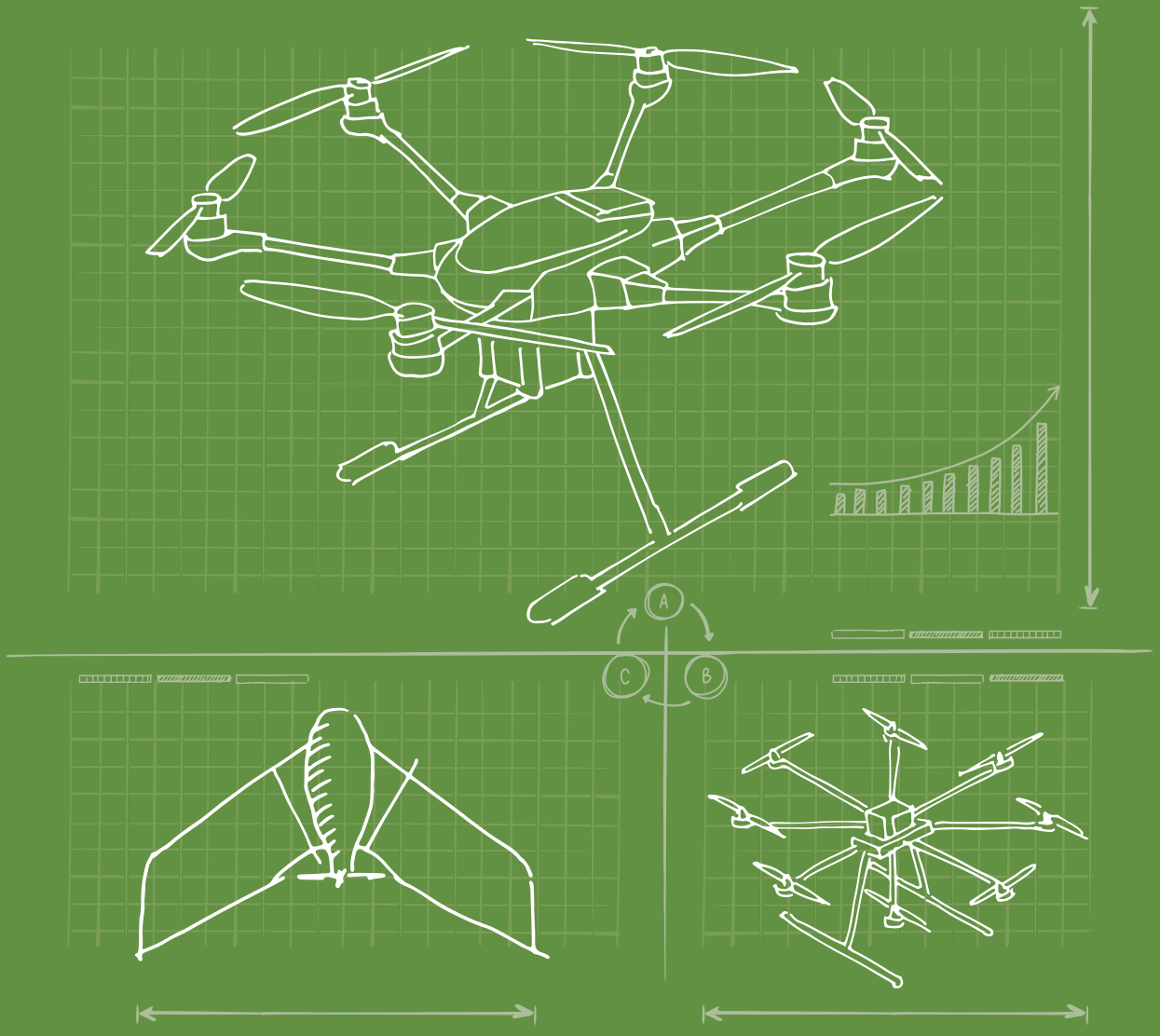
The military domain has embraced their use due to their certain advantages (e.g. remote command, cost-efficient, small size, no human pilot) that make them extremely efficient in a battlefield. As a result, drones have become a common weapon for many state and non-state actors, making their frequent presence in conflicts unambiguous. They already play a critical role in modern warfare, as they are used either for surveillance purposes or to perform air-strike attacks, functions that are expected to evolve even further in the future.

Over the last years, a great number of safety and security incidents concerning UAS have been reported in Europe, many of which are caused by actors with criminal or terrorist intent. Their direct availability, difficult detection (especially in an urban environment) and simple and remote piloting are characteristics that make them an attractive tool in the hands of aggressors who may use them for the smuggling of goods, privacy invasion, the disruption of services, spreading propaganda or even weaponising them with grenades, improvised explosive devices (IEDs) or chemical, biological, radiological or nuclear (CBRN) substances. Common examples include the transportation of illegal goods into prisons and across country borders, monitoring police activities, cyberattacks, privacy invasion through image and video recording and the disruption of manned air traffic. Moreover, several terror plots have been foiled in the EU over the last years that involved the use of UAS as part of the attack planning. Additionally, concerns have been raised regarding the data that are collected from UAS, such as images of critical infrastructures, and whether drone manufacturers have access to this type of information.

Tackling the security threats posed by the use of UAS for criminal and terrorist acts is extremely challenging, and a combination of different solutions may prove to be the most efficient approach. The EU has already taken concrete steps to address these pressing issues by incorporating UAS security threats in various documents, such as the action plan to support the protection of public spaces (European Commission, 2017) and the counter-terrorism agenda for the EU (European Commission, 2020), while research and innovation projects that examine UAS security-related issues have been granted several funds. Additionally, a dedicated European counter-drone programme was set out as a flagship action under the Commission communication 'A drone strategy 2.0 for a smart and sustainable unmanned aircraft eco-system in Europe' (European Commission, 2022). A legislative framework regarding pilot licencing and aircraft registration has also been set up, while efforts have focused on the integration of UAS traffic management into air traffic management.

Along with the proliferation of available UAS, a wide range of both sophisticated and simple solutions have been developed that are able to detect, identify, track, neutralise or mitigate the consequences of potential UAS-related threats. While striking the right balance among the different commercially available solutions is difficult to achieve, it is important for law enforcement agencies and site or event operators/owners to be aware of the capabilities, limitations and requirements of each measure. This handbook provides insight into the various physical hardening protective measures, focusing on their typology, performance, challenges and constraints, while elaborating on their suitability depending on developed threat scenarios. As will be demonstrated, most of the examined cases can also be used in civilian settings by private owners and entities without any legal restrictions. This poses a great advantage over many counter unmanned aircraft systems (C-UAS) technological state-of-the-art solutions that may be legally operated only by law enforcement units, which results in very prolonged reaction times in the event of a security-related incident.

1 UAS overview and categorisation

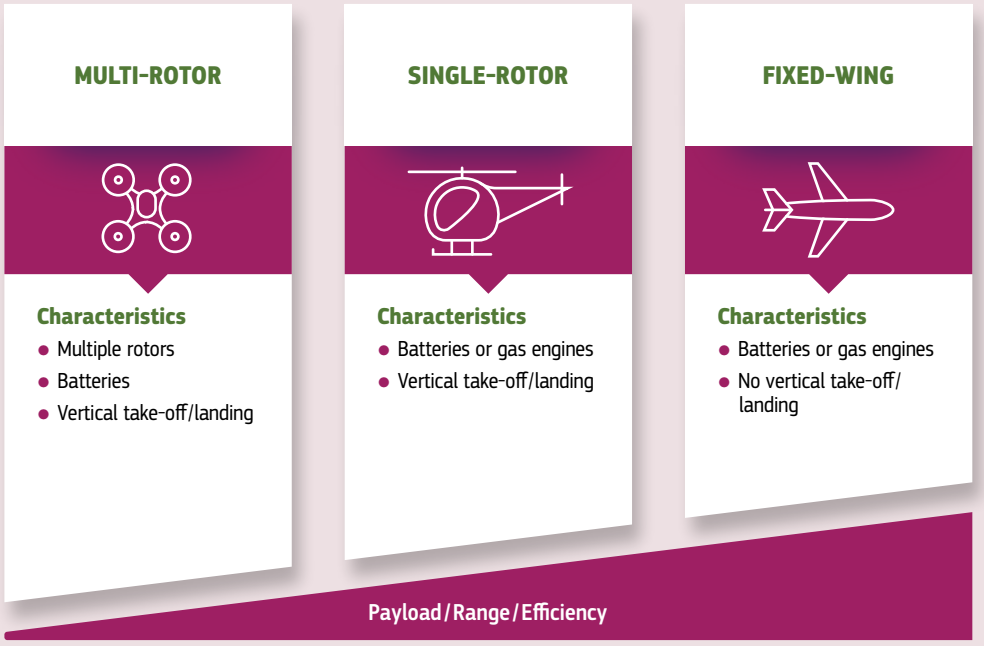


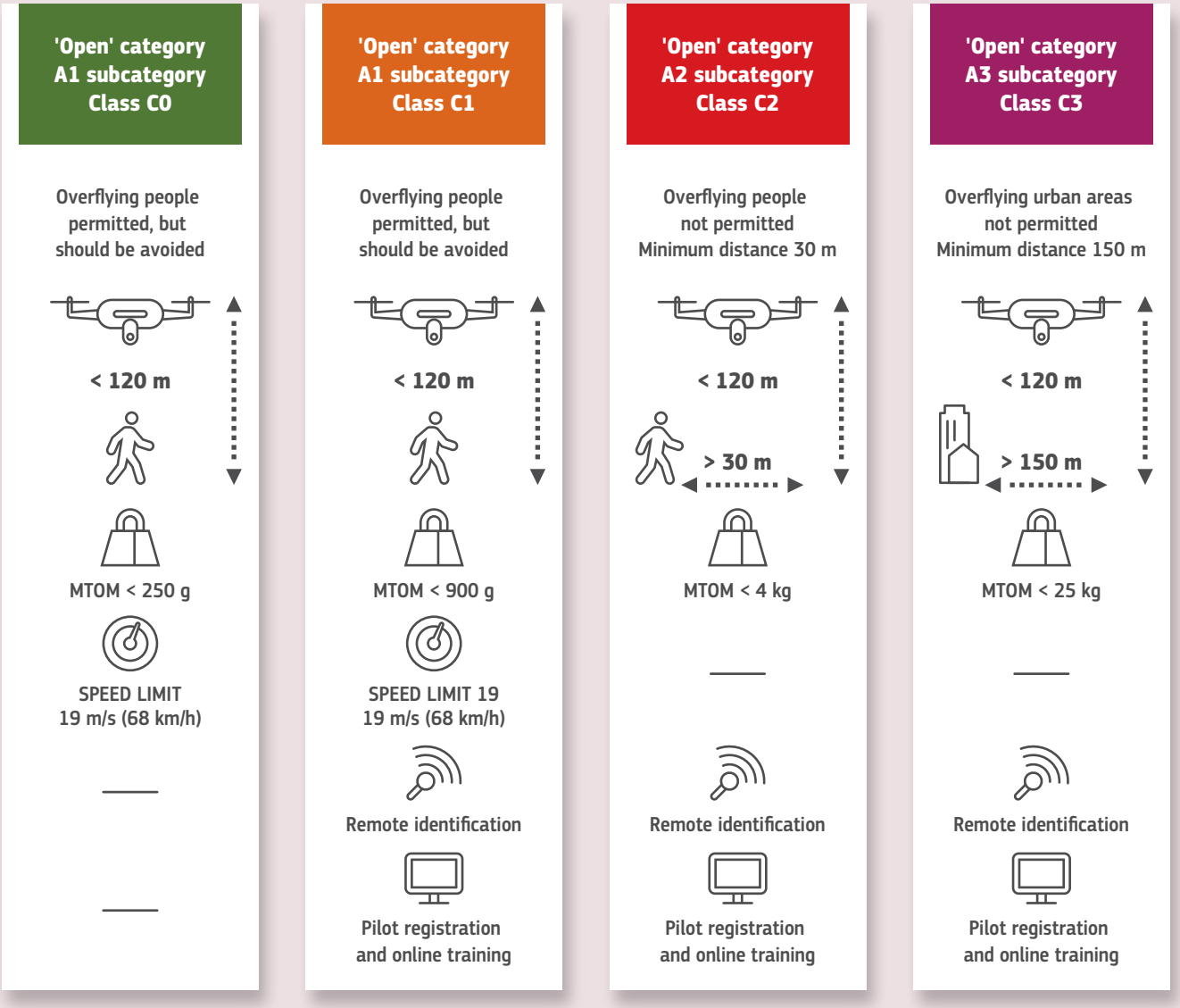
The simplicity, adaptability and relatively low cost of UAS has led to their wide use in various sectors and for a plethora of different applications. Their design and capabilities play an important role during the development of potential attack scenarios and therefore for the establishment of a protection strategy, as countermeasures are rarely effective against all UAS types. For instance, their flight capabilities – including maximum payload, endurance, range, manoeuvrability and velocity – can greatly affect the potential consequences on a non-cooperative intrusion, since their intentions remain unknown.

The main UAS categories are the vertical take-off / landing systems (which come with rotary-wing configurations) and fixed-wing systems. The vertical take-off / landing solutions have become the most popular category due to their adaptability in urban environments, their hovering potential and ability to take off from practically anywhere. They are usually powered by on-board battery packs or even internal combustion engines and have a maximum take-off mass (MTOM) that includes their payload capacity, body and motors. The MTOM is an important parameter to be considered during the generation of potential attack scenarios incorporating the transportation of hazardous loads. The flight time ranges greatly, depending on the drone type (e.g. fixed-wing systems equipped with combustion engines can travel for hours) and the transferred payload (the greater the load the smaller the flight time).

In response to the safety and security issues posed by the proliferation of the UAS use, the Commission adopted a number of regulations that set common rules for their operation and design. As a result, Regulation (EU) 2018/1139 established three operational categories (open, specific and certified) with respect to the risk level. In 2019, two Commission regulations set out the design and manufacturing requirements of UAS (EU 2019/945) and the provisions for their use (EU 2019/947). These regulations also propose a UAS categorisation system depending on the MTOM, the maximum attainable speed and the maximum height above take-off point, and they describe detailed operational and technical rules that have to be followed by manufacturers, operators and EU Member States. Of particular concern for security purposes are the UAS included in the ‘open/low risk flights’ category as they are also intended for use by the general public. Figure 1 shows an overview of the UAS characteristics and the limits that have to be respected by the operators and manufacturers. Additionally, a better focused C-UAS action was announced by the Commission through the communication ‘A drone strategy 2.0 for a smart and sustainable unmanned aircraft eco-system in Europe’ (European Commission, 2022).

Figure 1: UAS general characteristics and UAS 'open' category main operational requirements according to regulations (EU)2019/945 and (EU)2019/947





2 Risk assessment

2.1 OVERVIEW

A risk assessment within the security domain aims to identify the kind of threats we should consider, build attack scenarios, determine vulnerabilities, estimate the likelihood of occurrence of terrorist or malicious acts and evaluate their potential consequences. The assessed risk can subsequently be treated during the risk-management stage through appropriate intervention actions, including prevention, mitigation, preparedness, recovery and reconstruction or adaptation. Intentional malicious use of UAS is infrequent in Europe and, in the majority of cases, licensed users respect existing UAS rules, regulations and technical limitations. Nevertheless, clueless and careless individuals are responsible for the majority of incidents involving drones, while the intent for criminal and terrorist activities should not be overlooked. The disturbances caused by such events is of particular importance for public spaces, critical facilities and the citizen's right to privacy.

- **Clueless users:** are unaware or misinterpret existing regulations and restrictions.
- **Careless users:** are aware of existing regulations and restrictions but disregard them by fault, negligence or deliberately.
- **Criminal users:** despite being aware or not of existing regulations and restrictions, they deliberately use UAS to achieve their goals.

The advancing capabilities of drones raise serious security concerns in Europe, so a comprehensive understanding of the parameters that influence the likelihood of manifestation of a security-related incident and the potential consequences from an attack is required to establish a robust risk assessment and risk-management framework. Independent of their rarity, their direct consequences (e.g. injuries, fatalities and disruptions), and even more so their indirect consequences (e.g. psychological, economic and political), can be disproportionally high.

In this section, the proposed structured approach to assessing the risk related to UAS-driven attacks is based on the International Organization for Standardization (ISO) 31000:2018 standard's generic definition of risk assessment: 'Risk assessment is the overall process of risk identification, risk analysis and risk evaluation'. Such a description aims to incorporate both natural and human-induced hazards in the risk process, even if there are still major challenges when it comes to estimating the likelihood of rare human-induced events and quantifying the consequences in the human/social domain.

The malicious use of UAS that is analysed herein is only one of the means that may be employed by aggressors when targeting an individual, public space or infrastructure. Nevertheless, different attack tactics that take advantage of the UAS' distinct capabilities may be distinguished. To facilitate the evaluation, the development of attack scenarios is proposed depending on the vulnerabilities of the examined asset and the employed tactic. Figure 2 shows the distinct analysis stages that comprise the risk-assessment process.

- **Threat identification** involves identifying potential means and methods of attack and includes the assessment of current (if any) protective measures, the identification of vulnerabilities in the examined asset against the considered UAS attack tactic and the production of attack scenarios.
- **Risk analysis** includes assessing the likelihood and potential consequences of the occurrence of the identified attack scenario.
- **Risk evaluation** includes assessing the level of risk and deciding whether it is acceptable or not.
- **Risk treatment** includes describing and, if deemed appropriate, selecting potential measures for reducing the assessed risk.

Figure 2: Stages of the risk-assessment and management process

The result of the risk assessment may differ substantially depending on the background and the goals of the expert who is performing the assessment. If there are insufficient data to evaluate the attack scenario likelihood and the resulting consequences, experts may adopt qualitative methodologies and use their own judgement to assess the risk. Therefore, to reduce bias, experts need to have certain characteristics, such as clear evidence of expertise in conducting terrorism risk assessments, no conflicts of interest, impartiality and impeccable reputation. The risk-assessment results are subsequently communicated, usually accompanied with instructions for their precise interpretation, to the owners/operators of the examined asset who are responsible for establishing the acceptable risk level limits and decide if risk treatment is required.

2.2 IDENTIFICATION OF MALICIOUS UAS USE

The first step in the risk-assessment process is the identification of the terrorism threats that are relevant to the asset under evaluation. Threat identification focuses on pinpointing tactics that aggressors may use and on formulating possible attack scenarios. A threat is exerted on a target – that is to say on a person or a group of people, property, information or, more broadly, an institution, a state or a group of states. Identifying man-made threats and their likelihood of materialising is a challenging task, since, contrary to natural hazards, available data are scarce and therefore a large degree of subjectivity is usually involved when trying to link a specific threat to a potential target. Data relating to current and emerging threats, the intent of an attack and other related sensitive information may be requested from intelligence services and law enforcement units. Various commercial data providers may also have such information, but the quantity and quality of these data is not always guaranteed, especially at a local level. More information on available data sources that can facilitate the identification of threats may be found in Security by Design: Protection of public spaces from terrorist attacks (European Commission, 2022).

In this publication, the focus is on the different tactics that may be employed by an individual who has already resolved to use a UAS either as a means to transport hazardous/illegal loads or as a weapon. As already noted, their small size, easy acquisition and modification potential makes them an ideal tool both for professionals and amateurs, but also for actors with malicious intent, and, as a result, increases the relevant safety and security risks. Clearly, the majority of UAS users are compliant with the rules that have been described (as long as they are aware of them), which means that they do not pose a security threat. On the contrary, actors with malicious intent operate UAS in a non-collaborative

way and may target different assets with a varieties of motives. The tactic used depends on the type of target, its vulnerabilities and the purpose of the actor. Therefore, selecting appropriate countermeasures that provide effective protection of the target's valuable assets (e.g. persons, very important persons (VIPs), data) require the consideration of a plethora of different attack scenarios. The key threat categories that have been identified in recent years in a non-military context include the following.

- **Transfer of hazardous loads.** As the payload capacity of UAS has been increasing over the last years due to more efficient motors and batteries, they can be easily used for transferring an IED, grenades or CBRN substances within a secured perimeter. Modern UAS are able to carry substantial loads at great distances with increased accuracy through the use of cameras and geographical information system devices, as has been demonstrated on modern battlefields. The load may be placed at a point of interest, which could be at an elevated position (e.g. building's roof), be released through a specially designed mechanism or triggered while in mid-air, sacrificing the UAS. The UAS may even be deliberately piloted against an exposed facility in a 'kamikaze' attack type. Potential targets include the public (e.g. in an outdoor space), a specific individual (e.g. triggering the payload outside an office or a vehicle), compromising information storage facilities or the services offered by an asset (e.g. energy, economy, administration, defence). Moreover, the UAS may be weaponised by means of a firearm (or other projectile weaponry) specifically targeting individuals (usually a VIP) and having the ability to easily approach the target.
- **Smuggling/delivery.** The use of UAS for delivering equipment at specific locations has already been observed in a number of cases across Europe, since they can easily bypass traditional control points and specifically protected areas. The delivered equipment (e.g. firearm) may come into the possession of and be used by an aggressor who has already entered the secure area through the normal control procedure. For instance, a variety of different payloads (e.g. mobile phones, drugs, illicit goods, weapons) have already been delivered in prisons or smuggled across international borders.
- **Intelligence, surveillance and reconnaissance.** UAS may also be used to collect information and observe activities, mainly through the use of cameras. The increasing technological capabilities of cameras allows for operations during night-time or observation of human motion through thermal sensors. This enables aggressors to document the vulnerabilities of a potential target from a safe distance and exploit them during the planning of an attack, or even provide real-time information while the strike is taking place. Lately, powerful microphones have also being developed that allow eavesdropping of private/confidential conversations to take place. Moreover, private images captured by a drone invading the privacy of individuals may be used for criminal purposes, such as fraud or blackmail.
- **Cyberattacks.** A UAS can pose a cybersecurity threat by targeting local wireless networks and disrupting communications, delivering malware, hijacking and/or manipulating sensitive data. This can be performed if it is equipped with appropriate gear (e.g. network or radio frequency (RF) scanner) and manages to gain access to the wireless system by exploiting its vulnerabilities. Moreover, a UAS may be the target of a cyberattack (a.k.a. UAS hacking), as aggressors may gain control over it and alter its route, access its data or destroy it (e.g. spoofing, tampering and denial of service).

- **Jamming.** A UAS mounted with an appropriate electronic equipment may be used as a local jammer to interfere with perimeter security systems, GPS systems or mobile phone signals. This tactic can create additional vulnerabilities that can be exploited by an aggressor or even have a significant effect on the operations of the asset (e.g. airport).
- **Disruption and interference.** Even the presence of a UAS may be enough to interfere with the normal operations of an asset due to the safety issues that are raised from such an action (e.g. interference with civil aviation). Various types of mass events in urban areas may also be disrupted, initiating panic reactions from the attending public, which could lead to injuries/victims or create favourable conditions for a secondary attack (e.g. channel people into specific locations). Moreover, even without carrying any hazardous payloads, a UAS may cause injuries or damage if it crashes on the public or against a structure, usually in an unintentional manner.
- **Propaganda.** UAS may also be used by protesters and terrorist groups to record their actions, spread leaflets or other material in public spaces in an effort to reinforce their propaganda efforts. The filmed content may be broadcasted online (even in live-streaming mode) to attract sympathisers and encourage the recruitment of new terrorists or protesters, as it portrays the picture of a successful organisation with determined members.

These threat categories, which are summarised in Figure 3, are certain to evolve in the future, as many technologies associated with drone use are still progressing, while their commercial, professional and recreational use is expected to increase. Improved batteries and motors will mean longer flight time, elevated payload capabilities and greater range, while faster mobile networks (5G) and artificial intelligence applications will allow for long-distance communication and enhanced cooperation among drones forming a swarm.

Figure 3: Potential UAS threats in an urban context

2.3 UAS RISK ANALYSIS

2.3.1 Likelihood identification

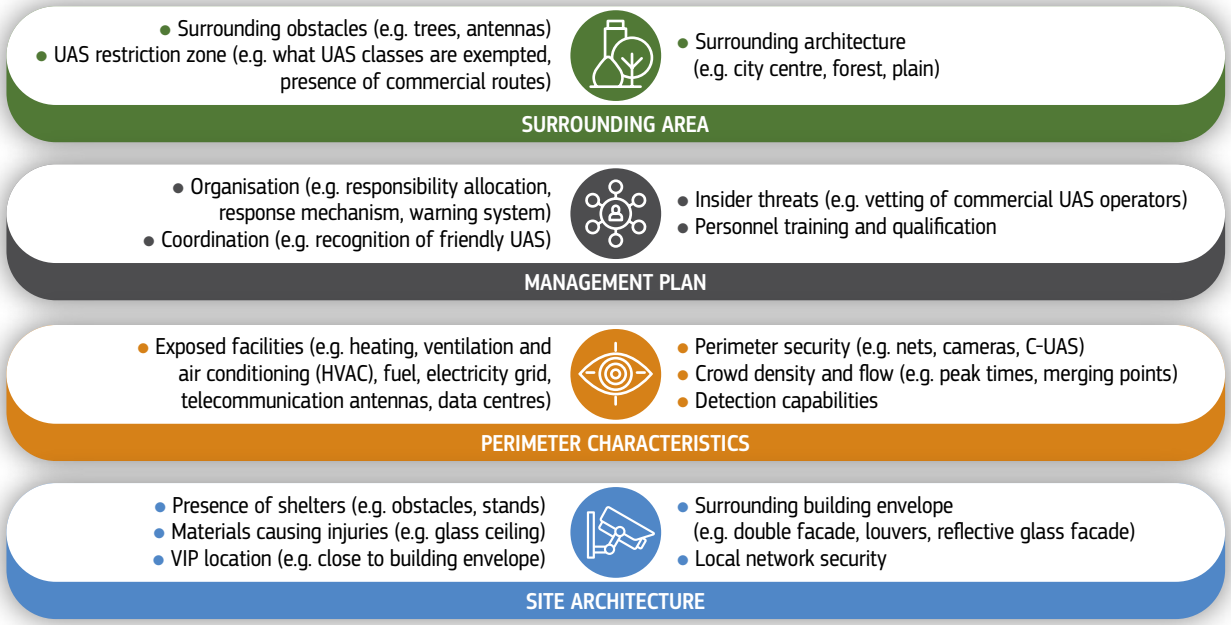
2.3.1.1 Vulnerability identification and attack scenario development

Vulnerabilities are the inherent weaknesses of potential targets that may render them susceptible to the consequences of a terrorist attack. Critically assessing vulnerabilities in the context of attack scenarios will assist decision-makers in taking informed decisions on deterrence and mitigation measures, designing strategies to minimise exposure and developing an effective emergency management plan. Attack scenarios are a practical way of illustrating what could occur in the future and can prove beneficial, as they follow possible events to be envisaged by making carefully considered assumptions. Building an attack scenario involves describing the incident and the modus operandi of the attackers, considering the general circumstances prevailing at the time of the assault, identifying vulnerabilities and helping to evaluate potential consequences. It is clear that all attack scenarios are plausible, but they differ in their likelihood of occurrence. Each developed scenario needs to be as specific as possible, taking into account any measures that are already present, and have a schematic structure that facilitates the deduction of educated decisions on potential required actions. It may differ in terms of tactics, severity, extent and impact, and is established for a limited period (e.g. the next 3 or 4 years), as it needs to be reassessed regularly to integrate newly acquired knowledge, trends and rapid technological developments.

Identifying the UAS-related vulnerabilities of an infrastructure or public space requires the examination of factors such as its accessibility, location, shape and existing protective measures (entry checks, video surveillance, UAS detection and identification equipment, security guards, perimeter physical protection, interception measures, etc.). Protective measures, if they exist, need to be identified, appraised and improved if deemed insufficient and outdated for UAS emerging threats. Such careful consideration can reveal residual risks owing to the insufficiency of the adopted solutions and/or their poor implementation or operation. Alternatively, the ineffectiveness of current measures may be attributed to unsatisfied technical requirements (e.g. technological limitations), lack of compliance with the manufacturer's operational guidance, equipment failure, insufficient equipment maintenance, insufficient operator training, a shortage of personnel or insider threats. Moreover, existing measures, if properly applied, can significantly reduce the required budget for upgrading the asset's security plan.

Figure 4 shows an example of the main fields that need to be examined in order to perform an educated vulnerability assessment. Such an assessment is usually assigned to qualified experts who have the required expertise to identify and document vulnerabilities in these areas, which are an essential element of the risk-assessment process.

Figure 4: Example of UAS-related vulnerability categorisation



The results of the vulnerability assessment may be presented in the form of a rating system as presented below, to provide visual aid during the risk-assessment process.

Table 1: Vulnerability assessment rating

Vulnerability rating	Description
Very low	A variety of protective measures (e.g. detection, mitigation, interception) are present providing sufficient protection against the examined attack scenario.
Low	Several protective measures (e.g. detection, mitigation, interception) are present, though some weaknesses have been identified that may be exploited by an aggressor using the examined attack scenario.
Medium	Some protective measures (e.g. detection, mitigation, interception) are present, though considerable (e.g. lower protection than anticipated) weaknesses have been identified that may be exploited by an aggressor using the examined attack scenario.
High	Existing protective measures (e.g. detection, mitigation, interception) are insufficient (e.g. ineffective systems) and aggressors may easily exploit the identified weaknesses.
Very high	Protective measures (e.g. detection, mitigation, interception) are either missing or are highly insufficient (e.g. completely ineffective systems) and aggressors may very easily exploit the identified weaknesses.

2.3.1.2 Threat assessment at a local level

The introduction of a universally accepted methodology for calculating the likelihood of occurrence of a specific attack scenario is problematic because attacks are frequently of opportunistic character and available data are usually insufficient, especially since they are considered sensitive and are commonly retained by intelligence agencies. The lack of precise quantitative methodologies on determining the probability of an incident occurring has led to the adoption of qualitative evaluations, despite the inherent large amounts of subjectivity and bias. To reduce this subjectivity margin, a number of indicators related to the characteristics of each examined asset have been introduced and are analysed in detail in Security by Design: Protection of public spaces from terrorist attacks (European Commission, 2022). The process analysed in this publication provides the risk levels of assets and public spaces for a large number of different threats (e.g. firearms, vehicle ramming, IED and UAS).

In this handbook, the focus is exclusively on the malicious use of UAS and the different tactics that stem from their use, as described earlier. This means that the proposed analysis takes for granted that the aggressor intends to use a UAS to conduct an attack against a specific target, thereby excluding other types of threats (e.g. vehicle ramming, active shooter) and other targets. Since the type of threat (i.e. use of UAS) and target are preselected, the recommended approach emphasises the importance of devising well-established attack scenarios utilising the different tactics presented in Figure 3, and finally assessing each scenario's relative likelihood of unfolding. The likelihood is classified as relative, as it is only compared in relation to other UAS-driven tactics against a predetermined target.

To quantify the relative likelihood of each attack scenario that is developed, the threat level in the area surrounding the examined potential target needs to be assessed – a challenging task since relevant data are usually scarce and are often unavailable due to their sensitive nature. To facilitate such an assessment, a limited number of indicators from the abovementioned publication are selected, considering only those the value of which differentiates depending on the UAS-related tactic used. The introduced simplified approach aims to assist stakeholders in the preliminary assessment of the relative threat, should a more precise evaluation from the intelligence services or relevant authorities be missing. Herein, the examined indicators for each UAS threat category are the following.

- **Threat history.** Examines information regarding previously reported, failed or foiled attacks/threats with each specific tactic (to the building or its users or in similar facilities). Considers public statements made from terrorist groups against civil targets and their motivations, especially if preference is exhibited on the examined attack scenario.
- **Attack complexity/capability.** Estimates the practical/technical expertise the aggressor would require to perform the UAS-driven attack (e.g. creating an IED or CBRN substance), and the difficulty in obtaining the UAS (e.g. depending on its size), the weapon or the components for its creation. Examines the financial resources required for acquiring the materials and other essential elements that might be needed (e.g. supporting infrastructure, communications network, supply chain).
- **Attractiveness/motivation.** Depends on the target attractiveness (e.g. cultural/religious/symbolic significance, people attendance) related to the potential attack tactic. It investigates if a certain modus operandi seems more attractive to the eyes of the attacker because it could have a greater impact due to the asset's functions (e.g. interdependencies with other facilities, collateral consequences for the state and society, public and/or sensitive data presence).

Table 2 presents in detail the introduced indicators and the scoring criteria to be followed when allocating the points. Nevertheless, these scoring criteria do not cover all the different factors that may be used to characterise the threat rating of a specific UAS-driven attack tactic against an asset.

Table 2: Scoring criteria per indicator

Indicators	Allocated points	1	2	3	4
	Threat history	• No previous threats/ statements • Past international security incident	• Threats/statements at an international level • Past national security incident	• Threats/statements at a national level • Relatively recent regional security incident	• Threats/statements at a local level • Recent local security incident
	Attack complexity/ capability	• Advanced expertise required • Very difficult to produce/acquire weapon • High cost of materials • Great number of resources required	• Expertise required • Difficult to produce weapon • Relatively high cost of materials • Significant number of resources required	• Low expertise required • Easy to produce weapon • Low cost of materials • Small number of resources required	• No expertise required • Readily available weapon • Very low cost of materials • Minimum number of resources required
	Attractiveness/ motivation	• Insignificant impact at national level in the event of an attack • Very small potential collateral damage (e.g. adjacent facilities) • Unattractive target	• Some impact at national level in the event of an attack • Low potential collateral damage (e.g. adjacent facilities) • Low target attractiveness	• Significant impact at national level in the event of an attack • Moderate potential collateral damage (e.g. adjacent facilities) • Attractive target	• Very big impact at national level in the event of an attack • High potential collateral damage (e.g. adjacent facilities) • Very attractive target

To determine the relative threat rating of an asset against a specific UAS-driven attack tactic, the points assigned to the abovementioned indicators are added together and compared with the scale provided in Table 3. This procedure needs to be repeated for each individual scenario to obtain a comparison among the different identified tactics. In addition, the credibility of each scenario is ideally verified by intelligence services and law enforcement units, as they may be able to provide additional information on known threat sources and emerging trends of terrorist activities

Table 3: Assessment of relative threat rating

Threat rating	VERY LOW	LOW	MODERATE	HIGH	CRITICAL
Total score (points sum)	3–4	5–6	7–8	9–10	11–12

2.3.1.3 Likelihood assessment

To determine the criticality and the risk level of an asset against the malicious use of drones, the assessor has to first evaluate the likelihood of occurrence of each identified scenario and the potential consequences if this scenario materialises. Such a process uses the results of the threat and vulnerability assessments that were presented above. Table 4 provides a five-level estimate of a UAS-driven attack likelihood of occurrence and is required to be developed for every potential modus operandi.

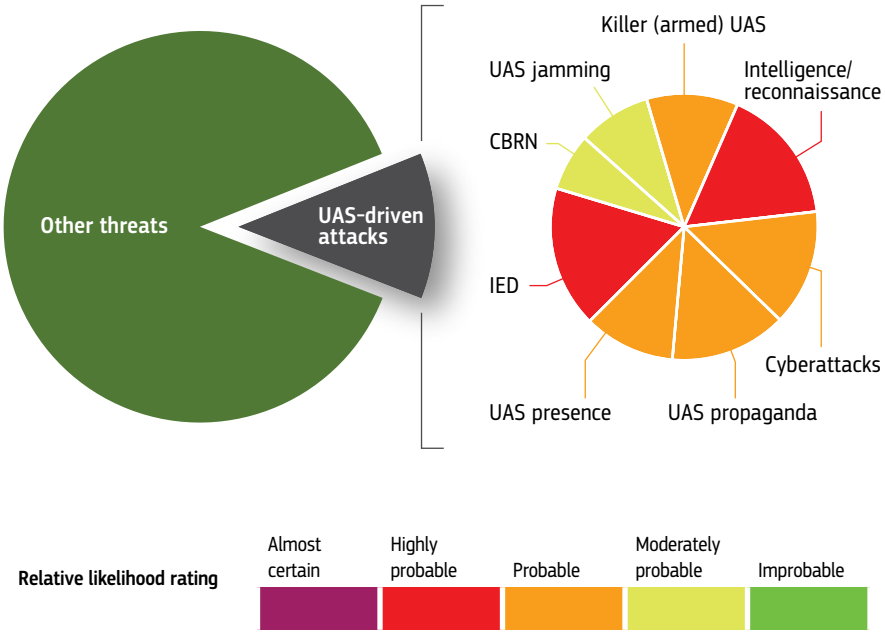
Table 4: Relative likelihood assessment of UAS-driven attacks

Threat \ Vulnerability	Very high	High	Medium	Low	Very low
Critical	Almost certain	Almost certain	Highly probable	Probable	Probable
High	Almost certain	Highly probable	Probable	Probable	Moderately probable
Moderate	Highly probable	Highly probable	Probable	Moderately probable	Moderately probable
Low	Highly probable	Probable	Moderately probable	Moderately probable	Improbable
Very low	Probable	Probable	Moderately probable	Improbable	Improbable

Relative likelihood rating: Almost certain | Highly probable | Probable | Moderately probable | Improbable

The end result of such a process will be similar to the example shown in Figure 5, which graphically demonstrates the relative likelihood of the previously identified UAS attack tactics against the examined site. From the image, it is clear that some UAS attack tactics have a higher relative likelihood of materialising than others, a valuable element for prioritising tactic-specific mitigation options.

Figure 5: Relative likelihood for UAS-driven attack tactics



2.3.2 Consequences assessment

The consequences of an attack are directly linked to the type of the targeted asset and the conditions at the time of the assault. Past incidents have demonstrated that the direct, immediate repercussions of an attack range from effects on human life (e.g. injuries or fatalities) to major economic losses (e.g. repair costs and disruption of services) and environmental disasters. Indirect, long-term consequences are more difficult to assess, as they include political/social aspects such as the effects on the population's psychology and (indirect) economic costs, for example, the impact on the tourism industry or the reputation of an institution/company. Despite the difficulty in precisely quantifying several of the consequences of the reasonable worst-case scenario of each type of modus operandi (especially those related to psychological reactions), an evaluation of potential immediate economic losses, property destruction, supply chain disruptions and loss of human lives are an important element of the risk-assessment process. To facilitate this evaluation, the assessor has to respond to a number of questions, including the following.

- How many people may be killed or injured after an attack with a UAS-driven tactic?
- What services may be disrupted if there is an attack? How long will the disruption last? Are there any backups for the services and how much will the repairs cost?
- Are there any cascading effects through interconnections with other assets or services?
- What are the expected costs of repairing infrastructure damage? Are replacements available?
- Does the asset include critical utilities or sensitive information that may be compromised? What are the repercussions of their loss or their disruption of service?
- Is there a possibility of any political consequences, reputational damage to the organisation/owner and/or security breaches (e.g. personal data breaches)?
- What are the indirect economic costs (e.g. to the tourism industry) and what are the consequences for the population's psychology?

Table 5 displays a classification depending on the potential consequences of the malicious use of a UAS. Several parameters are considered, including (but not limited to) human life, the economy, society, the environment and infrastructure damage. Their assessment is based on the reasonable worst-case scenario and may require intense scientific analyses, which means that the expertise of the assessor may significantly improve the accuracy of the results. The description and severity of the consequences that result in the assigned rating level may differ from those illustrated in the table, as they depend on the examined asset and its significance. It is therefore recommended that the owner/operator of the asset be consulted first and eventually revise and adapt the proposed rating included in Table 5.

Table 5: Consequences rating

CONSEQUENCES	DETAIL
INSIGNIFICANT	• No injuries or data leakage • No structural/material damage • No disruption of activities • Very small reputational damage • No economic impact and no indirect (e.g. psychological) consequences
MINOR	• Minor injuries • Minor structural/material damage • Short-term disruption of services • Small reputational damage • Limited economic impact and indirect (e.g. psychological) consequences
MODERATE	• Injuries (no life loss) • Moderate structural/material damage (does not pose a danger to structure's stability) • Medium-term disruption of services • Significant reputational damage • Considerable economic impact and indirect (e.g. psychological) consequences • Security breach that does not affect normal operations
CRITICAL	• Potential loss of life and serious injuries • Substantial structural/material damage (does not pose a danger to structure's stability) • Long-term disruption of services requiring immediate corrective actions • Extensive reputational damage • High economic impact and important indirect (e.g. psychological) consequences • Security breach that has direct consequences for the operations
CATASTROPHIC	• Extensive loss of life / serious injuries • Extensive structural/material damage requiring immediate intervention • Extensive reputational damage (VIP involvement) • Unacceptable long-term disruption to business operations • Very high economic impact and severe indirect (e.g. psychological) consequences • Total loss of services • Severe political consequences

2.4 RISK EVALUATION

At the end of the analysis phase, the outputs may be communicated in the form of maps, curves, indicators, matrices or other appropriate visualisation methods. The most commonly adopted method is a matrix, with the relative likelihood of the examined attack scenario on one axis and the expected consequences on the other, as the one shown in Table 6.

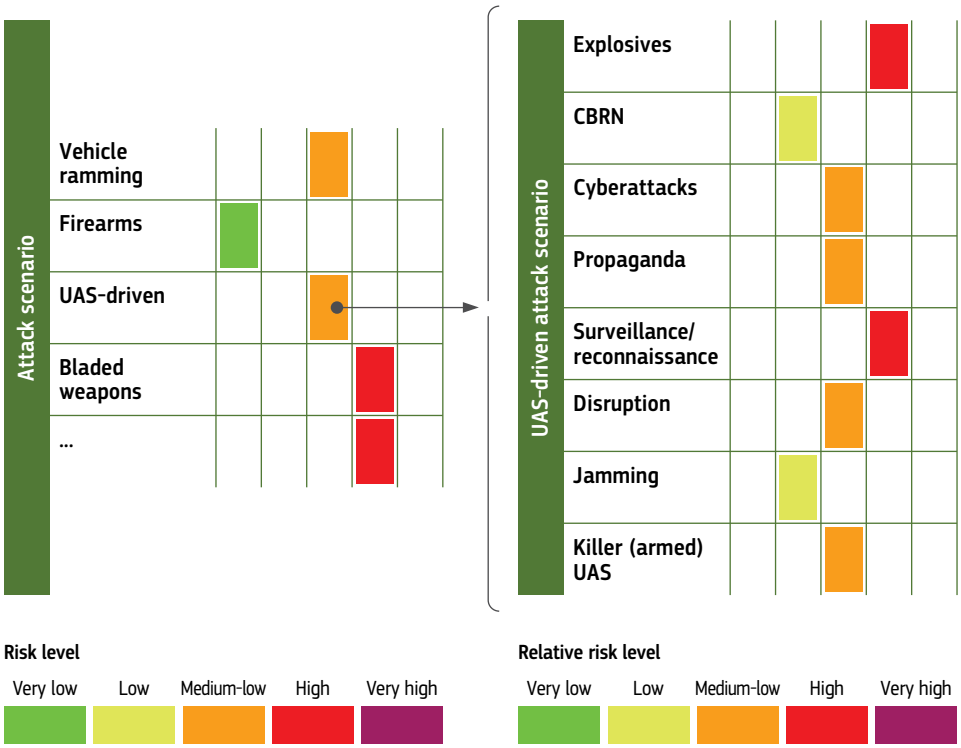
Table 6: Relative risk matrix

Relative likelihood	Consequences: Catastrophic	Critical	Moderate	Minor	Insignificant
Almost certain					
Highly probable					
Probable					
Moderately probable					
Improbable					

Relative risk levels	Very high	High	Medium low	Low	Very low

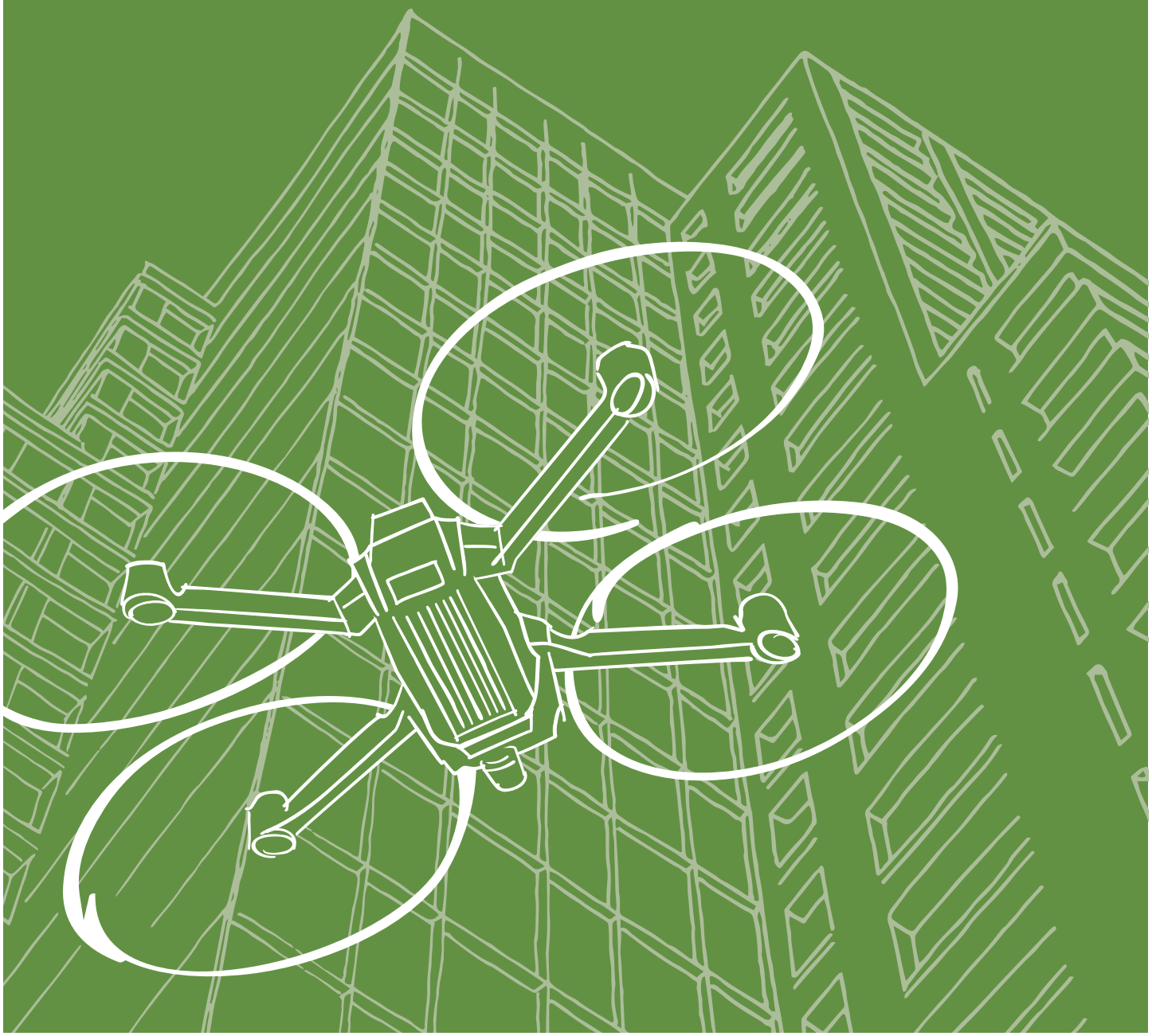
The result of the presented risk analysis is similar to the example in Figure 6, which demonstrates the fictitious relative risk for the identified UAS-driven attack tactics. The image in this example shows that drone attacks are only one element of the overall risk of a terrorism scheme, which considers additional attack scenarios, including (but not limited to) vehicle ramming, shootings and bladed-weapon attacks. Nevertheless, the currently proposed process is valuable for determining the relative risk of the different UAS-related attack scenarios, providing information to the interested stakeholders regarding the prioritisation of adopted (if deemed required) protective measures.

Figure 6: Example of relative risk for UAS-driven attack tactics



The outcomes of this analysis serve as input for comparing the different attack tactics and deciding the appropriate actions that may be deemed as required. They may also highlight where higher-order (quantitative) methods, such as a cost-benefit analysis, are desirable to help prioritise mitigation options when there is a high level of risk (European Commission, 2022). As the conductor of the risk analysis in the majority of cases is not responsible for deciding on the required actions, special care is needed to properly communicate the results to the decision-makers. Interpreting the results can be made easier for non-experts through clear instructions, which highlight the degree of uncertainty that is, inevitably, a component of the terrorism risk analysis.

3 Physical hardening against UAS-related threats



3.1 COMPARISON WITH C-UAS TECHNOLOGIES

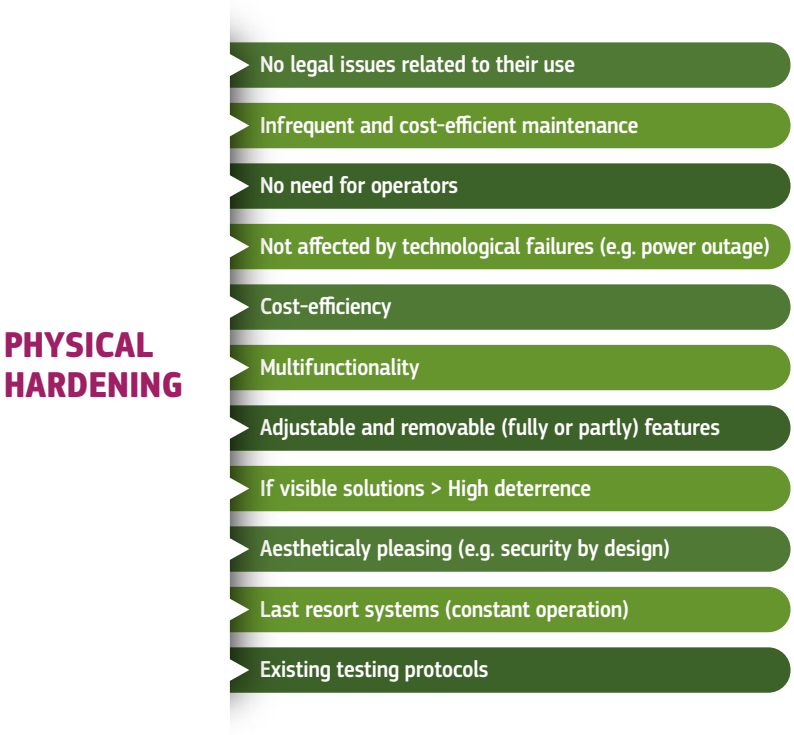
The consideration of UAS as a potential threat for non-military buildings and public spaces is relatively new, emanating from the great proliferation of such systems in the civil domain. Traditionally, physical hardening focuses on attack scenarios, where aggressors try to gain access into a building or cause damage using ground attacks. This means that in facilities potentially exposed to terrorist attacks, protective measures have been adopted mainly for the bottom floors, as the higher building levels were considered either inaccessible or with relatively low consequences. The destructive potential of air attacks with the use of UAS and the escalation in autonomous systems has led security officials to take into consideration new attack tactics and revise their response options. Through the employment of UAS, aggressors now have the opportunity to access building areas that were considered inaccessible when taking into consideration ground attacks only, such as interior courtyards, atriums, upper floors and proximity to VIP areas and offices.

Through the risk assessment that was presented in Section 3, asset vulnerabilities can be identified and provide insight about appropriate mitigation strategies. The majority of physical protective security measures that will be presented herein have not been developed specifically for attacks with the use of UAS, but are also efficient against such threats. These physical protective measures may focus not only on hardening, but on concealment or disguising of the asset in order to obstruct direct views or make it less attractive. Figure 7 summarises some of the main advantages of physical protective security measures in terms of cost, usability and effectiveness.

The use of many C-UAS solutions are prohibited for private stakeholders, as their operation is reserved exclusively for law enforcement units. Consequently, in the event of an unexpected security incident, private operators cannot rely upon swift police force intervention as its reaction time may be too slow, considering that drones can cover large distances in a matter of seconds. On the other hand, the adoption of physical security measures is generally not restricted to specific entities and there are no legal issues regarding their use. Since they usually lack electronic and/or moving parts, they require limited and relatively low-cost maintenance and there is no need for dedicated operators to activate them, after evaluating (usually within seconds) whether an approaching UAS poses a threat. This also means that these systems are not affected by potential failures of electronic parts and are not dependent on electricity or other energy sources to operate, so they are not affected by power outages.

One of the most important aspects of physical hardening measures is their multifunctionality, as each solution may be effective against various UAS attack tactics. The majority of these measures are economical, if compared to C-UAS technologies, and since they serve multiple purposes and their expected benefits are numerous, the initial cost might be easier to justify. Moreover, many of the proposed solutions are not of permanent nature and can be easily removed if the risk level decreases or if an alternative protective approach is selected in the future. Their constant operation and passive nature means that they can be easily combined with other C-UAS solutions and act as last resort systems if other measures fail to intercept a malicious UAS. If visible, they may also be harmoniously integrated into the surrounding space in line with the security-by-design principles, despite their high deterrence potential.

Figure 7: Typical characteristics of physical hardening measures



UAS misuse can take various forms, such as being weaponised and strapped with explosives, used for reconnaissance and spying, smuggling items in prisons, perform cyberattacks or support propaganda campaigns. More information regarding attack-scenario building and the risk-assessment process is analysed in Section 3. In the next sections, physical hardening measures that are effective against different attack tactics will be presented, providing advice on installation procedures and the established protection level.

3.2 OUTLINE OF C-UAS TECHNOLOGIES

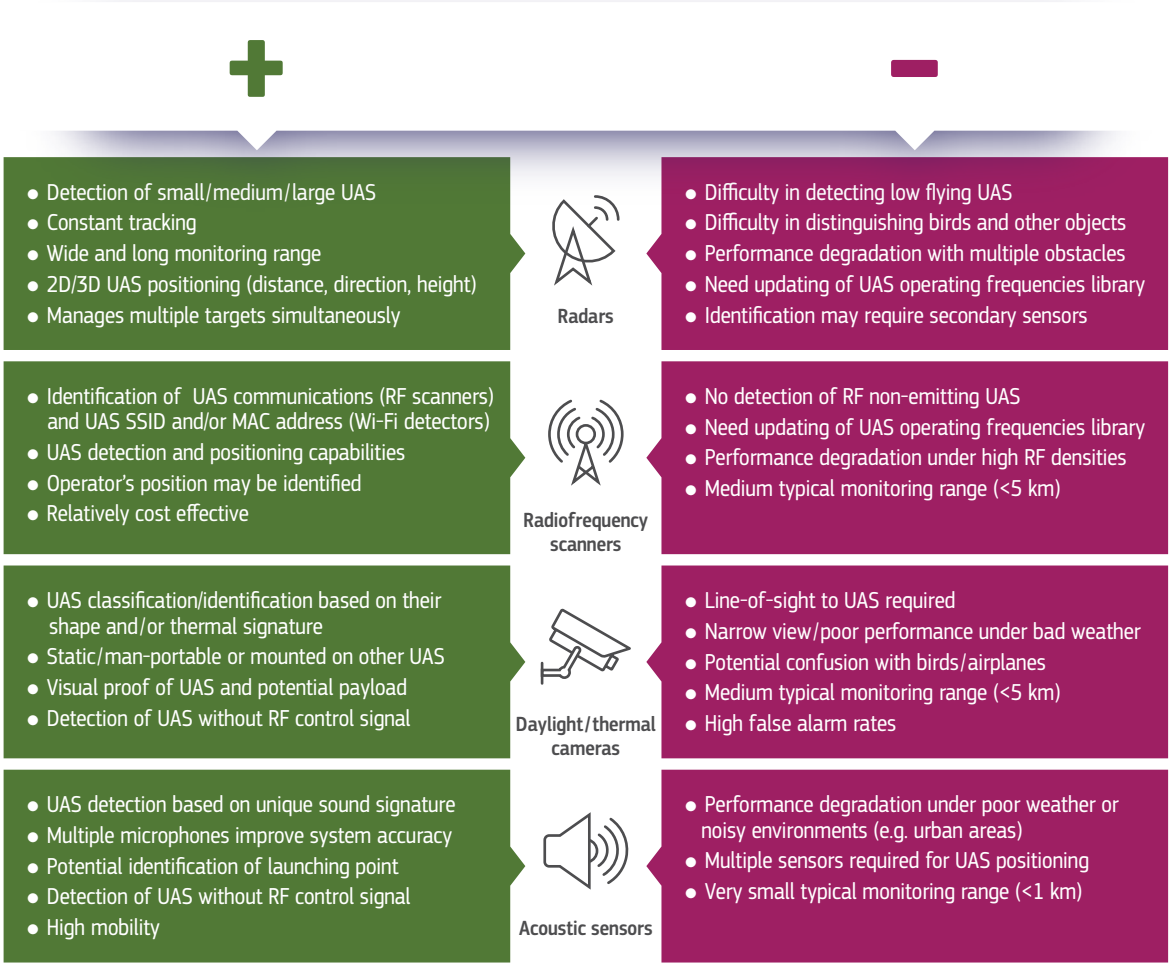
The strive to find effective countermeasures, and protect the examined asset from the threats posed by the malicious use of UAS, has been intensified in the last years due to the rapid increase in the number of security and safety incidents registered on a daily basis. Various technologies that mitigate the risk of malicious UAS have been introduced, but should be regarded as only one of the elements forming the protection strategy of an asset and definitely not the only option. In the current section, a brief summary of available technological solutions is provided, since the present guideline focuses on pointing out hardening solutions that offer protection against the modus operandi described earlier. Nevertheless, the current overview aims at providing to the reader a wide perspective of the available solutions for responding to the increasing UAS-related threats. More information on available technologies on setting up the security plan may be found in the handbook on the protection of critical infrastructure and public spaces (Hansen and Pinto Faria, 2023).

Two broad countermeasure categories may be distinguished. The first relates to systems that are able to detect, track and identify incoming UAS (detection, tracking and identification systems), while the second involves kinetic or electronic effectors that are activated to intercept potential drone intrusions. Selecting and deploying the most appropriate solution is a challenging task, as many of those systems have certain limitations when they have to operate within an urban environment. For instance, the adoption of countermeasures that have already been successfully applied for intercepting incoming UAS in military conflicts are not always recommended in urban and crowded spaces, as their use might lead to collateral damage for the surrounding facilities or the public/persons. As a result, the design of solutions that can be safely used in civilian environments poses one of the greatest concerns in the C-UAS industry.

3.2.1 Detection, tracking and identification

The detection, tracking and identification of incoming UAS in urban environments can be a difficult task due to their small size, low or high speed and low altitude. The main goal of such technologies is to provide real-time, reliable information to the user regarding the characteristics of the incoming UAS. Detection can be attained by the use of radar or RF scanners, which can identify the UAS-emitted radio waves. Moreover, cameras and electronic or acoustic identification systems can provide information concerning the UAS' size and its potential payload and track its movements. The identification of the UAS type, the operator's identity and the take-off location is more demanding, as it requires specialised information regarding the RF signature of the UAS. All sensor-based systems have certain limitations that have to be considered in detail before selecting the solution that is deemed appropriate for the asset / public space to be protected. For instance, distinguishing birds from small, low-speed UAS can prove quite difficult causing false alarms, so dedicated algorithms have been developed to overcome this shortcoming. Identifying the operator and matching them to a specific non-cooperative UAS usually depends on whether the UAS characteristics (frequencies and protocols) are included in the detection equipment's database and if the operator is registered. The engagement of multiple sensors may increase detection probability and accuracy, especially in an urban environment, but this usually results in higher purchase cost. Figure 8 shows an overview of some of the most commonly used detection technologies summarising some of their advantages and limitations.

Figure 8: Typical features and limitations of UAS detection/tracking/identification technologies



3.2.2 Interception/neutralisation technologies

Depending on the information provided by the detection, tracking and identification systems, a security operator has to decide on the proper course of action, which spans from doing nothing (e.g. false alarm) to informing the authorities and activating any technologies/procedures that will disable or eliminate the operation of the incoming UAS, and therefore mitigate or eliminate the potential threat. In the event of an incident, especially if it constitutes an attack, the time period available for the decision-making process is extremely limited, as a drone can cover very large distances in a matter of minutes. There are several different methods for disrupting the flight of a UAS, each with different limitations and legal/regulatory restrictions. Popular kinetic-interception technologies include: energy-based weapons (lasers, high-power microwaves and electromagnetic pulses) that destroy the electronics on board the UAS, nets that are launched either from the ground or from another drone, small projectiles similar to missiles used in battlefields, and expendable drones that collide with the incoming threat. In certain cases, trained birds were also used for this purpose. However, this method is progressively being suspended as it was discovered that it was not always effective under real conditions, and the act of interception could cause injury to the operating bird. A collateral effect of some of the abovementioned kinetic-interception technologies is the uncontrolled crash of a

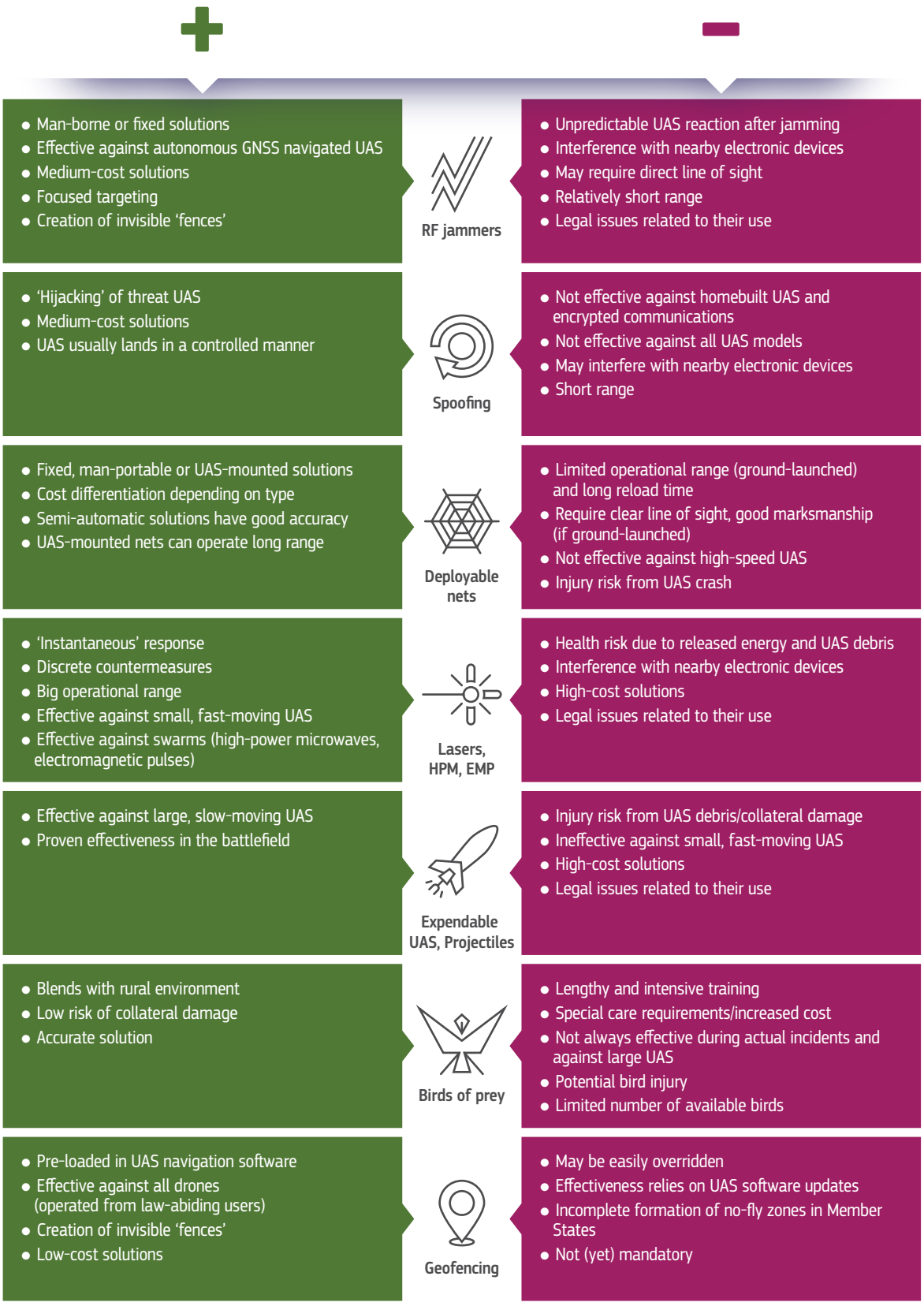
UAS, which may pose a danger to the public, especially in urban environments.

To minimise the risk of a UAS crash, non-kinetic interception systems aim at disrupting the communication capacity of the drone. These include RF and global navigation system jammers that obstruct the communication between the UAS and either the operator or the satellite link, respectively. A major concern during the employment of these systems is the reaction of the drone once its communication is interrupted, as it might hover in place, go back to the initial take-off position or even safely land. Spoofing also aims at taking control of the threat UAS by interfering with its communication or navigation link.

One of the most common ways of attempting to protect an asset / public space against malicious UAS is the introduction of 'no-fly' zones through an area-denial tool in the surrounding airspace (i.e. geofencing, not to be confused with 'geo-awareness'). When using this technique, the identification and the intentions of a UAS and its user are not of prior importance, since all UAS access is forbidden. This approach has been adopted by the majority of civilian airports and critical infrastructures, as well as in areas with major events. Geofencing uses position technologies (e.g. GPS, Wi-Fi, Bluetooth) to define the drone's exact position and prohibit its entrance into the restricted area. The latitude and longitude points that comprise the geofenced areas are embedded into the software of the UAS, which means that it is the responsibility of the manufacturers to update the software of the UAS in accordance with the recommendations of the area's operators or stakeholders. This calls for regular updates that, firstly, the manufacturers are not always willing to carry out and, secondly, the UAS users have to accept. Failure to satisfy one of those two conditions leads to the ineffectiveness of geofencing as a protection measure. Moreover, competent and determined aggressors may disable these electronic restrictions set by the geofencing and still gain access to sensitive/prohibited areas.

Figure 9 summarises the interception/neutralisation technologies that have been mentioned, focusing on the main advantages and limitations of these systems. Many producers propose systems that combine various technologies in an effort to minimise limitations and enhance interception capabilities.

Figure 9: Typical features and limitations of UAS interception/neutralisation technologies



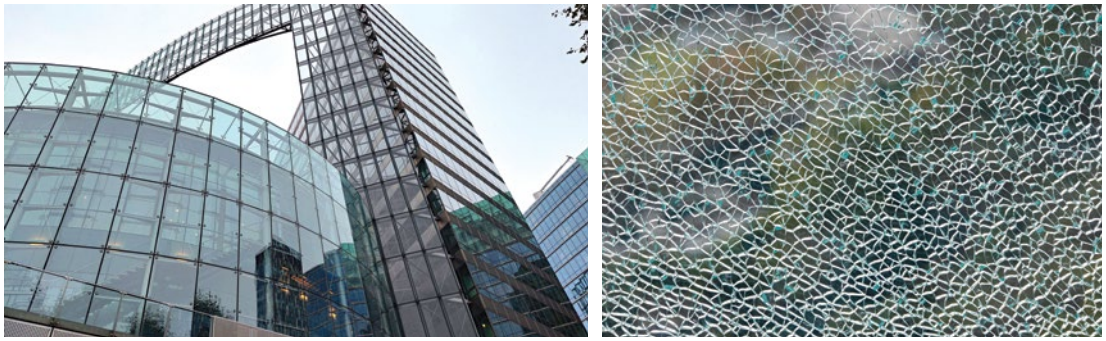
3.3 PHYSICAL HARDENING MEASURES

3.3.1 Blast resistant windows/facades

Modern commercial buildings and office complexes are characterised by the presence of extensive glass facades, which aim to bring more transparency and daylight into the building's core. Even though such facades are designed to resist extreme weather conditions, they are unable to withstand the effects of an external explosion, especially since they will be the first part of the building to be hit by the propagating blast wave. As a result, glass failure is followed by the formation of glass splinters, which, due to their high velocity, can prove lethal.

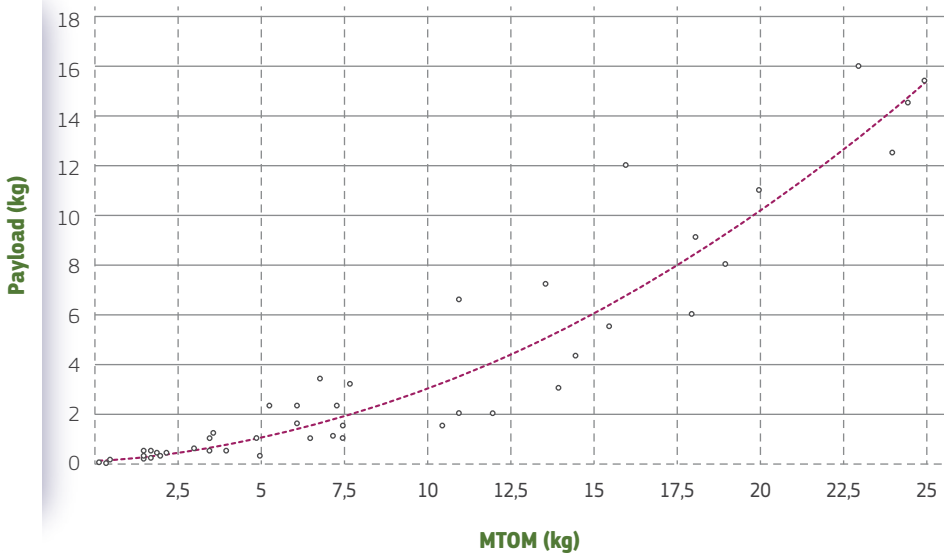
Despite the fact that the potential explosive payload of a threat UAS is relatively limited, its ability to get in very close proximity to the building envelope can lead to significant consequences due to the created blast wave and subsequent glass failure. The human body is not resistant to penetration from fast-travelling glass splinters and, consequently, an explosion outside an unprotected window may lead to extensive injuries and several fatalities. Moreover, other produced structural debris, such as those detached from the window frame or the room's interior, along with material originating from the bomb casing and its interior (e.g. screws, nails), may lead to additional injuries. It can therefore be deduced that the construction of window elements with increased resistance against explosions or the introduction of fragment-arresting mechanisms may lead to the minimisations of relevant injuries.

Figure 10: Typical building glass facade (left) and tempered glass failure without fragment detachment (right)



As mentioned in the JRC report (Larcher et al., 2018), the maximum payload capacity of UAS in the open category ranges from a couple of grams up to 15 kg (as shown in Figure 11, which compares the MTOM for publicly available UAS and their maximum payload). Similar conclusions can be drawn from the Directorate-General for Migration and Home Affairs' C-UAS mapping report (ENCO et al., 2019) and the report on minidrones from the European Defence Agency (2018). However, the majority of small and medium-sized UAS are generally characterised by payloads of up to 2–2.5 kg, as they can typically carry loads that are smaller than their own unladen weight.

Figure 11: Comparison of MTOM and maximum payload for various commercially available UAS



The performance of glass under explosive loads depends on its manufacturing process and its chemical composition. In most cases, it is characterised by large failure variations due to the presence of micro flaws, invisible to the human eye. The following three glass categories are the ones most commonly encountered.

Annealed glass. It is one of the most economic solutions and is produced by being cooled at a slow, controlled rate until room temperature. Its low tensile strength (nominal value: 45 MPa) makes it suitable for windows without heightened security needs or people presence.

Heat-strengthened glass. It has a higher tensile strength (nominal value: 75 MPa) than annealed glass as it undergoes a specialised heating and cooling process that includes surface compression. When breaking, the size of the produced fragments is similar to that of annealed glass.

Fully tempered or toughened glass. The manufacturing process is similar to that of heat-strengthened glass, but higher temperature ranges are used, making it approximately four to five times stronger than annealed glass (nominal value: 120–200 MPa). After production, both surfaces of the glass pane remain under compressive residual stresses and in the event of failure, the produced fragments are smaller and smoother, resulting in reduced injury risk.

Many commercially available solutions have been developed for applications with security requirements, bearing various hazard ratings. These ratings are based on guidance documents, such as the ISO 16933:2007 standard and the American Society for Testing and Materials (ASTM) F1642 standard. These two standards use a rating system based on experimental results derived from arena tests (illustrated in Figure 12) and according to which a very low hazard rating is assigned to fractured glazing when its significant parts are located up to 1 m from their original location, while a low hazard rating is assigned if they lie between 1 m and 3 m. Table 7 demonstrates the window glazing hazard ratings in accordance with these two standards. These ratings however, fail to consider the velocity, shape and size of the produced glass fragments and are applicable only to specific window geometries. Depending on the building use and the likelihood

of such an attack scenario, the acceptability of the existing window glazing or the need for reinforcement has to be defined by the responsible stakeholder. Generally, for buildings with people presence, glazing with a response that falls under the first three hazard categories (i.e. no break, no hazard and minimal hazard) is considered acceptable, while a response that falls under 'high hazard' is unacceptable. For the other two hazard categories, the consequences of an attack need to be defined before deciding on the acceptability of the glazing.

Figure 12: Glass hazard ratings under arena testing (modified from ISO 16933:2007 and ASTM F1642)

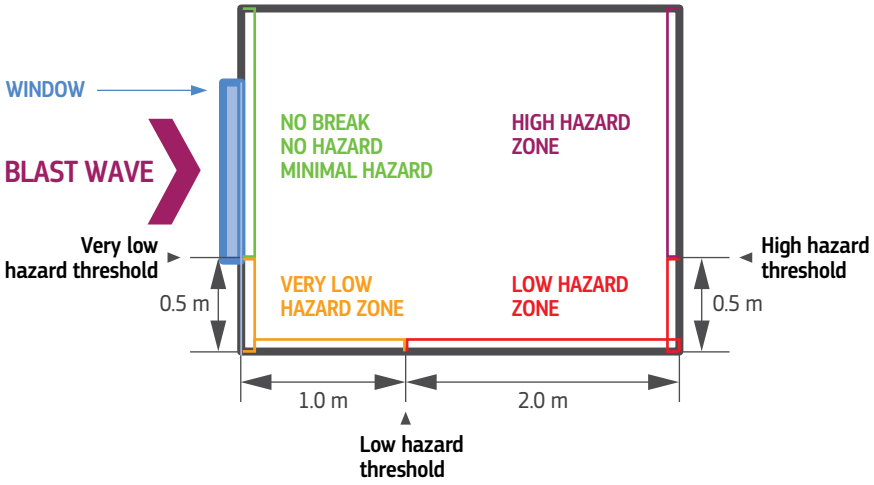


Table 7: Window glazing hazard ratings in accordance with ISO 16933:2007 and ASTM F1642

ISO 16933:2007 ASTM F1642	
Hazard rating	**Definition**
No break	No fracture.
No hazard	Fracture but no observed breach and fragments.
Minimal hazard	Insufficient or no resistance to the threat. No policy, or policy has been inadequately converted into actions.
Very low hazard	Significant fragments up to 1 m behind glass rear face and up to three fragments hitting the witness panel.
Low hazard	Significant fragments between 1 m and 3 m behind glass rear face and up to 10 fragments hitting the witness panel.
High hazard	More than 10 fragments hitting the witness panel.

The design of a building facade that can sustain the results of explosive loads may be unfeasible in both economic and technical terms. Instead, lighter measures that are able to mitigate the effects of glass failure may be adopted. For example, by minimising the number and velocity of the produced fragments, and consequently the probability of injuries/fatalities, through increasing the minimum feasible distance between a threat UAS and the glass facade. Moreover, a case-specific, scenario-based risk-assessment process, and a more detailed cost-benefit analysis, may reveal the required protection level and avoid overdesigned, costly solutions. During such a procedure, the explosive charge size,

the potential detonation point (allowing the blast wave's angle of impact and the stand-off distance to be evaluated), the window frame type and the glass dimensions/type need to be defined.

THE TWO MAIN OPTIONS FOR MITIGATING THE IMPACT OF AN EXPLOSION ON A BUILDING'S GLAZING ARE:

- increasing the stand-off distance between the UAS transporting the explosive and the building envelope;
- reinforcing the window system.

Increasing the distance between the potential detonation point and the window system poses a challenging task, especially in already existing infrastructure. Some of the measures that can be adopted include (but are not limited to):

- the use of nets outside the building facade, external curtain facades or double-skin systems to increase the distance of the potential detonation point from the building's face;
- concealing or repositioning critical utilities;
- moving building occupants away from the windows;
- changing the position of desks so as to not be directly in front of windows but at a 90° angle protected by wall elements.

More information on such measures will be provided in the following sections.

Both the glazing and the surrounding frame must be taken into account when reinforcing the window system, to render them more resistant to the results of an explosion. Some of the most commonly used solutions that focus on reinforcing the glass facade or blocking the produced fragments from entering the adjacent room are listed in the next subsections.

3.3.1.1 Anti-shatter films

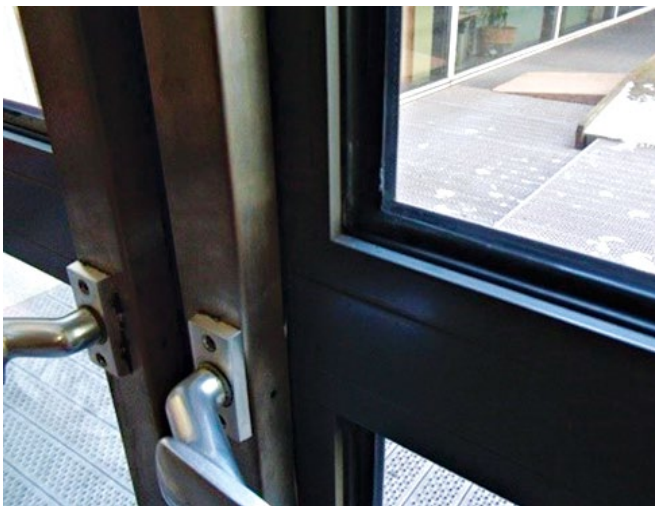
Anti-shatter films (ASFs) are a popular solution as they are one of the most economical and easiest methods for upgrading the resilience characteristics of existing annealed or tempered window glazing. ASFs are composed from a single or multiple polyethylene films that are affixed to the interior face of the glass through an adhesive and, during a blast, are capable of holding together the glass splinters produced. Their protection capabilities depend on a number of factors including (but not limited to) the adhesive component, the glass type, the window size and the strength, thickness and ductility of the film.

ASFs come in different thicknesses. The thicker options are used for large glass panes and/or thick glasses so as to increase their mitigation potential. Moreover, their effectiveness is heavily influenced by the employed application method. The most commonly used and cheapest method is called 'daylight application', where the film is applied to the inside of the glass and its size fits that of the window frame (there is a slight gap of a few millimetres at the window's edges for installation purposes). This means that the film is not wrapped around the rebates of the surrounding window frame. One of the outcomes of this type of installation

is that in the event of a blast, the whole glass sheet might fly inside the adjacent room as a single object since the generated glass fragments are held together by the film. If possible, a good practice is to install the ASF as a single piece avoiding large edge distance during the daylight application. Generally, the protection level of the ASF daylight application against explosive loading is limited. Specialised glass with anchoring and edge-retention systems are available on the market. These are fixed to the window frame (as long as it is strong enough) and might be able to hold the failed filmed glass in its place.

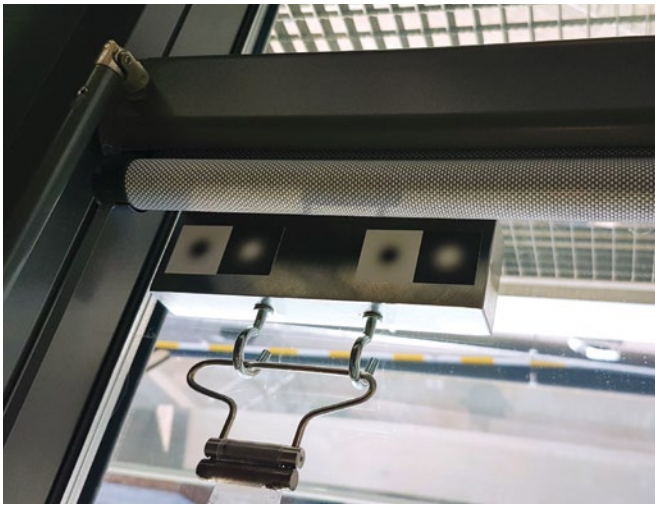
Alternatively, the ASF may be wrapped around the edges of the glass, a procedure that is both time-consuming and demanding, as it includes the removal of the glass from its frame. Another installation option includes the wet/dry type, where the edges of the ASF are attached to the window frame through a high-strength sealant (e.g. silicone). Such a process is costlier than the daylight application, but it is not extremely time-consuming. Alternatively, the film may be anchored to the frame through mechanical systems (e.g. screws, strips), a solution that may not be aesthetically pleasing, since the anchorage system is visible. Figure 13 shows an example of a wet/dry installation method where a triangular silicone joint connects the edges of the ASF to the surrounding frame.

Figure 13: ASF film attached to the surrounding window frame by means of a silicone joint



In addition to protecting against explosive loads, ASFs might also be effective against intrusion attempts with the use of sharp objects, accidental impacts and windstorms and are typically equipped with ultraviolet (UV) protection characteristics. Their impact (and not blast) performance is certified through the European Standard (EN) 12600:2002. Whereas the performance of the adhesive (e.g. aging) can be assessed through a peel test, which, according to the Centre for the Protection of National Infrastructure (CPNI) guidance note (CPNI EBP 10/13), is a procedure that entails testing the adhesion of the ASF to the glass by applying force to a narrow film strip, as shown in Figure 14.

Figure 14: Peel test for assessing the behaviour of the adhesive in an ASF



It should be noted that even though the effectiveness of ASFs is influenced by a variety of parameters, the efficiency of the ASF in combination with a certain glazing (not the entire window) is verified only for explosions taking place at relatively large-scaled distances (calculated as the division of the stand-off distance to the cube root of the explosive weight), a condition that is completely different from the scenario of a UAS carrying an explosive device next to a window. For example, Table 8 shows the combination of explosive charge / distance under which two commercially available ASFs were experimentally tested. The performance of each ASF was validated under explosions at relatively large-scaled distances (5.4 to 8.5 m/kg1/3), resulting in unique combinations of overpressure-impulse values. For comparison purposes, the scaled distance of a UAS carrying and detonating 0.5 kg or 1 kg of TNT at 2 m from a window is equal to 2.5 kg/m1/3 and 2.0 kg/m1/3, respectively. This means that the combination of maximum overpressure-impulse values varies substantially to the one under which the ASF was tested.

To ascertain if an ASF meets the desired requirements for blast protection, the data from its experimental performance need to be taken into account. However, experimental results usually correspond to a specific scaled distance, a specific glass type and a specific window geometry, values that may be completely different from the characteristics of the examined attack scenario. Modern facades in particular are typically composed of large-sized windows, whereas ASF tests are usually performed with smaller window sizes; a feature that may lead to great discrepancies regarding the performance of the ASF under blast loads. A direct comparison of the equivalent number of explosives corresponding to a similar ASF performance under much smaller stand-off distances (as is the case with a UAS transporting an IED outside a window) is very risky, as the glass failure mechanism might differ substantially (depending on the window's mechanical parameters and the stand-off distance/charge weight combination of the explosive). The performance of the ASF may not be primarily influenced by the maximum overpressure or the maximum positive impulse only, but by the combination of overpressure and impulse. Nevertheless, it is certain that the ASF will fail under a very small explosive charge that may be easily carried by a UAS belonging in the 'open' category. Therefore, the protection level of such films is usually very small, and they might offer a false sense of security regarding the scenario of a UAS carrying an explosive device.

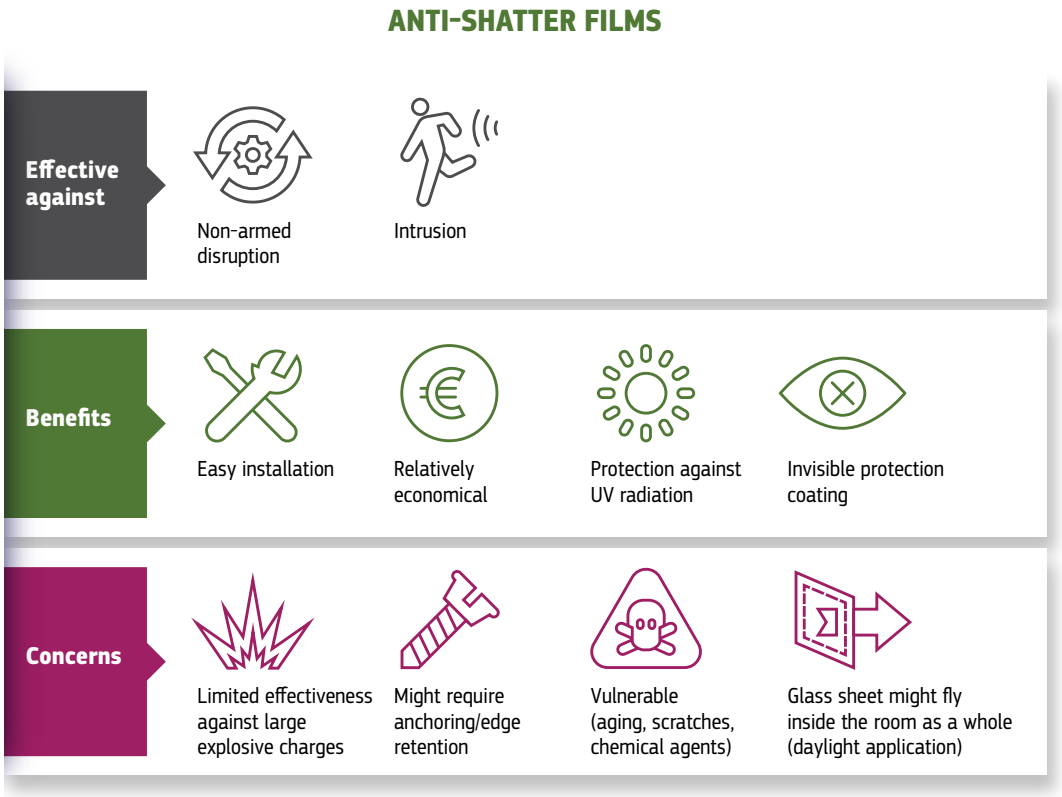
Table 8: Examples of experimental parameters under which the performance of two commercially available ASFs were assessed

Protection type	Glass type	Attachment	Maximum (tested) overpressure (kPa)	Maximum (tested) impulse (kPa·ms)	Scaled (tested) distance (m/kg $^{1/3}$)
3M Scotchshield™ Ultra S800	6 mm annealed (or 6 mm tempered)	3M Impact Protection Adhesive System	41.4	289.6	8.5 (70 kg at 35 m)
	25 mm double pane annealed (or 6 mm double pane tempered)		62.0	413.7	6.5 (80 kg at 28 m)
Madico Safetyshield 800	6 mm annealed	Madico FrameGard System	63.4	444.9	6.46 (100 kg at 30 m)
	6 mm annealed		88.1	543.2	5.38 (100 kg at 25 m)

As a final note, it is reminded that the extensive use of ASFs for retrofitting existing facades is due to both their easy installation and their relatively low price, combined with the usual integrated protection against UV radiation. However, such films are not embedded in two-glass layers like in laminated glass, as discussed in the following section, leaving them exposed to the environmental conditions may result in faster material aging. Additionally, this exposure makes them vulnerable to scratches, chemical agents (e.g. cleaning material) and extreme heat, since they are less resistant than glass. Different films are available, though it is important to carefully select products that are able to certify their performance with proper documentation, while remaining under warranty (against cracking, peeling, bubbling, delamination, discoloration, strength loss, tear, etc.) for at least 10 years following their installation.

Figure 15 presents an overview of the attack scenarios under which the ASFs are usually efficient and pinpoints some of their aspects that should be considered before being adopted.

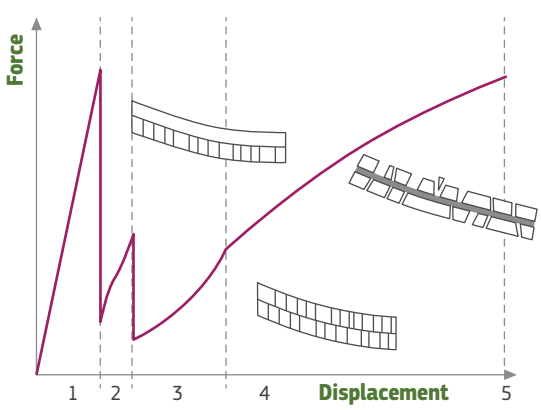
Figure 15: Effectiveness and considerations of ASF use against UAS-driven attack tactics



3.3.1.2 Laminated glass

Laminated glass, despite its elevated price, is gaining popularity in the design of explosive-resistant building glass facades due to its high efficiency. It is composed of two or more glass sheets that are bonded together by polymer interlayers, such as polyvinyl butyral, ionoplast polymers and ethylene-vinyl acetate. During the failure of laminated glass, the film's interlayer(s) holds together the failed glass sheets and prevents them from falling apart if breached, since the created glass fragments remain stuck to the interlayer(s). Figure 16 graphically depicts the failure mechanism of a laminated glass pane with one interlayer (Larcher et al. 2012). As observed in the graph, during the first phase of its failure, laminated glass responds as an elastic plate, similar to a monolithic pane. However, after the two glass sheets are fractured, their fragments remain glued to the interlayer and the laminated glass behaves as a membrane, only failing when the interlayer bonding material tears.

Figure 16: Failure mechanism of laminated glass with two glass sheets and one polymer interlayer



- **Area 1:** Elastic behavior of glass sheets
- **Area 2:** First glass sheet breaks (second glass sheet and interlayer intact)
- **Area 3:** Second glass sheet breaks (interlayer intact)
- **Area 4:** Interlayer deforms obtaining large deformations
- **Point 5:** Polymer interlayer fails

Laminated glass becomes more resistant when using multiple and/or thicker glass panes and interlayers, as in the case of bullet-resistant glass, similar to the glass in Figure 17. Just like ASFs, the use of laminated glass as a retrofitting solution needs to be combined with strengthening the surrounding window frame, to limit the probability of the entire window being propelled into the adjacent room due to the propagating blast wave. Practically, this means that the window's surrounding frame and its connections must not fail before the laminated glass does to prevent the early detachment of the entire frame from the supporting wall. If the pressures to be sustained by the window system are high, as is usually the case in small-scaled distances, the window frame can be anchored to the surrounding wall by means of steel bars, cables or steel plates, as will be described later. Special attention is also required regarding the glass depth that is captured by the frame (minimum recommended depth equal to 1.5 cm) and the amount of sealant that is used.

Figure 17: Laminated glass with five polyvinyl butyral interlayers and six glass sheets

Different standards are available for the classification of laminated security glass depending on the type of attack to be mitigated (e.g. ballistic, manual or explosive). Classification is provided once physical testing corresponding to the mitigation needs has been carried out, meaning pendulum tests for glass impact (EN 12600:2002), steel ball tests for manual attacks (EN 356:1999), ballistic tests for bullet proof glazing (EN 1063:1999) and blast tests (shock tube (EN 13123-1:2004) or arena testing (EN 13123-2:2004)) for explosion resistance.

Table 9 shows the test conditions when assessing the performance of explosion-pressure-resistant glass panes for use in buildings. During these tests, the window frame was replaced by a stiff metal setup. The glass sizes used in the experiments were approximately 1 m^2 (1.1 m × 0.9 m) and were positioned in a shock tube or a similar device able to produce a plane shock wave, propagating at a 90° angle to the clamped specimen. Glass panes having acquired one of the following classification ratings (ER1 to ER4) are certain not to have experienced during the test any 'through' holes from their front to their back or openings near their clamped edges.

Table 9: Classification for the resistance of glass panes to explosive attacks

Attack type	Standard	Classification	Maximum reflected overpressure (kPa)	Positive reflected impulse (kPa·ms)
Attack with explosives (glazing)	EN 13541	ER1	$50 \leq P_r < 100$	$370 \leq i_{r+} < 900$
		ER2	$100 \leq P_r < 150$	$900 \leq i_{r+} < 1\,500$
		ER3	$150 \leq P_r < 200$	$1\,500 \leq i_{r+} < 2\,200$
		ER4	$200 \leq P_r < 250$	$2\,200 \leq i_{r+} < 3\,200$

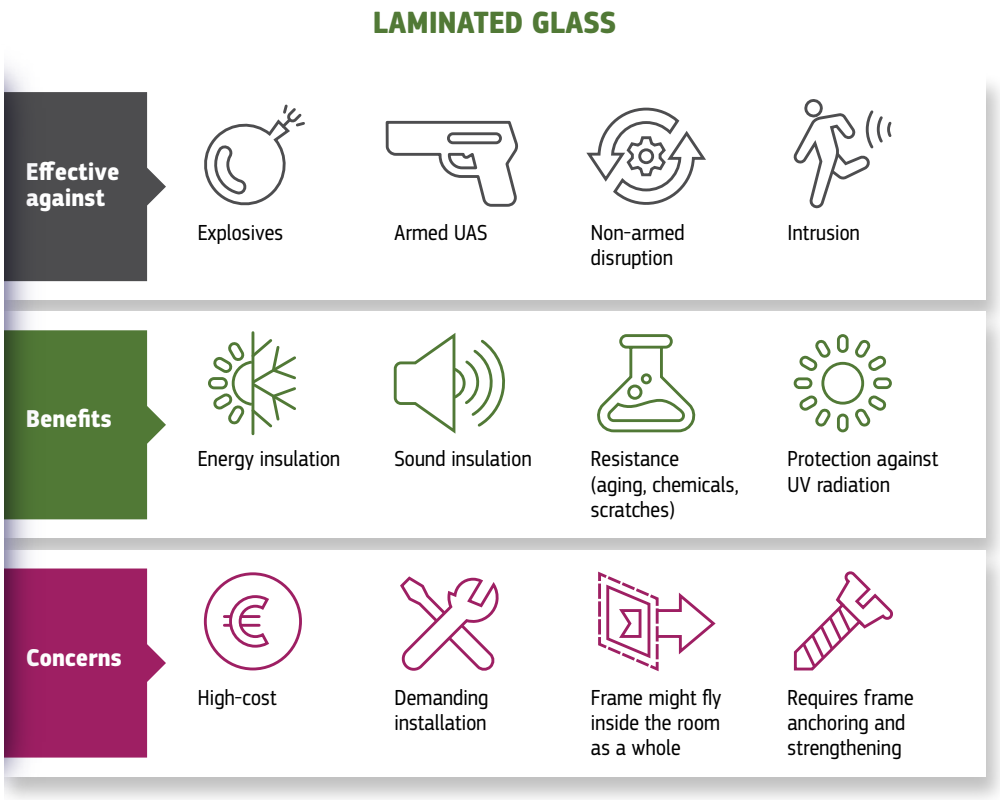
Table 9 only describes the classification requirements for explosion-resistant glass panes, whereas a different standard has to be used for assessing the resistance of the entire window system against explosions, to avoid the scenario of being propelled as a whole into the building. These experimental procedures may be performed either through the use of shock tubes (EN 13123-1: 2004) or arena tests (EN 13123-2: 2004). Table 10 presents the test conditions and performance classification levels, which guarantee that no perforation is observed and no parts or the frame are ejected from their rear face. It is highlighted that, in many cases, the window frame is the weakest part of the overall window system, so before reinforcing the glazing, the appropriateness of the surrounding frame has to be ensured.

Table 10: Classification for window system resistance to explosive attacks

Attack type	Standard	Classification	Maximum reflected overpressure (kPa)	Positive reflected impulse (kPa·ms)
Attack with explosives (window system)	EN 13123-1 (shock tube)	EPR1	$50 \leq P_r < 100$	$370 \leq i_{r+} < 900$
		EPR2	$100 \leq P_r < 150$	$900 \leq i_{r+} < 1\,500$
		EPR3	$150 \leq P_r < 200$	$1\,500 \leq i_{r+} < 2\,200$
		EPR4	$200 \leq P_r < 250$	$2\,200 \leq i_{r+} < 3\,200$
	Standard	**Classification**	**Charge mass (kg)**	**Stand-off distance (m)**
	EN 13123-2 (arena test)	EXR1	3	5.0
		EXR2	3	3.0
		EXR3	12	5.5
		EXR4	12	4.0
		EXR5	20	4.0

Laminated glass is also characterised by certain security-unrelated characteristics, since it is UV resistant and can efficiently block the majority of harmful radiation, while the presence of glass panes at both sides guarantee that the polymer interlayer does not come in contact with the environment preventing any discoloration or tearing. This means that its life cycle is longer than the ASF's, so its elevated price might be compensated by its longer life span. Moreover, by adding various reflective coatings between the glass panes, the energy demand of the building in terms of air conditioning may be significantly reduced. Undesirable noise levels may also decrease, as laminated glass may act as a sound insulation barrier due to its geometrical characteristics of multiple glass sheets and interlayers. Figure 18 summarises the attack tactics under which the use of laminated glass is efficient and goes through several considerations that are required before its adoption as a solution.

Figure 18: Effectiveness and considerations of the laminated glass use against UAS-driven attack tactics



The blast-protection level of a laminated glass window or facade component is of crucial importance for safety and security design purposes, and in most cases is performed through complex experimental analysis supported by finite element numerical models. These experimental tests are commonly performed under far-field conditions that do not correspond to the near field case of a UAS carrying an explosive charge in proximity to a window. As noted by Bedon et al. (2023), in the near field, laminated glass windows are highly vulnerable to even small charges, whereas the performance rating evaluated from far-field experiments cannot be entirely trusted for the near-field case, as the failure mechanism might be different. This means that special attention is required during the design of such solutions, to guarantee that the desired protection level is attained.

3.3.1.3 Catching systems

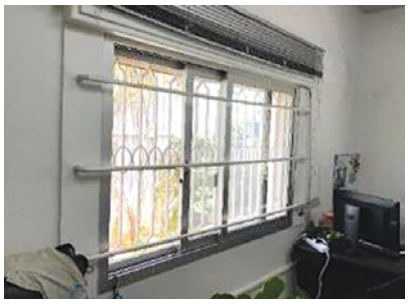
Such systems are designed to stop the failed glass or the whole window from entering the building, and therefore mitigate the consequences of their failure. They can be divided into two broad categories: the ones that are usually installed in combination with other protective systems and the ones that are also effective as stand-alone solutions. The former include bars, cables and other anchoring systems that are typically combined with one of the glass types described earlier (usually ASFs) and the latter encompasses curtains and catching nets. Both of these systems (i.e. curtains and nets) are mainly used when there are very high security demands, since their installation may result in the reduction of window transparency, which may be unacceptable if not properly justified.

Bars/cables/anchoring systems. The installation of these systems is usually combined with the presence of ASFs or laminated glass to increase the effectiveness of the overall solution if the failed glass panes are detached from the window frame in one piece. Catcher rigid bars are anchored to the interior of the window frame and positioned horizontally and/or vertically to stop glazing

from flying as a whole into the adjacent room. A single rigid bar may also be used and placed at the opening's midpoint, so that the failed glazing wraps around it if it detaches from the frame while still held together by the interlayer or interior films. A crucial parameter in the design of such bars is their anchoring to the window frame, as it needs to be strong enough to sustain the created blast forces, since rigid systems accumulate large amounts of energy, even in cases of relatively small explosive charges transported by UAS. As a result, the supporting structure (e.g. surrounding wall) needs to be capable of restraining the created forces without failing.

Cables and other similar flexible solutions (flexible catcher bars are also available) are designed to absorb an amount of energy, which is transmitted to the system after the impingement of the glazing. Due to their flexibility, cables can be retrofitted to different window geometries. They can also be combined with shock-absorbing devices to increase the system's energy-absorbing capacity. These devices may be considered if the window frames are relatively weak so that part of the impacted energy is absorbed by the device, therefore reducing the resistance requirement of the window frame (which would be higher in the case of rigid connections). The characteristics of the blast, meaning the weight of the explosive charge transported by the UAS and the distance of the detonation point from the glass facade, are used for assessing the design parameters of such systems, including the cables' diameter, their fixings and their spacing.

Figure 19: Example of rigid bar catcher system (left) (source: United Nations Department for Safety and Security (UNDSS), Physical Security Unit) and flexible cable catch system (right) (source: Window Gard B.V.)



Curtains/nets. Contrary to the previous category, these systems can be used either as stand-alone protective solutions or coupled with ASFs or laminated glass (catching nets are usually combined with other measures). Their main goal is to catch any flying glass fragments or frame pieces produced from the window's failure as a result of the propagating blast wave. Typically, they are installed behind the building's facade and their anchorage needs to be properly designed. They do not stop glass fragments from flying into the adjacent room, but they are able to limit their travelled distance after failure, and therefore greatly reduce injury hazard to the occupants. Blast curtains are generally manufactured from ductile polyester materials and are fixed only at the top of the opening. Their installation guarantees adequate venting of the blast wave as they are not mounted on the sides or the sill of the window. It is clear that such protective drapes need to be left in their intended position, and if pushed aside from the building occupants, they lose their mitigation capacity. However, since they are not fixed to the sides of the window or its sill, this means they can easily be pulled away for cleaning purposes or safety reasons (e.g. in the event of a fire). The type and colour of their material greatly influences the light penetrating the room, so they can be selected based on interior design needs. Nets on the other hand are made of steel or polyester ropes that are typically anchored to the entire perimeter of the window frame. They can be very effective in retaining larger glass parts, but their performance is usually poor if smaller glass splinters are produced, which indicates that they should be coupled with an ASF installation.

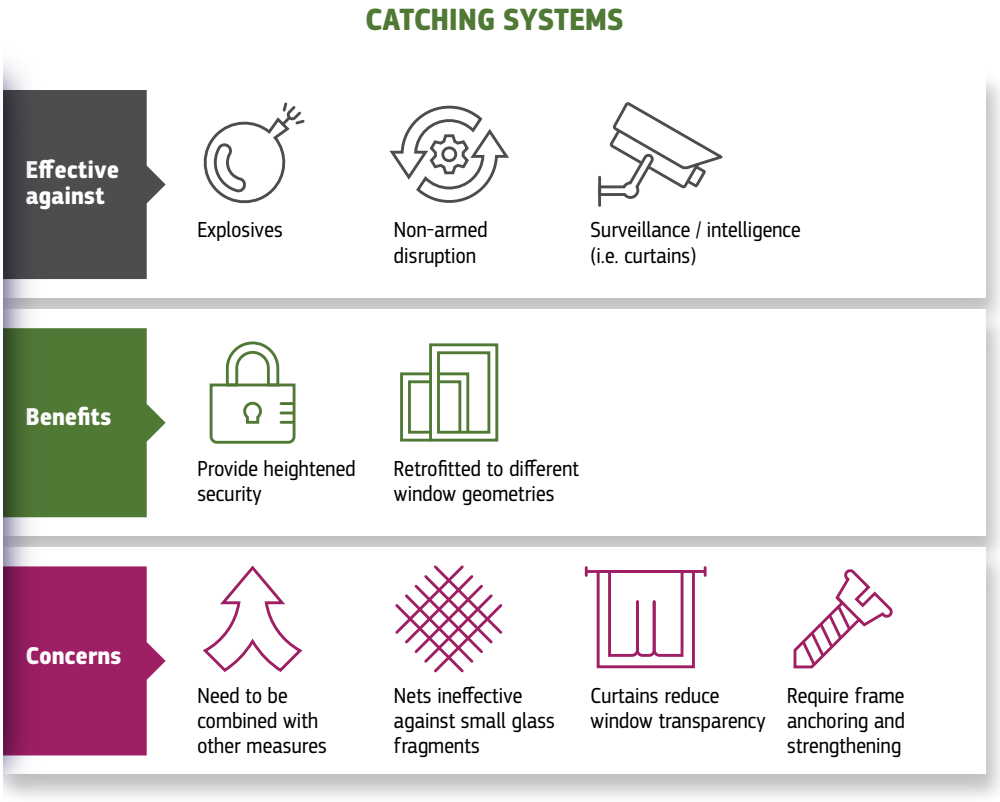
Figure 20: Example of blast curtains (source: UNDSS, Physical Security Unit)

Despite being popular blast mitigation solutions adopted during heightened security demands, their performance and installation are not regulated through dedicated standards, like that of glazing, but instead constitute solutions developed through best practices and lessons learned. One of the main elements that need to be carefully designed is their anchoring, as they need to absorb large forces originating from the failure of the glazing or the window (even for small amounts of explosives located at small distances, as in the case of UAS-transported IEDs). If possible, cables and bars should be anchored to the strongest structural elements of the buildings, such as the beams, columns and slabs. Moreover, the window frames may be directly anchored to the concrete slabs or the building's perimeter beams (spandrel beams), so that the resulting reaction forces do not have to be sustained by the surrounding walls. As mentioned in the PSU Information Bulletin (UNDSS, 2021), the following recommendations should be considered:

- bar/cable spacing to be approximately 0.5 m horizontally and/or vertically;
- solid steel bars of 12 mm diameter and 50 kN of tensile strength, with a 5 mm thick, rectangular or round (10 × 10 cm) plate welded at their ends with four screws;
- wire steel cables of minimum 6 mm diameter and 25 kN of tensile strength, preferably made from a small number of large wires;
- anchoring to concrete walls (and reinforced masonry if it is resistant enough) should be made with the use of stainless-steel anchors of at least 8 mm diameter and 10 cm in length;
- when anchoring to non-concrete walls (e.g. masonry, cement blocks), anchors need to cross the wall and should also be equipped with a 5 mm thick metal plate (15 × 15 cm in dimensions) on the exterior wall face.

Figure 21 presents an overview of which types of catching systems are effective against UAS-related attack tactics and indicates certain considerations regarding their use.

Figure 21: Effectiveness and considerations of catching systems used against UAS-driven attack tactics

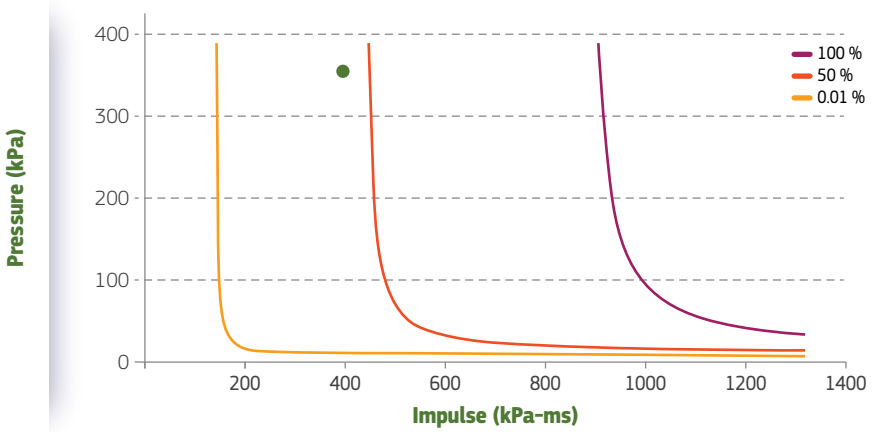


3.3.1.4 Surrounding/supporting walls

The surrounding walls of a building are usually overlooked during a blast assessment, as they are considered to be able to withstand the produced blast wave. The fact that the number of explosives that can be transported by a UAS is, in the majority of cases, relatively limited, the likelihood that a surrounding wall will fail is small. If the examined attack scenario predicts an elevated transported charge weight (> 5 kg of TNT equivalent), special attention may be required for weak, unreinforced masonry walls, aluminium or other unreinforced cladding types that may fail or be perforated in large explosions. For example, Figure 22 shows the probability of perforation of a 0.7 mm thick steel panel cladding after an explosion of 4 kg of TNT positioned at 2 m from its face, which is the approximate minimum distance of a hovering UAS. The results are the product of the JRC's BLADE tool[2] (based on pressure-impulse diagrams) and it may be seen that the probability of plate perforation is equal to 60 %. Consequently, in cases where sensitive materials or humans are situated right next to a potential detonation point, depending on the attack scenario, the surrounding steel panels might need to be reinforced (or the sensitive materials / people be moved further away from the surrounding wall).

2 See https://counterterrorism.ec.europa.eu/

Figure 22: Probability of perforation for a 0.7 mm thick steel panel after the explosion of 4 kg of TNT located at 2.0 m from its surface (source: JRC's BLADE tool)



Similar to the graph presented in Figure 22, the JRC's BLADE tool may be used for performing preliminary assessments on the probability of perforation for various types of external walls. The following table provides estimates as evaluated from this tool. The malicious UAS is presumed to be carrying an explosive TNT device and hovering at one or two metres from the face of the wall. It is noticed that the probability of wall perforation is generally small for small explosive loads but can rise substantially for bigger explosives, and if the exterior wall is made of low strength materials. The size of the explosive device each UAS in the 'open' category could carry is evaluated from the data presented in Figure 11.

Table 11: Probability of external wall perforation as assessed with the JRC blast assessment tool

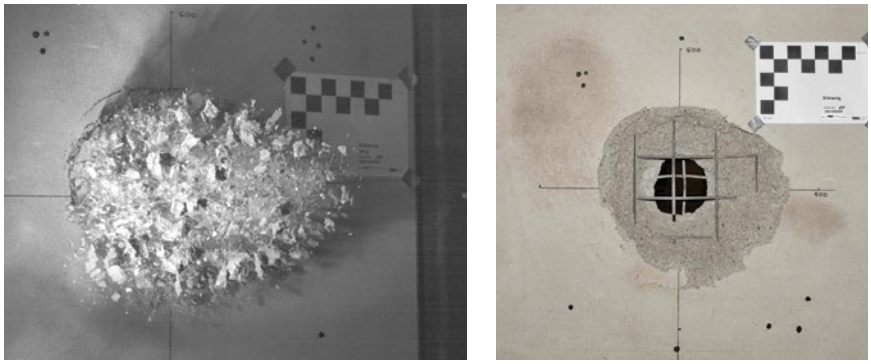
External wall type	UAS distance from wall	UAS-A2 subcategory (MTOM<4kg)		UAS-A3 subcategory (MTOM<25kg)	
		Payload (with respect to Figure 11)			
		MEDIUM	HIGH	LOW	MEDIUM-LOW
Unreinforced brick	1 m	10-20 %	40-60 %	50-70 %	>70 %
	2 m	<5 %	10-20 %	10-20 %	>70 %
Unreinforced concrete blocks	1 m	5-10 %	10-20 %	10-20 %	10-20 %
	2 m	<5 %	<5 %	5-10 %	10-20 %
Reinforced concrete (10 cm)	1 m	<5 %	<5 %	10-20 %	10-20 %
	2 m	<5 %	<5 %	<5 %	10-20 %
Steel panel (1.2 mm)	1 m	<5 %	5-10 %	10-20 %	20-30 %
	2 m	<5 %	<5 %	<5 %	10-20 %
Steel panel (0.7 mm)	1 m	5-10 %	30-40 %	50-70 %	>70 %
	2 m	<5 %	5-10 %	5-10 %	50-70 %

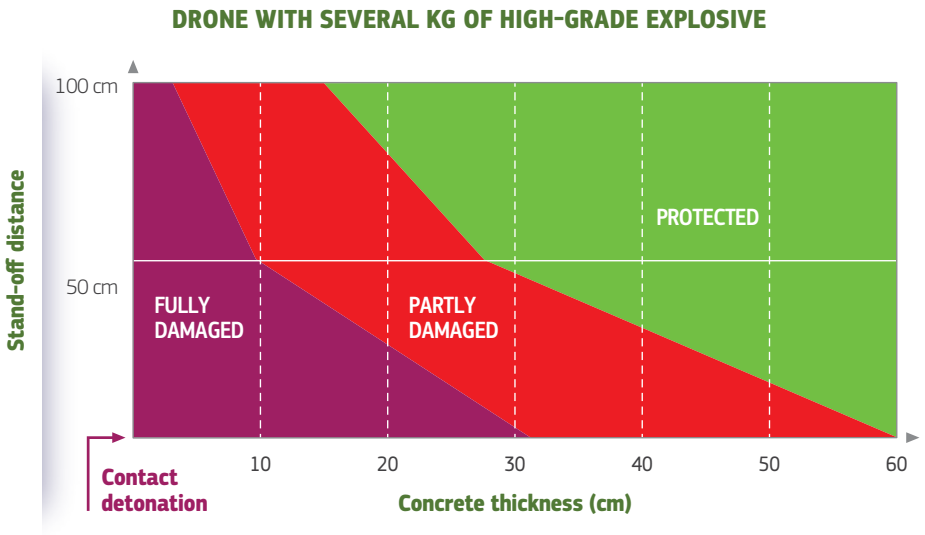
Limiting the produced exterior wall fragments may be performed through the application of an interior (and potentially exterior) spayed-on polymer coating or the retrofitting of a geotextile fabric, as they are characterised by a ductile nature and enhanced deformation capabilities. Neither of the solutions strengthen the wall, but are instead able to restrain potential debris from propagating into the occupied space.

3.3.1.5 Top floor slab

Typically, slabs on the top floor of buildings are designed to sustain the dead and live loads (and occasionally accidental loads) they might face during their lifespan. Even in highly protected buildings, such as governmental buildings and embassies, where there is credible threat of an attack with the use of explosives, top floors / roof slabs do not usually undergo additional hardening. This is attributed to the fact that traditionally, attack scenarios with an explosive device place the potential detonation centre at ground level, since the considered transportation means is usually either a person or a vehicle. This leads to a big stand-off distance, which results in relatively small loads that have to be sustained from the roof. However, the potential use of a drone for carrying an explosive device to the top floor of a building means that the slabs might face localised extreme loading, which may lead to localised damage and perforation and might be unacceptable if sensitive areas are situated in such locations. Despite the fact that such a close-in (or contact) detonation to a slab will not cause a progressive collapse mechanism, the generated fragments might lead to extensive injuries that could even prove fatal for persons under the roof, as presented in Figure 23. In the same figure, the performance of a concrete slab after the detonation of several kg of high-grade explosives is demonstrated in relation to the distance of the explosive from the slab's face and the slab's thickness. It is pointed out that metal decks, usually made of cold-formed corrugated steel sheets, are very vulnerable to localised explosive loads as their energy absorption potential is limited.

Figure 23: Example of concrete slab perforation under the detonation of medium quantity of TNT at 20cm from its face (upper) (source: Moritz Hupfauf, University of the Bundeswehr Munich) and slab performance under the detonation of several kg of high-grade explosives (lower)





Several possibilities are available for strengthening slabs (or other structural members) in locations deemed as vulnerable. An easily applicable and economic technique for existing concrete slabs is to apply an additional layer of high-strength concrete above the old slab and increase its thickness. If the additional weight from this layer is undesirable in fear of it affecting the structural stability of the slab, lightweight alternatives exist which provide the requested protection without substantially increasing the slab's weight. Another technique for strengthening a reinforced concrete slab is by adding metal plates made from steel, aluminium alloys and titanium. The protection level of steel plates is generally higher than titanium or aluminium, but the steel's density leads to considerable additional structure weight. Titanium may be considered where weight is an issue, but it has a higher cost and its welding is more difficult. Aluminium alloys, on the other hand, require greater thickness to provide the same protection level as steel, but have good welding capabilities. Polymer matrix composites (e.g. Kevlar) in the form of layered plates may also be used for increasing the structural protection level, but their application may be expensive. Moreover, ceramics, commonly used for projectile resistance, may be employed but are usually combined with a metal or polymer backplate that acts as an additional layer for stopping the created fragments from their failure.

As already noted, increasing the stand-off distance of a potential UAS transported IED from the building's envelope is one of the most efficient techniques for mitigating the effects of an explosion, though if it cannot be guaranteed, several of the abovementioned materials with energy absorption capabilities may be used. Contact detonations may require the adoption of materials with greater absorbing potential in order to decrease the amount of energy that is transmitted through slabs and mitigate potential injuries from fragmentation. Laminate structures combining different materials are also being constantly developed and are able to combine the advantages of diverse materials to provide optimum protection level.

3.3.2 Netting/fences

The major objective of anti-drone nets and fences is to create an enclosure and prohibit the entrance of unauthorised drones at the protected site premises, while at the same time guaranteeing a minimum distance of a potentially malicious cargo from the site's perimeter or building envelope. Nets and fences are easily custom fitted to different area sizes and can be effectively used in various settings, including (but not limited to) stadiums, prisons, universities, atriums and courtyards.

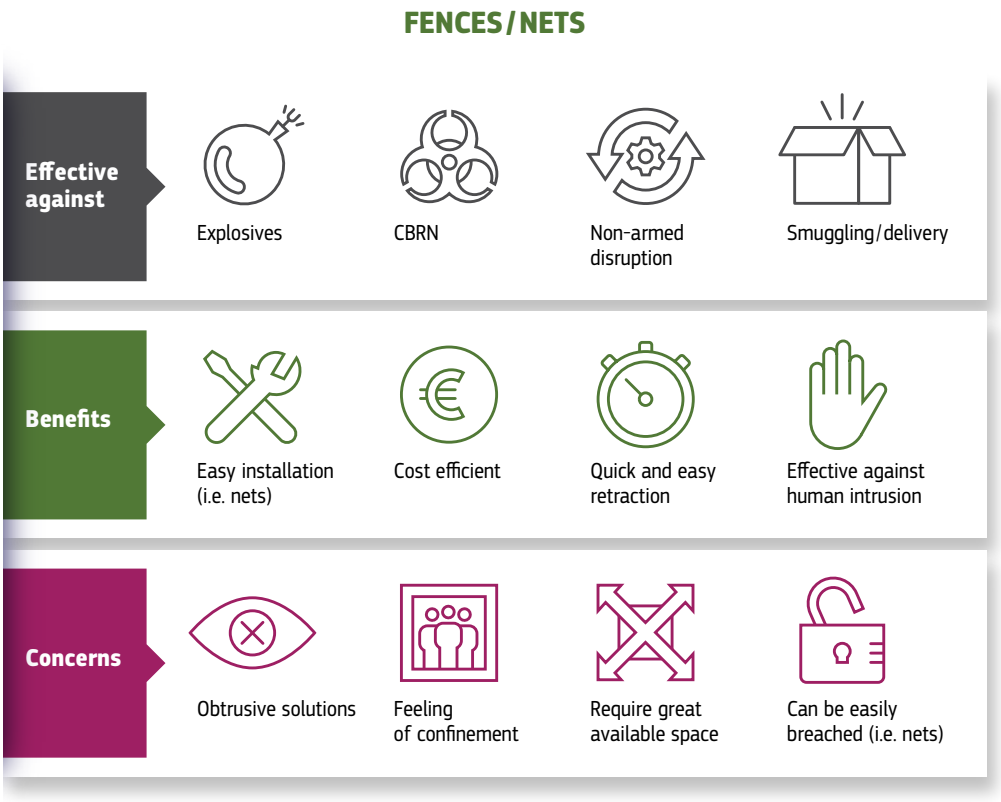
- **Fences** are of rigid nature (usually made of steel-wired mesh), making their installation more difficult, and are able to provide heightened protection against incoming UAS, with the combination of appropriate detectors. Nevertheless, their obtrusive appearance makes them less popular among stakeholders who usually prefer more discreet solutions that do not generate a feeling of confinement.
- **Nets** on the other hand are easily installed, low-cost and provide a good view through their mesh, as they are less visible than fences. Their flexibility means that in the event of a UAS crash, the net will experience great deformation and the resulting force will be distributed to a greater area. They are made from different materials, like nylon, polypropylene, polyester, stainless steel or even Kevlar and may be knotted or knotless.

By increasing the distance of a malicious UAS from its potential target, such systems guarantee the limitation of resulting consequences that may be further mitigated with the adoption of lighter and less costly measures. For example, by increasing the minimum distance between a UAS transporting an IED and a window or a slab, the resulting blast parameters are exponentially decreased (Karlos and Solomos, 2013). Consequently, the requirements for glazing or slab reinforcement will be substantially lower, and therefore so will the relevant cost. Likewise, nets or similar measures may be adopted to increase the distance between a harmful parcel (i.e. a CBRN device) and the HVAC system's exterior air intakes, therefore reducing the risk of interior contamination from such a weapon. The HVAC intakes should also be positioned, if possible, on a sloped surface, so the placement of an item would be impossible as it would slide away from the enclosure's face.

Figure 24: Examples of anti-drone fence (left) and stainless-steel net (right) deployed solutions

The cord diameter is selected depending on the strength and the velocity of an incoming drone, while the net mesh size should match its expected size. UAS that may be used for eavesdropping or intelligence purposes are usually smaller in size (e.g. minidrones) than the ones that may be employed for transporting an item, so the mesh size needs to be adjusted accordingly, ranging from 45–50 mm in the former case to 120–160 mm in the latter. Typically, nets that are used for this purpose are fire resistant and can be retracted if deemed necessary. They are usually attached to a perimeter wire rope, rod or tube, which in turn is affixed to the underlying structure through specialised holders and connectors. The connectors need to be able to sustain the created force in the event of a UAS crash and transfer it safely to the structure. The distance of the fence/net from the protected area may need to be carefully selected to minimise the consequences from a potential hazardous load. For instance, the distance of the employed net from the facade of a building also defines the distance of the potential IED detonation centre, and consequently the effects for the building envelope and its inhabitants from the created blast wave. Figure 25 provides an overview of the attack scenarios where fences/nets may be efficiently employed and indicates a number of considerations that need to be regarded before their adoption.

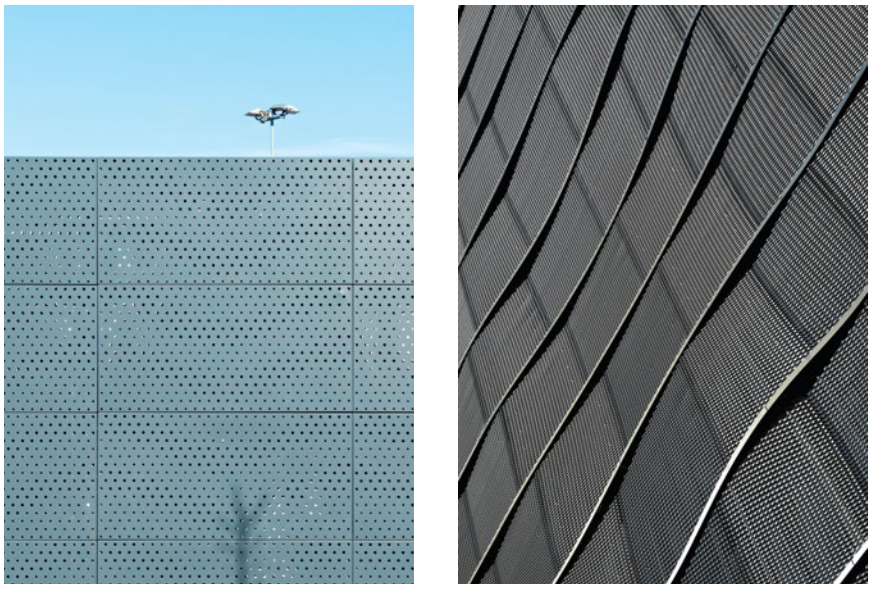
Figure 25: Effectiveness and considerations of anti-drone fences/nets against UAS-driven attack tactics



3.3.3 External building skins

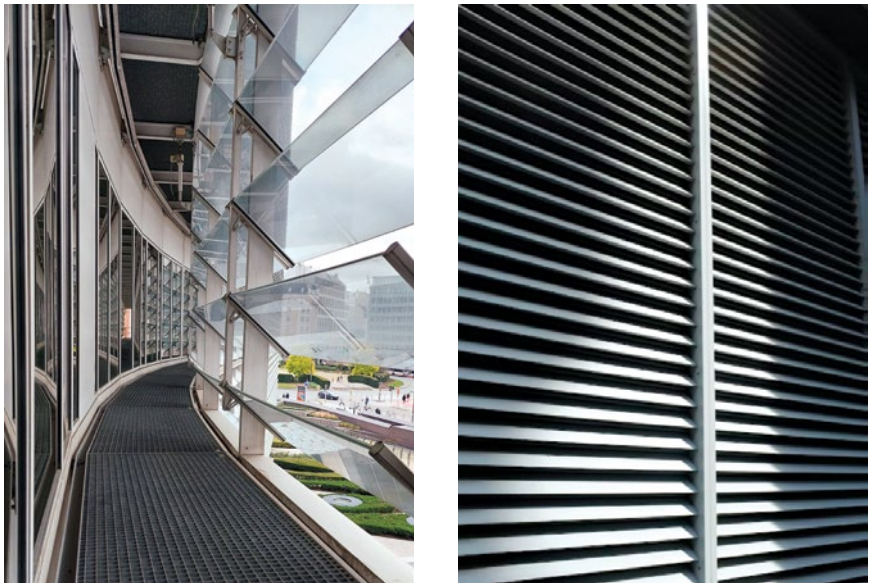
These solutions are applied to the exterior of a building in order to block the propagating blast wave from entering its interior. They are usually adopted to upgrade the security level of existing buildings, though they can also be introduced to new constructions. They usually have the form of perforated plates or chain meshes and are fitted inside a panel or a frame, which is in turn attached to the building facade, as shown in Figure 26. They may be fixed or electronically operated and are usually made of steel. They provide shading, thus contributing to the energy efficiency of the building, and on the other hand, they block the view from the building interior. Despite this, some options can be pushed aside to provide more light or for cleaning purposes, they should however remain in their original position to guarantee the expected protection. Experiments have shown that if such elements are covered by a film of water, further reduction in the blast parameters can be achieved.

Figure 26: Perforated steel plates (left) and steel-chain mesh (right) installed on the exterior of a building's facade



Another solution that has migrated to commercial buildings from refineries, factories and military bases, while resembling hurricane shutters, is the use of louvers – which may also be applied in front of the building facade. The blades are adjustable to regulate shading in the building, but in the event of an explosion, the propagating blast wave automatically closes the blades and is reflected on their surface. A locking mechanism may also be designed to keep the blades locked after their closure and to avoid them opening during the negative phase of the blast wave. Fixing these shutters to the building frame is both challenging and crucial to avoid them becoming a projectile during the blast. Moreover, these shutters may be closed through the push of the button in the event of an unauthorised UAS to hide the interior of the building.

Figure 27: Glass (left) and metal (right) louvers



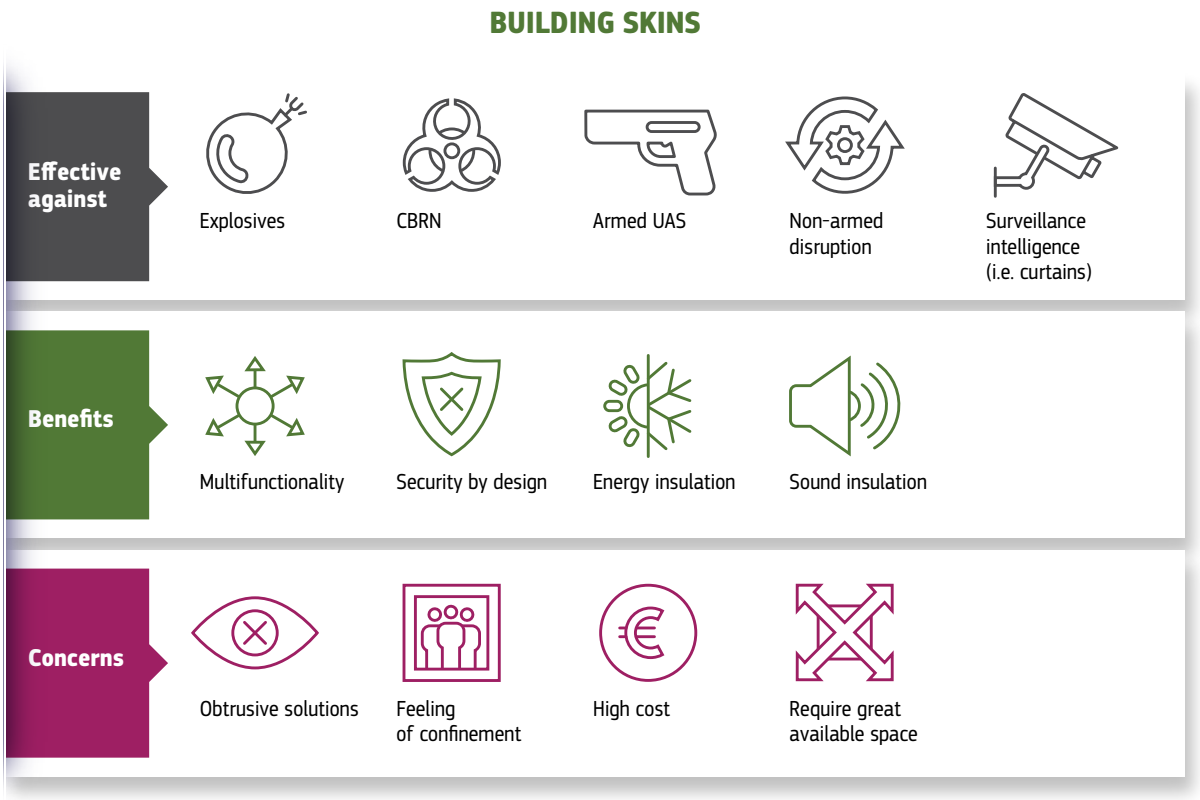
The presence of louvers positioned at a certain distance from the building's facade, as seen in Figure 27, also guarantees the increase of the minimum

distance between a malicious UAS and the building occupants. The same effect is achieved by the integration of other architectural and design elements, such as the double-skin facades. These systems are composed of two layers (usually both made of glass) and have become popular in the last decades, especially in high-rise buildings, as they can effectively reduce building energy demands. The space between the two layers, which varies from some dozens of centimetres up to a couple of metres, allows the air to circulate (either naturally or mechanically) and provides insulation against extreme temperature conditions and noisy environments. Figure 28 shows two typical cases of double-skin buildings, where the external building layer is made of glass to allow for a clear view and the presence of natural light.

Figure 28: Examples of double-skin office buildings in Wroclaw, Poland (left) and Milan, Italy (right)

It may be noticed that the currently presented measures were primarily developed without bearing in mind the risk posed from UAS-driven threats, as they were aiming at improving occupant comfort, reducing heating costs or mitigating the consequences of an explosion on a building's exterior (non UAS related). Nonetheless, their utility is not limited to their original design purpose and may serve as multifunctional elements that may also provide protection against various UAS-driven attacks. The fact that these systems obstruct the view to the building interior (depending on the transparency of the external skin material) means that they can also be used to conceal individuals, such as VIPs, from intended assassination attempts using armed UAS. Moreover, it makes it more difficult for intelligence and/or surveillance UAS trying to engage in espionage activities to gather information. Monitoring a target from a distance (e.g. video recording, eavesdropping) and documenting vulnerabilities becomes more challenging if an additional layer is present, as the UAS cannot approach its target at a close range. Additionally, as already mentioned, the presence of a second skin increases the distance of a potential explosive device carried by a drone from the building occupants and therefore significantly reduces the consequences of an explosion. Ultimately, the duality of these solutions is in line with the security-by-design principles, which call for the endorsement of multifunctionality and harmonic integration with the surrounding environment. Figure 29 provides an overview of the attack scenarios where the presented building skins may be efficiently employed and indicates a number of issues to be considered before being adopted.

Figure 29: Effectiveness and considerations from the use of anti-drone building skins against UAS-driven attacks



3.3.4 Attenuation solutions

Protecting information from theft or destruction is a challenging task, as electronic systems emit electromagnetic radiation and, therefore, a potential attack does not demand an electronic or software connection. An antenna installed in proximity to a computer can detect the emanating signal if it is strong enough and reconstruct the generated information. As the signal intensity decreases rapidly with increasing distance, drones can be used by an aggressor to bring an antenna or a similar device closer to the information source. Similarly, a small-sized bug may be carried as close as possible to the source, in order to eavesdrop on conversations. Modern UAS are becoming much smaller in size, achieve greater range and are more reliable, which means that they can fly, in many cases, undetected and approach facilities handling sensitive/classified data or hosting confidential conversations. Therefore, they can serve as the means for hacking nearby Wi-Fi or other wireless networks and use infrared microphones to overhear conversations.

Metallised window films, as a result of their metal content, can provide substantial shielding against electromagnetic fields and therefore reduce or even eliminate the emanating signals. Such measures have been gaining popularity due to the fact that drones can easily reach facilities that, up to date, were considered safe, and consequently stakeholders had to revolutionise their protective strategy. Such films can be effectively used for blocking emissions from within an enclosed space even through glass, while at the same time maintaining outward visibility. This means that they provide RF, infrared and electromagnetic field attenuation, without having visible aesthetic effects. As a result, they protect sensitive information and confidential data from being breached by preventing attempts to spy on electronic communications and reduce the probability of successful electronic eavesdropping attacks. Moreover, they are usually paired with UV protection characteristics or even anti-intrusion protection.

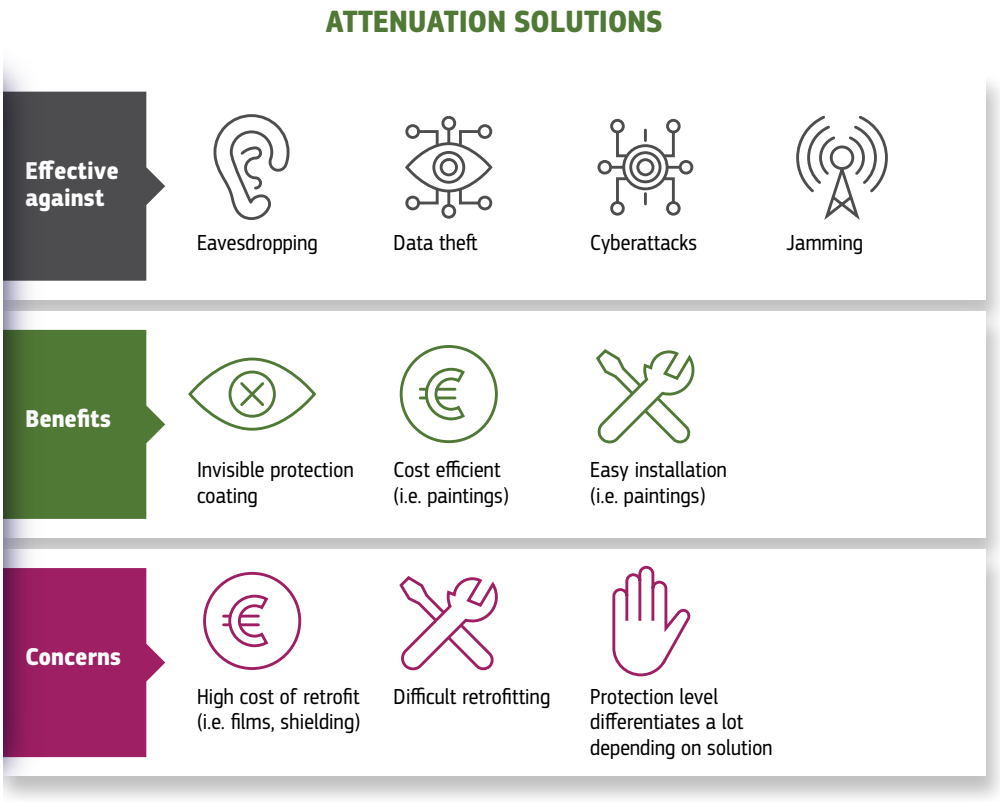
Such attenuation films are applied directly to the interior of a glass, similar to the ASFs, irrespective of the window geometry. Its size needs to fit the one of the window frame and should preferable be installed as a single piece to achieve a better visual outcome. Their protection capabilities depend on various factors, including their thickness, properties and metal content. The assessment of their effectiveness may be performed through dedicated test methods (ASTM F3057-16 or the IEC061000-5-7:2001) that also provide classification procedures for various degrees of protection.

Apart from windows that form the most vulnerable part in terms of RF leakage, the surrounding components of a room or a building (i.e. walls, roof, floors and doors) may also be properly protected to block espionage, cyberattacks and security breaches. This is usually achieved through a metallic shield (e.g. metallised fabric wallpaper) that encircles the room, creating a type of Faraday cage and specialised shielded doors. Metallic meshes that can be installed within walls, glued on concrete surfaces or laid underneath the roof may also be used. Similarly, shielding textiles that resemble curtains or mosquito nets may be introduced behind windows, but need to always remain in place to be efficient.

Figure 30: Metallic foil applied as an interlayer in the walls surrounding the sensitive area

ontaining the electromagnetic and infrared emanations within a room can also be achieved with the use of conductive paints, which can be applied with a spray gun or with a roller on walls and ceilings. Their advantages are their low cost, their adaptability to different room designs, their easy application and the fact that they can be painted over with normal architectural paints. The effectiveness of these conductive coatings depends on their composition, but overall they provide an efficient alternative to selective plating or metallic meshes.

Figure 31: Effectiveness and considerations from the use of attenuation solutions



3.3.5 Concealment and repositioning

Camouflaging, concealing, encasing and repositioning various assets that may be the target of a UAS-driven attack might prove to be one of the most cost-efficient methodologies for mitigating the consequences of a potential incident. The risk-assessment process that was described earlier is able to identify the vulnerable elements in the examined facility that put the public and/or structure at greater risk. Such elements may be camouflaged to hide them from the drone's line of sight by employing landscape materials, furniture or other visual obstructions, while signs pointing to critical utilities should be minimised. This form of site planning and landscape design may be performed following the key principles of security by design, ensuring the integration of multifunctional, sustainable and aesthetical elements into the design security plan.

3.3.5.1 Repositioning actions

UAS-driven attacks may have numerous different objectives, including (but not limited to) causing victims harm, obtaining sensitive information, generating panic reactions and provoking reputational damage. Repositioning assets that may be the target of an aggressor decreases their vulnerability and substantially reduces the impact of a successful attack (deterrence potential also increases since the target becomes unattractive). For instance, moving a high-risk, open-air event to the interior of a structure substantially reduces the relevant risk, as it eliminates the ability of the UAS to approach the gathered crowd and conduct an attack. Similarly, the approach route and access of a VIP to a facility may be altered at regular intervals, so it becomes harder for a UAS operator to predict where to focus its attention. As already mentioned, the explosion of an IED on the exterior of an unprotected or partly protected window leads to the creation of glass fragments that are propelled inside the adjacent room, leading to significant injuries and victims. Repositioning offices and building occupants so they are located at a greater distance from exterior windows reduces the relevant risk, as

the fragments quickly lose their lethal potential due to the increased distance they have to cover. Moreover, the ability of a UAS, equipped with appropriate sensors, to conduct a cyberattack is greatly influenced by the distance of the cyber-vulnerable items from the drone, and therefore moving such elements away from the surrounding windows reduces the risk of a successful local-network hacking and manipulation of sensitive data.

3.3.5.2 Concealment actions

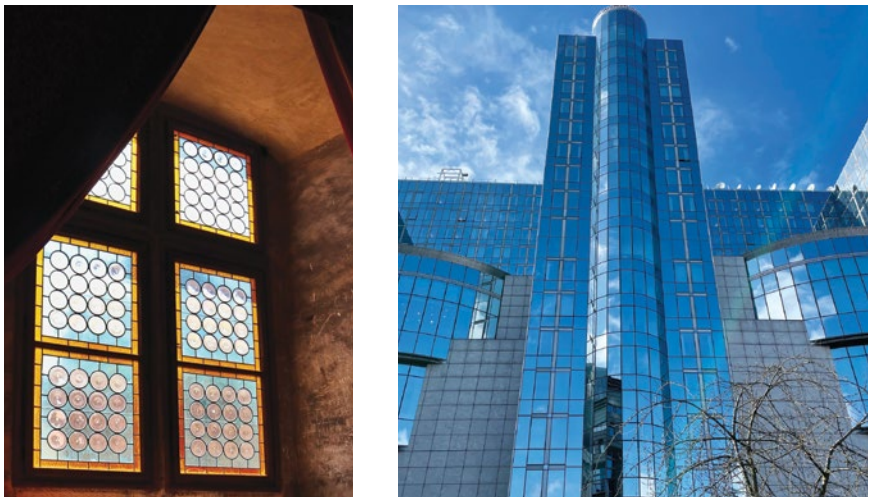
Privacy glasses, films and blinds are also a way to block the view of a UAS carrying a camera inside a facility, and therefore protect against privacy breaches, acquisition of sensitive information, the appropriate placement of microphones or other sensors, and can even safeguard from firearms (i.e. killer drones) and IED attacks, since the target is not visible.

Various types of opaque glasses and films that offer different levels of opacity are available on the open market.

- Translucent glass is produced by sandblasting or acid-etching, creating a marked surface on one side of the glass pane. Light can still pass through, so images are not completely hidden, but are blurred.
- Textured glass has a design or pattern engraved on the glass pane. The light can still pass through, but images are distorted.
- Tinted/coloured glass is actually crystal clear, but the addition of colour makes it opaque. Darker colours increase the amount of privacy, but images can still be recognised.
- Smoked glass, like coloured glass, is clear and its dark colour makes viewing more difficult, but it does not completely block the view from the building's exterior.
- Glass bricks are thick blocks of glass that allow natural light to pass through, but distort the images due to their texture.
- Smart glasses combine certain characteristics from the previously mentioned categories, as their opacity level can change by an external stimulus, such as voltage. These glasses turn from transparent to opaque through the pressing of a button.
- Mirror films are adhesive and have a metallised layer, providing a mirrored appearance reflecting the light and offering extremely high level of opacity. They provide great daytime privacy as they reflect the glass' brightest side (i.e. the sun in daytime conditions) and allow for a one-way viewing from the side with the least light. At night, the level of reflection drops substantially, especially if the room to be protected has bright lights, even though the film can still reflect a certain amount or ambient glow from street lights and city glow.

A side effect of these glass and film solutions is their ability to provide heat insulation by reducing the amount of heat entering the building, since sunlight is reflected away from the facade and therefore the air-conditioning requirements are limited. The combination of different glass layers and security solutions (e.g. catching systems) is also possible to enhance their blast-protection, intrusion or bullet-protection characteristics.

Figure 32: Examples of textured/coloured glass (left) and glass equipped with mirror films (right)



A simple and cost-efficient solution that may provide great concealment is the integration of privacy blinds, shutters, shades or drapes equipped with blackout linings, to completely block the view from the building's exterior. Fabrics that are lighter in colour and weight do not entirely block natural light, and a drone with a mounted camera can still distinguish shapes from the room's interior, an effect that becomes more pronounced during night-time if the room is brightly lit. Moreover, external shutters could be closed electronically or manually in the event of a UAS detection to block the view to the inside of the building. It is clear that such solutions are effective if they stay in a closed position, inevitably limiting the amount of light entering the room. However, the type, colour and shape of the preferred solution can be adjusted so as to be in line with the interior design of the room. Remaining in the open position to allow for more light is an option that increases the risk, as they have to be closed after detecting a UAS in the vicinity of the building. This means that an effective and swift detection mechanism, complemented by an appropriate awareness campaign, has to be in place to inform occupants on how to proceed with the closing of the adopted solutions in the event of a security incident.

Figure 33: Examples of window aluminium shutters (left) and dark-coloured drapes (right)

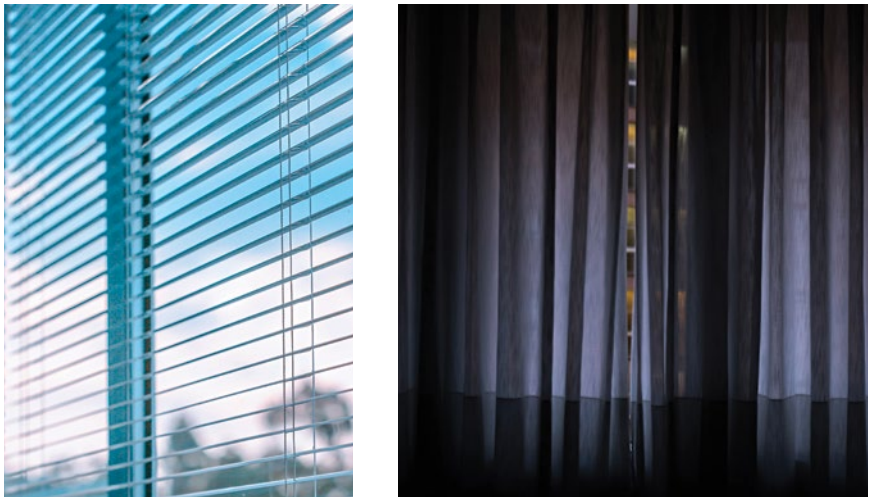
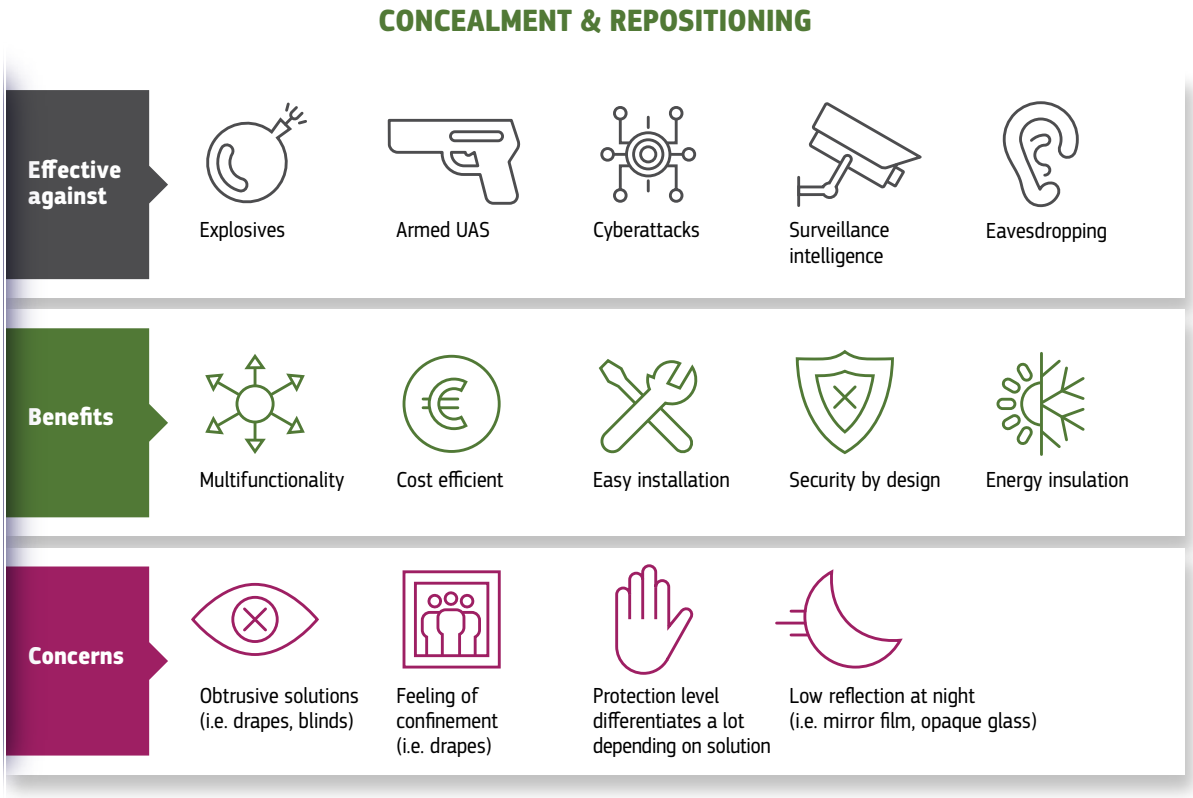


Figure 34 provides an overview of the attack scenarios where the presented concealment and repositioning methodologies may be efficiently employed and indicates a number of issues to be considered before being adopted.

Figure 34: Effectiveness and considerations from the use of concealment and repositioning methodologies



3.3.6 Awareness raising, geofencing and identification potential

The majority of drone incidents in Europe are currently related to negligent and reckless use, without excluding intentional malicious acts. Different measures may be employed to limit such occurrences but may prove inadequate against determined aggressors, as they can be easily bypassed or ignored. Such measures include:

- awareness raising and communication building;
- geofencing;
- increasing identification and response potential.

It is important to come in contact with local businesses, employees and residents in an effort to increase their awareness on the concerned risks due to the malicious use of drones and educate them on the appropriate response in the event of a sighting. Security resources are usually limited, so reliable reporting of suspicious activities from private entities and citizens, including the observed UAS location, description and behaviour, is a key aspect for accomplishing a precise and swift response from the law enforcement units. Engaging the local community and staff to be part of the detection effort may also be performed through communication campaigns (i.e. social media, internet) and the placement of signage, such as the one shown in Figure 34, constraining UAS use in certain

zones. Such signage shows facility visitors and staff that their reaction to sightings is priceless for raising the security level, and it helps authorities in their effort to fight illegal and irregular operator behaviour. Moreover, it demonstrates to potential aggressors the active engagement of the community on collective protection efforts and therefore deters their malicious activities.

EU Member States have authorities that are responsible for handling limitations in the airspace and control the flights of manned or unmanned aircrafts. Such flight prohibitions already exist around critical facilities (e.g. nuclear factories, refineries), military sites, airports and prisons. In certain cases, operators and organisations can request the relevant authority to include their facility in their list of restricted areas (if not already included) or even issue a temporary flight restriction due to an event or heightened threat incident. The information regarding the zones with the flight constraints is then transmitted to UAS manufacturers who embed it into a geofencing software pre-installed in off-the-shelf drones and is updated at regular intervals. Such software ensures that UAS cannot be operated in a restricted airspace, creating an invisible barrier around the area. However, this does not mean that every airspace included in a national list of restricted areas is automatically protected, especially against malicious acts. The software can easily be hacked, circumvented or not updated by determined actors, as it is based on the combination of the GPS network and the UAS's Wi-Fi or Bluetooth connection. Nevertheless, it can still be valuable in preventing incidents stemming from reckless and negligent UAS use.

Figure 35: Examples of UAS warning signs

The development of a robust planning and training scheme is of high importance for security and law enforcement units to reinforce their UAS identification and intervention potential. Such a plan can build the required capabilities through dedicated training and exercises in terms of reporting procedures, response plans, roles and responsibilities, technology exploitation, coordination and collaboration. The overarching goal is to build a protection strategy that will involve operators of potential targets, citizens and authorities to collectively help increase the resilience of public spaces or infrastructures against UAS-driven threats. More information regarding this planning process can be found in the handbook on the protection of critical infrastructure and public spaces (Hansen and Pinto Faria, 2023).

4 Conclusions

The current handbook seeks to raise awareness and inform both state and private stakeholders to update their protection strategy in response to threats and challenges arising from actors with criminal or terrorist intent, who employ UAS to conduct an attack. A number of different UAS-driven threats against a building infrastructure and public spaces have been collected, adapted and presented in this document, focusing on the principles that guided the selection and installation of appropriate physical protective measures. As is highlighted, the adoption of digital technologies poses great challenges as relying on a sole technology is highly unlikely to safeguard against all different UAS types and models. Consequently, physical hardening is an alternative and attractive protection strategy that may effectively integrate different measures, which combine certain advantages within a broad multi-threat framework.

A thorough, structured risk-assessment approach is essential for establishing a comprehensive understanding of the influencing parameters of UAS-related threats. Despite the infrequent malicious use of drones in Europe, the many incidents due to clueless or careless users, in combination with the UAS growing capabilities, calls for a robust assessment that may estimate the severity of potential consequences, track the target's vulnerabilities and evaluate the incident's probability of occurrence. The proposed analysis focuses exclusively on UAS-driven attacks and its outcomes serve as input for comparing the relative probability of the different attack tactics and their impact, facilitating the decision on potential actions. Clearly, risk cannot be completely eliminated, as full protection is a chimera in both economic and technical terms, so decision-makers need a clear definition of 'acceptable'.

To counter complex and rapidly evolving UAS-driven threats, it is important to prepare for aggressor tactics that were not considered in the past and respond dynamically by investing in a variety of available solutions. Careful consideration is required when selecting digital counter technologies, as legal restrictions, lack of common testing protocols, need for operator presence and costly maintenance may result in operational constraints and ineffectiveness. The response to this multifaceted threat posed by the misuse of UAS depends greatly on the operating environment, the location and mission of the infrastructure or public space, along with the regulatory and legal framework in each Member State.

The proposed physical hardening solutions can form a basis, allowing for the development of a reliable protection strategy. The majority of these measures have not been exclusively developed for the threats posed by UAS-driven attacks, but have been adjusted to provide effective protection against such threats. Due to their existence preceding the UAS threat, their effectiveness has been extensively tested during security incidents and several standards have been developed for evaluating their performance. In many cases, their multifunctional nature means that they can serve several occupant needs, leading to long-term cost effectiveness and harmonic integration to the surrounding architecture, following the principles of security by design. The collected and adjusted information can help security officers and engineers to build their physical hardening strategy in an orderly manner, overcoming the obstacle posed by the fragmented information that usually characterises this field.

References

American Society for Testing and Materials (2017), ASTM F1642, *Standard test method for glazing and glazing systems subject to airblast loadings*.

Bedon, C., Markovic, D., Karlos, V. and Larcher, M. (2023), *Numerical Investigation of Glass Windows Under Near-field Blast,* European Commission, Joint Research Centre, Publications Office of the European Union, Luxembourg, JRC 133288.

Centre for the Protection of National Infrastructure (2013), 'Guidance note: Peel adhesion testing and assessment of anti-shatter film (ASF)', CPNI EBP 10/13.

ENCO, Belgian Nuclear Research Centre and International Security and Emergency Management Institute (2019), *Mapping C-UAS Capabilities Now and in the Future – A prospective view on mitigating the UAS threat,* European Commission, HOME/2017/ISFP/FW/CBRN/0086 (limited).

European Commission (2017), Commission communication – Action plan to support the protection of public spaces, COM(2017) 612 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX %3A52017DC0612.

European Commission (2019a), Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems, *Official Journal of the European Union,* L 152, Publications Office of the European Union.

European Commission (2019b), Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft, *Official Journal of the European Union,* L 152, Publications Office of the European Union.

European Commission (2020), Commission communication – A counter-terrorism agenda for the EU: anticipate, prevent, protect, respond, COM(2020) 795 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:795:FIN

European Commission (2022), Commission communication – A drone strategy 2.0 for a smart and sustainable unmanned aircraft eco-system in Europe, COM(2022) 652 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022DC0652&qid=1682336605326.

European Commission (2022), *Security by Design: Protection of public spaces from terrorist attacks,* Joint Research Centre, Publications Office of the European Union, Luxembourg.

European Committee for Standardization (1999a), EN 356:1999, *Glass in building – Security glazing – Testing and classification for resistance against manual attack*.

European Committee for Standardization (1999b), EN 1063:1999, *Glass in building – Security glazing – Testing and classification of resistance against bullet attack.*

European Committee for Standardization (2001), EN 13123-1:2001, *Windows, doors and shutters – Explosion resistance – Requirements and classification – Part 1: Shock tube.*

European Committee for Standardization (2002), EN 12600:2002, *Glass in building – Pendulum test – Impact test method and classification for flat glass.*

European Committee for Standardization (2004), EN 13123-2:2004, *Windows, doors and shutters – Explosion resistance – Requirements and classification – Part 2: Range test.*

European Committee for Standardization (2012), EN 13541:2012, *Glass in building – Security glazing – Testing and classification of resistance against explosion pressure.*

European Defence Agency (2018), *A conceptual analysis of hybrid threats in the context of countering minidrones,* Mass Consultants Limited (limited).

European Parliament and Council (2018), Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91, *Official Journal of the European Union,* L 212, Publications Office of the European Union.

Hansen, P. and Pinto Faria, R. (2023), *Protection against Unmanned Aircraft Systems: Handbook on the protection of critical infrastructure and public spaces,* European Commission, Joint Research Centre, Publications Office of the European Union, Luxembourg, JRC 132714.

International Organization for Standardization (2007), ISO 16933:2007, *Glass in building – Explosion-resistant security glazing – Test and classification for arena air-blast loading.*

International Organization for Standardization (2018), ISO 31000:2018, *Risk management – Guidelines.*

Karlos, V. and Solomos, G. (2013), *Calculation of Blast Loads for Application to Structural Components,* Joint Research Centre, Publications Office of the European Union, Luxembourg.

Larcher, M., Karlos, V., Valsamos, G. and Solomos G. (2018), *Scenario Study: Drones carrying explosives,* European Commission, Joint Research Centre, Publications Office of the European Union, Luxembourg (limited), JRC 107683.

Larcher, M., Solomos, G., Casadei, F. and Gebbeken, N. (2012), 'Experimental and numerical investigations of laminated glass subjected to blast loading', *International Journal of Impact Engineering,* Vol. 39, No 1, pp. 42–50.

UNDSS (2021), *PSU Information Bulletin – Blast protection for windows,* Division of Specialized Operational Support, Physical Security Unit.

List of abbreviations

ASF	anti-shatter film
ASTM	American Society for Testing and Materials
CBRN	chemical, biological, radiological or nuclear
CEN	European Committee for Standardization
CPNI	Centre for the Protection of National Infrastructure
C-UAS	counter unmanned aircraft systems
EC	European Commission
EU	European Union
HVAC	heating, ventilation and air conditioning
IED	improvised explosive device
ISO	International Organization for Standardization
JRC	Joint Research Centre
MTOM	maximum take-off mass
RF	radio frequency
UAS	unmanned aircraft system
UNDSS	United Nations Department for Safety and Security
UV	ultraviolet
VIP	very important person

List of figures

List of tables

GETTING IN TOUCH WITH THE EU

IN PERSON

All over the European Union there are hundreds of Europe Direct centres. You can find the address of the centre nearest you online (european-union.europa.eu/contact-eu/meet-us_en).

ON THE PHONE OR IN WRITING

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

- **by freephone:** 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),
- **at the following standard number:** +32 22999696,
- **via the following form:** european-union.europa.eu/contact-eu/write-us_en.

FINDING INFORMATION ABOUT THE EU

ONLINE

Information about the European Union in all the official languages of the EU is available on the Europa website (european-union.europa.eu).

EU PUBLICATIONS

You can view or order EU publications at op.europa.eu/en/publications. Multiple copies of free publications can be obtained by contacting Europe Direct or your local documentation centre (european-union.europa.eu/contact-eu/meet-us_en).

EU LAW AND RELATED DOCUMENTS

For access to legal information from the EU, including all EU law since 1951 in all the official language versions, go to EUR-Lex (eur-lex.europa.eu).

OPEN DATA FROM THE EU

The portal data.europa.eu provides access to open datasets from the EU institutions, bodies and agencies. These can be downloaded and reused for free, for both commercial and non-commercial purposes. The portal also provides access to a wealth of datasets from European countries.

The European Commission's science and knowledge service

Joint Research Centre

JRC Mission

As the science and knowledge service of the European Commission, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle.

EU Science Hub
joint-research-centre.ec.europa.eu

@EU_ScienceHub

EU Science Hub-Joint Research Centre

EU Science, Research and Innovation

EU Science Hub

EU Science

Publications Office
of the European Union