Countering the Drone Threat

Implications of C-UAS technology for Norway in an EU and NATO context

This report provides a critical analysis of the typology, procedures, and challenges of counter-drone technology, as well as an assessment of its application in both civilian and military scenarios. Counter-drone technology – or, as it is also designated, C-UAS – refers to systems designed to detect, track, identify and/or intercept unmanned aircraft (commonly referred to as drones), particularly small drones that cannot be countered with traditional anti-aircraft systems designed for use against manned aircraft.

The report argues that C-UAS technology is often not fully effective, and that those wishing to use the technology face a range of hurdles with respect to legality, coordination, planning, and safety. Current legal frameworks are lagging behind technological developments, and therefore many of the available technological solutions cannot be used in civilian settings due to legal restrictions.

Malicious drone use represents a significant security challenge. However, policymakers and practitioners should be careful not to allow this challenge to trigger an over-zealous securitization of civilian airspace.

Drones offer a range of important benefits when used properly. While a balanced approach towards C-UAS is certainly difficult to achieve, it is important that policy-makers, regulators, and law enforcement agencies take both the risks and the opportunities of C-UAS into account in their strategic decision-making.
Countering the Drone Threat
Implications of C-UAS technology for Norway in an EU and NATO context

Bruno Oliveira Martins
*Peace Research Institute Oslo (PRIO)*

Arthur Holland Michel
*Center for the Study of the Drone, Bard College*

Andrea Silkoset
*Peace Research Institute Oslo (PRIO)*
Funding

*Research for this report was funded by the Norwegian Ministry of Defence.*
1. Executive Summary

This report provides a critical analysis of the typology, procedures, and challenges of counter-drone technology and an assessment of its application in both civilian and military scenarios that are relevant to Norway. Counter-drone technology – or, as it is also designated, C-UAS – refers to systems designed to detect, track, identify and/or intercept unmanned aircraft (commonly referred to as drones), particularly small drones that cannot be countered with traditional anti-aircraft systems designed for use against manned aircraft. While portions of this report focus on Norwegian legal frameworks and strategic documents, they nevertheless raise questions that are widely applicable in many other geographical contexts.

The report argues that C-UAS technology is often not fully effective, and that those wishing to use the technology face a range of hurdles with respect to legality, coordination, planning, and safety. As normally happens with emerging technologies, the current legal frameworks are lagging behind technological developments, and therefore many of the available technological solutions cannot be used in civilian settings due to legal restrictions.

As drone technology has proliferated, concerns have grown regarding the potential safety and security threat that it poses. With respect to the civilian context, the report covers legal, societal, and institutional issues in three different scenarios: drones in proximity of a large crowd in an urban area, nuisance or nefarious drone usage at an airport, and a drone attack at a Norwegian oil platform. Regarding the military context, the report highlights the protection of critical military infrastructure, the defence of Norwegian and allied forces abroad, and challenges and opportunities in multinational force deployment. The report then proceeds to explore the most recent C-UAS-related developments taking place at the EU and NATO levels in order to provide a more comprehensive understanding of the international legal, regulatory and strategic environments that impact Norway’s decision-making on the issue.

Norway is adapting to this new threat environment by mobilizing human and financial resources and by reforming regulatory and legislative frameworks. This is taking place in both its civilian and its military spheres. Such efforts often entail cooperation between these two environments, and from this perspective, some of the strategies being explored to address the drone threat involve the erosion of a strict separation of civil and military organizations and practices.

Recent EU and NATO frameworks and initiatives provide important opportunities to bring Norway closer to the technological leading-edge in C-UAS and to participate in setting international best practices. Through its security research programme, the upcoming European Defence Fund, and the Permanent Structured Cooperation (PESCO) scheme, the EU is investing financial and political capital in developing C-UAS technology. These programmes are open to Norwegian participation, and could enhance domestic C-UAS integration and R&D.

Malicious drone use represents a significant security challenge for Norway. However, policymakers and practitioners should be careful not to allow this challenge to trigger an over-zealous securitization of civilian airspace. The need to ensure security and safety in the airspace needs to be balanced with broader societal implications. C-UAS technology raises privacy concerns, and can lead to psychological stress and to elevation of threat perception. For these reasons, decision-making processes behind C-UAS acquisition and use must factor in societal impact assessments. This applies to both private actors and public authorities.
Drones offer a range of important benefits when used properly, and C-UAS efforts must be cautious not to overly inhibit such benefits. Likewise, the improper use of C-UAS raises troubling concerns around safety, legality, privacy, coordination and planning, and airspace integration.

While a balanced approach towards C-UAS technology is certainly difficult to achieve, it is important that policy-makers, regulators, and law enforcement agencies take both the risks and the opportunities of C-UAS into account in their strategic decision-making.
2. Introduction

Over the last years, drone technology has become increasingly common in both civilian and military contexts. It has been used extensively for a range of applications, including disaster response, monitoring, precision agriculture, inspections, recreation, surveillance, and topographical surveying and mapping, and it has been used in a host of different military contexts, from surveillance and reconnaissance to kinetic operations. Unmanned aircraft have been employed by state and non-state actors alike in recent conflicts, and over the past few years, drone sightings close to airports have caused major disruption and resulted in multiple international airports having to temporarily shut down their operations.

As drone technology has proliferated, concerns have grown regarding the potential safety and security threat that it can pose. These concerns have spurred intense interest in counter-drone systems (C-UAS), which are technologies that are designed to detect, track, identify and/or intercept unmanned aircraft, particularly those small unmanned systems that cannot be countered with traditional anti-aircraft systems designed for use against manned aircraft. Like any other country around the world, Norway will increasingly have to contend with such threats in a range of different contexts over the coming years, and will invest significant resources and effort in the integration of C-UAS systems and practices.

In the military domain, small drones have been proliferating at a rate that has alarmed battlefield commanders and planners alike. At least 95 countries now possess drones, which can potentially furnish even poorly funded state actors with an aerial command of the battlespace that was previously only available to those possessing a sophisticated aircraft programme. Drones are also becoming a common weapon for non-state groups that employ the technology for surveillance, battlespace management, propaganda, and aerial strike attacks, often to considerable effect. As a result of the proliferation of this technology, counter-drone systems will become a ubiquitous weapon in all future conflicts, and could play a critical role in future Norwegian military operations.

In the civilian domain, the threat of small unmanned aircraft is no less troubling, and counter-drone systems are likewise set to figure as an important tool for security and law enforcement in the years ahead. With relatively simple modifications it is possible, for example, to convert cheap ‘off-the-shelf’ consumer drones and hobby kit aircraft into rudimentary yet potentially lethal guided missiles or other airborne attack systems. Other dangerous and/or criminal uses of drones include surveillance and counter-surveillance, smuggling, and reckless interference with manned air traffic, particularly at airports. Norway has not been spared from such threats. In 2019, forty incidents of rogue drone use in proximity of an airport were reported, and the possibility of other drone-related incidents might be regarded not so much as a matter of ‘if’ but ‘when’ – a few such potential scenarios are described at length in the chapter ‘Civilian Scenarios’.

For all organizations wishing to adopt C-UAS, this technology poses several significant and unresolved challenges. These range from considerations around effectiveness and safety through legal obstacles and privacy concerns. Addressing these challenges will be fundamental to Norway’s efforts to mitigate the threat of rogue and adversary drone use.

---


This report provides an analysis of the C-UAS technological state-of-the-art, focusing on typology, procedures, and challenges, and elaborates on the different civilian and military scenarios of relevance to Norway. On the civilian front, the report covers legal, societal, and institutional issues in three different scenarios: drones in proximity of a large crowd in an urban area, nuisance or nefarious drone usage at an airport, and a drone attack at a Norwegian oil platform. With respect to the military context, the report highlights the protection of critical military infrastructure, the defence of Norwegian and allied forces abroad, and challenges and opportunities in multinational force deployment. The report then explores the most recent C-UAS-related developments taking place at the EU and NATO levels in order to provide a more comprehensive understanding of the international legal, regulatory and strategic environment that impacts Norway’s decision-making on the issue.

While portions of this report focus on Norwegian legal frameworks and strategic documents, they nevertheless raise questions that are widely applicable in many other geographical contexts. As the report will show, many C-UAS solutions are ineffective in a real-world situation, and in most cases they cannot be used in civilian settings due to current legal restrictions. This points to important unresolved vulnerabilities in Norway and beyond, both in civilian and military settings. Yet at the same time, this conclusion should not trigger processes of securitization of civilian airspace. The need to ensure security and safety in the airspace needs to be balanced with broader societal implications. Drones offer a range of important benefits when used properly, and C-UAS efforts must be cautious not to overly inhibit the enjoyment of such benefits. Likewise, the improper use of C-UAS raises troubling concerns around safety, legality, privacy, coordination and planning, and airspace integration. While this balancing is certainly difficult to achieve, it needs to remain at the centre of the strategic thinking of policy-makers, regulators, and law enforcement agencies.

2.1. Methodology

This report is largely based on background interviews with dozens of stakeholders, regulators, law enforcement agents and technology developers in Norway, in other European countries, in the United States, and within international institutions such as NATO and the EU. The project team members participated in a number of international technology exhibitions and conferences in Norway (Unmanned Nordic Conference, Oslo, November 2019) Europe (Amsterdam Drone Week, December 2019, and the European Commission’s High-Level Conference on Countering threats posed by unmanned aircraft systems, Brussels, October 2019) and the United States (Xponential, Chicago, IL, April 2019), where they interacted with different actors in the C-UAS environment and acquired specialized knowledge about the technological state-of-the-art.

In Norway, research for this report benefitted from interviews, informal talks, email exchanges and phone conversations with practitioners from the Norwegian Ministry of Defence, the Bomb Squad at the National Police Special Response Unit / Oslo Police District, the Civil Aviation Authority of Norway (Luftfartsstilsynet), Avinor, and UAS Norway, as well as with other security consultants and drone technology researchers from the private sector in Norway and other Scandinavian countries.

Throughout 2019, team members attended high-level meetings convened, inter alia, by the European Commission and NATO, and have presented ongoing research in these settings. Preliminary findings of the research were also discussed at a meeting organized in September 2019 by the Norwegian Ministry of Defence.
This report benefits from a close collaboration with the Center for the Study of the Drone at Bard College, in the U.S., and leverages the research carried out for the second edition of the report *Counter-Drone Systems*,³ published in December 2019 by Arthur Holland Michel. The latter publication is based on open-source research of technical and policy reports, written testimony, news and analysis pieces, and manufacturer information; background interviews with government and law enforcement officials, industry representatives, and subject matter experts; and participation in both public and closed conferences and workshops. It puts forward a database of more than 500 C-UAS solutions available in the market. This is the most comprehensive database of C-UAS solutions to date, and it constitutes the basis for the analysis conducted in the present report. The following chapter on typology, procedures, and challenges of C-UAS technology reproduces and adapts parts of the report *Counter-Drone Systems*, second edition.

---

3. C-UAS Technology: Typology, Procedures, and Challenges

Rogue and malicious drone use is a novel threat that cannot be addressed with traditional defence and security systems. The air defence infrastructures that have traditionally been used to protect airspace are mostly designed with inhabited aircraft in mind – that is, they are optimized for detecting, tracking, and shooting down large fast-moving objects. As a result, they cannot always pick up small, slow, low-flying drones. In Norway’s civilian airspace, like all other airspace systems around the globe, drones are not yet required to carry transponders, so they cannot be detected and tracked with existing air traffic control systems. Relying on visual observation to detect drones is equally ineffective; at a distance of several hundred feet, drones can become all but invisible to the naked eye. Designed-for-purpose C-UAS systems rely on a variety of techniques for detecting and/or intercepting drones. This section describes the main detection and interdiction methods employed by products currently available on the market, as well as the principal platform types.

Table 1: Detection, Tracking, and Identification Systems

<table>
<thead>
<tr>
<th>Detection, Tracking, and Identification Systems</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Radar</td>
<td>Detects the presence of small unmanned aircraft by their radar signature, which is generated when the aircraft encounters radio frequency pulses emitted by the detection element. These systems often employ algorithms to distinguish between drones and other small, low-flying objects, such as birds.</td>
</tr>
<tr>
<td>Radio-frequency (RF)</td>
<td>Detects, locates, and in some cases identifies nearby drones by scanning for the frequencies on which most drones are known to operate.</td>
</tr>
<tr>
<td>Electro-optical (EO)</td>
<td>Identifies and tracks drones based on their visual signature.</td>
</tr>
<tr>
<td>Infrared (IR)</td>
<td>Identifies and tracks drones based on their heat signature.</td>
</tr>
<tr>
<td>Acoustic</td>
<td>Detects drones by recognizing the unique sounds produced by their motors. Acoustic systems rely on a library of sounds produced by known drones, which are then matched to sounds detected in the operating environment.</td>
</tr>
<tr>
<td>Combined Sensors</td>
<td>Many systems integrate a variety of different sensor types in order to provide a more robust detection, tracking, and identification capability.</td>
</tr>
</tbody>
</table>

4 Even though the emergence of small, low-flying, unmanned aircraft poses a new challenge that cannot fully be addressed with existing air defences alone, many legacy air defence and electronic warfare weapons do figure as a component of a ‘layered’ approach to C-UAS that many established militaries appear to be adopting. Furthermore, many dedicated counter-drone products are based on existing air defence technologies, particularly radar and counter-mortar systems.

5 In an effort to facilitate the integration into Norwegian airspace, Avinor signed a contract in January 2020 for a new air traffic management ecosystem, Unmanned Aircraft System Traffic Management (UTM), which will be tested at three airports. For more information, see www.uasnorway.no/utm-kontrakt-signert-dette-betyr-det-for-deg-som-droneoperator/.
### Table 2: Interdiction Systems

<table>
<thead>
<tr>
<th>Interdiction Systems</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RF Jamming:</strong></td>
<td>Disrupts the radio frequency (RF) link between the drone and its operator by generating large volumes of RF interference. Once the RF link, which can include WiFi links, is severed, a drone will usually either descend to the ground or initiate a ‘return to home’ manoeuvre.</td>
</tr>
<tr>
<td><strong>GNSS Jamming</strong></td>
<td>Disrupts the drone’s satellite link, such as GPS or GLONASS, which is used for navigation. Drones that lose their satellite link will usually hover in place, land, or ‘return to home’.</td>
</tr>
<tr>
<td><strong>Spoofing</strong></td>
<td>Allows one to take control of, or misdirect, the targeted drone by feeding it a spurious communications or navigation link. (For our purposes, we include within this category a range of measures such as cyber-attacks, protocol manipulation, and RF/GNSS Deception).</td>
</tr>
<tr>
<td><strong>Dazzling</strong></td>
<td>Employs a high-intensity light beam or laser to ‘blind’ the camera on a drone.</td>
</tr>
<tr>
<td><strong>Laser</strong></td>
<td>Destroys vital segments of the drone’s airframe using directed energy, causing it to crash to the ground.</td>
</tr>
<tr>
<td><strong>High Power Microwave</strong></td>
<td>Directs pulses of high intensity microwave energy at the drone, disabling the aircraft’s electronic systems.</td>
</tr>
<tr>
<td><strong>Nets</strong></td>
<td>Designed to entangle the targeted drone and/or its rotors.</td>
</tr>
<tr>
<td><strong>Projectile</strong></td>
<td>Employs regular or custom-designed ammunition to destroy incoming unmanned aircraft.</td>
</tr>
<tr>
<td><strong>Collision Drone</strong></td>
<td>A drone designed to collide with the adversary drone.</td>
</tr>
<tr>
<td><strong>Combined Interdiction Elements</strong></td>
<td>A number of C-UAS systems also employ a combination of interdiction elements to increase the likelihood of a successful interdiction. For example, many jamming systems have both RF jamming and GNSS jamming capabilities in the same package. Other systems might employ an electronic system as a first line of defence and a kinetic system as a backup measure.</td>
</tr>
</tbody>
</table>
Table 3: Platform Types

<table>
<thead>
<tr>
<th>Platform Types</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ground-based:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Fixed</strong></td>
<td>Fixed systems are designed to be used from stationary positions on the ground.</td>
</tr>
<tr>
<td><strong>Mobile</strong></td>
<td>Mobile systems are designed to be mounted on vehicles and/or operated on the move.</td>
</tr>
<tr>
<td><strong>Hand-held</strong></td>
<td>Systems designed to be operated by a single individual by hand. Many of these systems resemble rifles or other small arms.</td>
</tr>
<tr>
<td><strong>UAV-based</strong></td>
<td>Systems designed to be mounted on drones.</td>
</tr>
</tbody>
</table>

3.1. Four Steps to Countering a Drone

Counter-drone technology can serve in a wide variety of roles. In wartime, the Norwegian Armed Forces may seek to employ C-UAS for protecting bases, naval vessels, convoys, and ground units. In civilian environments, counter-drone technology will primarily be used for securing the airspace around critical infrastructure, sensitive facilities, and large events such as party conventions and sports games, as well as for protecting VIPs and countering airborne smuggling at prisons.\(^6\) In any of these contexts, countering a drone is a complex, multi-step process involving interaction between several distinct systems and between those systems and the human operator(s).

1. First, a sensor system must detect, identify, locate, and track the incoming drone. Depending on the type of system used, a sensor that makes an initial detection, such as a wide-area radar or an RF detector, may have to ‘cross-cue’ to secondary sensors such as cameras or electronic identification elements to confirm that the detected object is in fact a drone, as well as determine its precise location and track its movements. Secondary sensors may also serve to provide additional information about the drone, which may help determine intent. For example, a camera may be able to show whether a drone appears to be carrying explosives. Certain electronic sensors may be able to additionally identify the location of the drone operator. Sensor data can often be stored for later use as evidence.

2. Based on the information from these sensors, a human operator must decide how to respond to the incoming drone. This may not always involve activating an interdiction system. For example, a federal law enforcement team operating a C-UAS system with mitigation capabilities at the 2019 Super Bowl found that they could usually just locate the operator of the drone and ask them to cease flying in the area.\(^7\) Particularly in civilian environments, C-UAS operators often describe mitigation as a ‘last resort’ measure. C-UAS teams may have a very limited window of time to make this decision.

---


3. A mitigation system is activated, and the drone is intercepted. Depending on the technique used, this could result in a range of effects, including the drone landing on the ground or activating a ‘return to home’ mode (in the case of jamming or spoofing), the capture of the drone (nets), or the complete or partial destruction of the drone (lasers, projectiles, collision UAVs, high-powered microwaves).

4. Depending on the circumstances, once a drone is intercepted the device may need to be isolated and retrieved. If the drone is potentially armed, an explosive ordnance disposal team may be called in to assess and, if needed, disable the device. Unarmed drones must likewise be treated with caution. If the device is damaged, its lithium-ion battery poses a risk of combustion. If the device continues to be functional, its rotors can pose a risk of injury. Those wishing to perform forensic analysis on the device may need to follow a series of steps to ensure that the integrity of the system and the potentially valuable data it carries are not compromised.

3.2. Challenges of Countering Drones

At present, the technical challenge of countering drones has not yet been fully surmounted. In a solicitation published in March 2019, the U.S. Defence Innovation Unit stated that ‘it has proven difficult to identify and mitigate threats using currently fielded technologies’. Dozens of background interviews with military and law enforcement personnel have validated this assertion. In the Norwegian context, as well as in other scenarios, the challenges posed by and to counter-drone technology extend beyond a simple matter of effectiveness. This section outlines the following challenges for counter-drone technology: detection effectiveness; false negatives and false positives; distinguishing legitimate and illegitimate drone use; limited response windows; interdiction hazards; interdiction effectiveness; advances in drone technology; lack of operational data; cost; legality; lack of standards; and privacy.

Detection Effectiveness

Every detection system has drawbacks. For example:

- Radar systems may struggle to pick out small drones and UAS flying very close to the ground.

- Camera systems might confuse a drone with a bird or an airplane, and may also struggle in adverse weather with low visibility, or if the drone is backlit by a strong light source such as the sun.

- Electro-magnetic interference can degrade the detection capabilities of RF sensors. In urban environments, there are many potential sources of such interference, including communications antennae, two-way radios, telemetry systems, and even power lines and LED lights.9

---

Certain RF sensors, including some systems marketed as ‘passive’ may likewise emit RF signals that could interfere with other communications, making them potentially dangerous to deploy in some environments.\textsuperscript{10}

Radar, certain RF systems, and EO/IR sensors must have a direct line of sight with the intruding drone in order to make a detection. This could be particularly problematic in urban environments, where a drone may only appear within a sensor’s line of sight for a couple of seconds before disappearing again.\textsuperscript{11}

Some detection systems may only be capable of providing a rough estimate of an incoming drone’s location.\textsuperscript{12}

Certain flight patterns – most notably hovering and moving vertically – can make drones harder to detect with automated tracking algorithms applied to radar or camera data.\textsuperscript{13}

Acoustic sensors rely on a library of sounds emitted by known drones, while RF detection systems likewise only detect certain frequency bands in a pre-established library. Given the rapid rate at which drones are emerging on the market and proliferating, even libraries that are updated often will never cover 100 percent of the drones that might be operating at any given time.

**False Negatives and False Positives**

In order to be useful, C-UAS detection systems must generate low levels of false negatives and false positives. This is difficult to achieve. C-UAS detection elements must be sensitive enough to detect all drones operating within the area of use, but systems that are too sensitive may create an overwhelming number of false positives, rendering the system unusable. According to the results of the U.S. Federal Aviation Administration (FAA) counter-drone systems testing, distinguishing true positives from false positives in cluttered environments requires ‘a high level of manpower’.\textsuperscript{14}

**Distinguishing Legitimate and Illegitimate Drone Use**

As Norway’s Civil Aviation Authority (CAA) continues to work to integrate routine drone use into the airspace, legitimate unmanned aircraft will become more common in the country’s skies. As such, it will become increasingly important for C-UAS operators to be capable of differentiating between legitimate and rogue drones. For example, in future editions of the 17 May children’s


parade in Oslo, the airspace may be crowded with legitimate aerial cinematography drones that do not pose a security risk alongside rogue drones that do. Particularly given the potential hazards of mitigating a drone in civilian environments, C-UAS operators will need to develop means to rapidly and reliably determine the threat level of an incoming drone based on the limited information provided by existing detection technologies.\(^{15}\) (Remote ID technology may go a long way to addressing this issue once implemented, but it will not be a total fix). In the military domain, this could also be an issue; a C-UAS system that cannot tell the difference between allied and adversary unmanned aircraft could accidentally shoot down friendly drones.

**Response Window**

Counter-drone operators may only have a very brief window of time to make a decision as to whether an incoming drone is indeed malicious. For example, imagine that a security team is protecting a large public gathering with a counter-drone system that has an effective identification range of 750 metres and an interdiction element that could pose a certain level of hazard to the crowd when activated (see following section). If a drone is travelling toward the crowd at 15 metres per second (a fairly standard speed for many commercial systems available on the market today), the team will have less than 50 seconds to decide upon an appropriate response. Thanks to advances in propulsion technologies, commercially available drones will become much faster in the years ahead, further reducing the viable response window for C-UAS.

**Interdiction Hazards**

Many – if not all – counter-drone interdiction techniques can be dangerous in certain circumstances. Drones that are intercepted by kinetic means may fall to the ground with considerable force. Even certain net-based systems that are equipped with a parachute to bring the ensnared drone down to the ground in a controlled manner may be risky if the parachute fails to deploy correctly or if the interdiction occurs at low altitude. Interdiction elements must be incredibly precise to hit a moving drone, and could be dangerous to bystanders if they miss. Long-range effectors such as lasers and high-powered microwaves could pose a serious threat to aircraft operating above a targeted drone. Jamming systems, meanwhile, can interfere with legitimate communications links in their vicinity; if used at an airport, for example, they could interrupt air traffic management operations.\(^{16}\) The use of GPS jamming or spoofing systems, in particular, is especially dangerous in areas where other entities rely on reliable GPS navigation (for example, manned aircraft at an airport).

**Interdiction Effectiveness**

Like detection systems, no interdiction system is 100 percent effective. Following a five-day counter-drone exercise in 2017 in which a variety of established defence firms and startups tested their counter-drone products on drones operating at a distance of roughly 200 metres, the Joint Improvised-Threat Defeat Organization, which organized the event, reported that the drones

---

15 Some systems may be able to identify the drone’s registration number, which could aid in this estimation, but such systems still wouldn’t be able to prove beyond reasonable doubt that a drone is being operated with malicious intent at that very moment. Imagine, for instance, that a malicious actor uses a stolen drone to conduct an attack.

16 Advanced jamming systems that only block the frequency on which the targeted drone is operating, as well as directed jamming antennas, may reduce interference with legitimate communications, but this technology is only beginning to emerge on the market, and it has not yet been certified as entirely safe. See O’Donnell, Michael J. (2016) *Letter from Michael J. O’Donnell, A.A.E., Director of Airport Safety and Standards, U.S. Federal Aviation Administration*, October 26. Available at: [connect.ncdot.gov/resources/Aviation%20Resources%20Documents/faa-uas-detection-testing-letter.pdf](connect.ncdot.gov/resources/Aviation%20Resources%20Documents/faa-uas-detection-testing-letter.pdf).
were, in general, ‘very resilient against damage’ and concluded that most of the C-UAS systems needed further development.\textsuperscript{17} More recent C-UAS exercises and numerous background interviews confirm that this problem remains an enduring one.

Like detection systems, all interdiction systems have specific drawbacks.

- **RF jamming systems** have no effect against drones that operate without an active RF link.

- **Many signal jammers** have a limited effective range of a few hundred metres – meaning that the system must be very close to the intruding drone to successfully mitigate it – and are not effective without a direct line-of-sight to the drone. Jammers that are capable of operating at long ranges and beyond line-of-sight must be significantly more powerful, but more powerful jammers also pose a higher risk of interference to legitimate communications.

- **All kinetic systems** may struggle against drones that are moving quickly or in unpredictable patterns. (And when they do work as intended, they may destroy components of the drone that are necessary for forensic investigations).

- **Spoofing systems**, meanwhile, are technically very difficult to build and implement, and may not be universally effective against all drones. Unmanned aircraft that have been built with protected communication links, for example, could be resistant to spoofing attacks.

**Advances in Drone Technology**

Drone technology itself is not standing still, and advances in this area will pose new challenges for counter-drone systems. As the unmanned aircraft systems market expands and the range of readily available aircraft types becomes more diverse, counter-drone systems will need to be flexible enough to detect and neutralize drones that come in a wide variety of shapes and sizes. These could span from large unmanned aircraft capable of carrying heavy payloads at very high speeds to low-flying micro surveillance drones that might only weigh a few grams.

There are also individual technological advances emerging that pose unique challenges from a counter-drone perspective. Perhaps most notably in the near-term is the active research to develop drones that can operate in GPS-denied environments,\textsuperscript{18} which would be resilient to any kind of jamming (which is currently by far the most common interdiction method on the market). For example, according to Russian state media, the Russian military is planning to deploy GLONASS-free surveillance drones to the Arctic to track vessels across wide areas.\textsuperscript{19}

Other research tracks seek to develop systems capable of actively defeating jamming or spoofing attacks. Eventually, drones could be programmed to evade the specific frequencies targeted by a jammer, or to switch frequency bands across a broad spectrum, or initiate a series of evasive


maneuvers, as soon as they detect a jamming signal. Modern GPS receivers are also increasingly being designed to minimize interference from the ground, which can make them difficult to jam with terrestrial systems. Others are being developed with features to detect incoming spoofing attacks.

In a similar vein, consumer drones may soon be controllable via mobile LTE networks rather than through an RF link. An LTE drone could be operated at what one paper describes as an ‘essentially unlimited operation range’, making the pilot harder to find. Furthermore, LTE drones would be difficult or dangerous to interdict with jamming systems without interfering with ubiquitous cellular communications.

Not all of these advances are motivated by a desire to make drones harder to counter. Somewhat ironically, many of these advances are driven by efforts to make drones safer. Certain commercially available drones today already come with frequency-hopping systems as standard, a feature intended to create a more resilient link to the operator that could nevertheless make the aircraft more robust against jamming. Researchers at the University of Zürich are developing a multirotor drone that can autonomously dodge fast-moving objects at close range. The idea is to enable unmanned aircraft to avoid obstacles such as birds or other aircraft, but the same feature could also enable the drone to avoid nets and other projectiles.

The proliferation of C-UAS technology will also accelerate the development of technologies that will render C-UAS systems less effective – countermeasures to the countermeasures – particularly in military environments. For example, drones might be programmed to operate in patterns that make them difficult to detect with automated target detection algorithms. Rotors might be modified to dampen a drone’s engine noise so that it can evade acoustic detection. Military drones could begin carrying devices to detect incoming spoofing attacks. Drones might be designed in such a way as to reduce their radar signature (some have speculated that ISIS drones are often wrapped in tape for precisely this reason). Groups might programme an explosives-laden drone’s ‘home’ location as its intended target, so that if the drone is jammed and initiates a ‘return to home’ mode (a standard feature on many commercial drones), it will fly straight to the very place that the C-UAS operators are trying to protect.

Finally, the advent of drone swarms (or simple agglomerations of multiple drones) would present a range of particularly vexing technical challenges from a defensive perspective. A swarm of drones would outmatch any interdiction system with a smaller number of ‘shots’ than the number of aircraft in the swarm – consider, for example, a swarm of ten drones against a net-cannon that only holds five nets. A swarm would also defeat any counter-drone system with a smaller effective detection or interdiction area than the spread of the swarm itself; directional

---


21 Information provided by Red Six Solutions, a U.S. red teaming firm specializing in drones and counter-drone dynamics.

22 LTE stands for Long Term Evolution, a ‘4G wireless communications standard developed by the 3rd Generation Partnership Project (3GPP) that is designed to provide up to 10x the speeds of 3G networks for mobile devices such as smartphones, tablets, netbooks, notebooks and wireless hotspots’. See: www.webopedia.com/TERM/4/4G_LTE.html.


26 In 2018, a committee of subject matter experts convened by the National Academies of Sciences, Engineering, and Medicine concluded that the technologies necessary to deploy collaborative swarms of up to hundreds of drones will be widely available by 2025. ‘Counter-Unmanned Aircraft System (C-UAS) Capability for Battalion-and-Below Operations’, Board on Army Science and Technology Division on Engineering and Physical Sciences, National Academies of Sciences, Engineering, and Medicine, 2018. (Abbreviated Version of a Restricted Report.).
jammers, for example, only project a narrow beam of radio frequency, and as such they would be ineffective against a group of drones spread across an area that is wider than that beam. Certain detection and tracking products may even be unable to track more than a handful of drones simultaneously. A ‘swarm’ doesn’t have to be dynamic or truly autonomous to achieve these effects; ten individual drone operators flying ten drones in unison may be just as difficult to defend against as a true autonomous swarm of ten aircraft. While a number of firms are developing counter-drone products capable of mitigating multiple incoming aircraft, this remains a developmental capability.

Lack of Operational Data

There is a distinct lack of information regarding the operational track record of deployed systems. Not a single C-UAS manufacturer approached in the preparation of this report would provide details about their product’s performance in real-world use. This information vacuum makes it difficult for would-be C-UAS owners to know what actually works and what doesn’t, anticipate potential issues, and select a system that is best suited to their needs.

Cost

Counter-drone technology is expensive. Though most manufacturers do not disclose their price lists, the relatively sparse pricing information available suggests that the technology falls beyond the reach of many small organizations wishing to protect their airspace. According to a 2019 study by Sandia National Laboratories, out of 123 C-UAS products for which pricing information was available, 77 cost more than $100,000. Just two weeks after the Gatwick drone incident, the airport announced that it had already spent more than $6 million installing counter-drone systems to prevent future incidents. According to a study by Deutsche Flugsicherung, equipping Germany’s 16 busiest airports with drone detection systems would cost upwards of half a billion euros. Personnel training, maintenance, and staff time to operate the counter-drone system all incur significant additional costs.

Legality

There is significant ambiguity as to the exact legal dimensions of counter-drone technology use. This is because, in the absence of tailored legislation, the technology is often subject to numerous overlapping laws that were drafted long before counter-drone technology existed. Norway is no exception. As discussed in ‘Civilian Scenarios’, the ability of Norwegian law enforcement to employ C-UAS measures is restricted by existing legal frameworks, except in some exceptional circumstances as per the principle of necessity (nedrett). Even certain detection techniques may run afoul of Norway’s Criminal Procedure Act, which imposes restrictions on when and where police are allowed to intercept electronic communications, including a warrant requirement for

---

28 See for example, the U.S. Air Force THOR programme, the U.S. Army’s Indirect Fires Protection Capability system, and Raytheon’s High-Power Microwave and laser systems.
most types of communication taps. The national legislation layer should then be complemented with international legal frameworks and regulations. In the case of Norway, as will be explored below, the EU framework is highly relevant. The EU-funded ALADDIN project published a preliminary study on the different data protection, social, ethical and legal frameworks in Europe that have legal implications for the C-UAS problematique.

As opposed to Norway, both Finland and Denmark have legal frameworks that allow law enforcement to use jamming devices. In Denmark, law enforcement may apply for temporary permits allowing them to utilize jamming equipment, on the basis of a 2016 report where an expert group recommended it as a preventative measure for illegal use of mobile devices in prisons. In Finland, authorities have made amendments to the legal framework allowing police to intercept drones by force, including disturbing the connection between the drone and its operator. The amendments to Finnish law entered into force on 18 March 2019.

Lack of Standards

No international standards exist for the proper design and use of C-UAS systems. This means there may be significant variances between the performance and reliability of systems that might, at the spec-sheet level, appear to be very similar. Given that the demand for this technology has only emerged in the past few years, many of the products offered by the companies that we identified have not yet had time to mature – more than 200 products have likely been brought to market in the last 18 months alone. In more extreme cases, some firms appear to be working to capitalize on the growing interest in this technology before properly maturing or field-testing their products. U.S. and European security officials who spoke on background have noted that a large proportion of systems that are actively marketed to government customers do not perform as advertised. The absence of standards also raises questions about safety. Particularly in civilian environments, a malfunctioning C-UAS system might present a public safety threat – consider, for example, a jamming system that interferes with emergency radio communications, or a kinetic system that misses its intended target.

Privacy

Because counter-drone detection systems are a form of surveillance technology, they potentially pose a risk to privacy if misused or if the data they collect is not handled properly. For example, electronic identification systems could be capable of obtaining personally identifiable information – such as the aircraft’s registration number – for drones operating across a broad area. Similarly, wide-area camera systems could inadvertently record individuals or vehicles on the ground that are not relevant to the counter-drone operations themselves. This is in addition to private digital
information that could be collected from a drone either at the point of detection and tracking or during forensic analysis. So far, there have been relatively few efforts to evaluate how to mitigate privacy risks that could arise from the use of these systems.\textsuperscript{38}

### 3.3. Concluding note

The challenges detailed in this section are complex and formidable. They are best addressed through rigorous testing and standards-writing, multi-stakeholder collaborations – including, crucially, input from academia and civil society – and rigorous technological forecasting to anticipate novel threats (rather than playing a perpetual game of catch-up).

\textsuperscript{38} One notable exception is the EU-funded project ‘Advanced hoListic Adverse Drone Detection, Identification & Neutralization’ (ALADDIN), which develops a counter-drone detection and neutralization system.
4. Civilian Scenarios

The proliferation of cheap, commercial drones was recognized as a security threat for Norwegian civilian and military facilities by the Norwegian National Security Authority (NSM) in a 2017 risk assessment report. Since then, public institutions and private companies have taken steps to implement regulatory, preventive and protective measures against the threat posed by drones in Norwegian civilian contexts.

In early 2018, several Norwegian ministries co-published the Norwegian Drone Strategy – a strategic document to facilitate the development and usage of drones by private and public sector organizations. In 2017, the Bomb Squad, part of the Oslo Police Department, was given responsibility for the police’s C-UAS efforts and technical expertise, and is the national contact point for other partner entities within the C-UAS field. The Bomb Squad delivered a report mapping the risk landscape and recommended counter-drone measures to the National Police Directorate (POD) in December 2018. At the time of writing, the POD has not established a strategy for countering drone threats in Norway nor a C-UAS unit, and the police does not have an autonomous operative counter-drone capacity. At the same time, other actors responsible for critical infrastructure in Norway (e.g. Avinor and Equinor) have taken steps to incorporate the threat posed by drones into their strategic, safety and security considerations.

None of the actors spoken with for the purpose of this report have conducted structured societal impact assessments on potential implementation of C-UAS technology.

4.1. Legal frameworks

The application of many C-UAS measures is illegal under current Norwegian law. In Norway, these legal restrictions severely limit who, when, and under what conditions C-UAS technology may be applied. The Civil Aviation Authority (CAA) is the actor generally responsible for establishing restricted zones where the usage of drones is forbidden or limited. The police may also institute interim restriction zones under the terms of The Police Act (Lov om politiet – Politiloven) §7, which outlines exemptions that may be granted as necessary to meet security, tactical or investigative needs.

Intercepting drones is defined as a use of force, and may only be carried out by the police. Jamming is the default strategy currently being pursued by the relevant agencies; however, the police does not have the legal basis to interfere with or stop electronic communication. Further, the use of sensor detection systems may grant access to personal data, thereby infringing privacy laws. In practice, this means that the police may only use counter-drone measures such as jamming when justified within the principle of necessity (nødrett) – that is, to respond to a threat to life or national security. Operating within this legal realm puts severe restrictions on the conditions under which C-UAS may be utilized for training purposes or active missions.

The POD has submitted proposed changes to The Police Act and the Electronic Communication Act (Lov om elektronisk kommunikasjon - Ekomloven) to the Ministry of Justice specifically regarding the usage of C-UAS technologies. In a formal response to opposition politician Emilie Enger Mehl

---

(The Centre Party – *Senterpartiet*) in September 2019, then Minister of Justice Jørn Kallmyr stated that the Ministry of Justice was considering clarifying the legal frameworks to counter drone threats. As of January 2020, no amendments encompassing C-UAS technology have been made to The Police Act or The Act on Electronic Communication.

To illustrate which forms drone threats may take in a Norwegian civilian context, three hypothetical scenarios are outlined below. These scenarios describe the context of the threats, the actors who will be involved in capacity building and in the response, and existing hurdles to threat mitigation.

![Photo: Bruno Oliveira Martins](image)

### 4.2. Scenario 1: Drone(s) in proximity of a large crowd in an urban area

**Context and threat scenario**

Large gatherings of people have been the targets of terror attacks in Europe before. By operating an armed drone in a civilian crowd, a potential attacker may cause severe harm and panic amongst civilians. Importantly, the drone does not have to be armed to pose a security risk. The sight of a low-flying unarmed drone in proximity of a crowd may still cause panic and trampling. The Oslo police has already begun planning for such incidents, with assistance from the Armed

---

Forces. In 2019, the agencies ran drills on a scenario where the 17 May children’s parade in Oslo is targeted.42

**Actors**

The emergency response is complicated by the fact that the employment of any form of C-UAS system may affect numerous collateral actors. The Police has to issue Notice to Airmen (NOTAM) warnings via Avinor to pilots in proximity of the operation informing them that the C-UAS technology may disturb their GPS signals. The National Communication Authority (NKOM) will have to be informed for them to ensure that the usage of counter-drone equipment will not cause major safety hazards for other lines of communication, such as railways. At present, the police also have to enlist assistance from the Armed Forces according to Bistandsinstruksen, a framework that outlines the ways in which departments of the military may support police operations.

**Current situation and persisting challenges**

In March 2019, the Oslo Police and the Armed Forces ran drills both at Mastemyr and in front of the Royal Palace in preparation for the 17 May parade, and were operative during the actual celebrations a few weeks later. The drills included experts on explosives for potential situations where drones are armed. These drills exemplify how the police do not have the capacity to handle C-UAS without the support of the Armed Forces. While Bistandsinstruksen allows for police-military cooperation, there are two factors which make the present state of this practice unsustainable in the long run. First, the Armed Forces have not scaled up their C-UAS resources to also cover police operations. Second, police-military cooperation under Bistandsinstruksen becomes highly expensive for the police, as the police are responsible for paying the salaries of the army operators that contribute to the joint efforts.

4.3. Scenario 2: Nuisance or nefarious drone usage at airport

**Context and threat scenario**

Drone usage close to an airport does not need to be intentionally harmful to be dangerous. Any mid-air collision with an object could be dangerous to an aircraft, and a study commissioned by the British Department for Transport, the Military Aviation Authority and the British Airline Pilot’s Association has found that drones above a certain size could be more dangerous to aircraft than birds.43 Even if the aircraft is able to withstand the collision impact, ‘drone-strikes’ may affect the pilot’s ability to navigate, creating potentially dangerous situations. Therefore, just spotting a drone in proximity of an airport risks disturbing traffic or closing it down completely, as has occurred at several international and Norwegian airports. In 2019, Avinor reported 40 incidents of illegal drone usage near an airport,44 and air traffic had to be closed at Bodø airport twice in the

---


Practitioners interviewed for this report indicate that the actual number of incidents may be significantly higher.

**Actors**

The CAA establishes restriction zones and is the main communicator of drone regulations, while Avinor is responsible for the management of most civil airports in Norway. Avinor has worked specifically with drones since 2016 and expanded its work to include C-UAS after the drone incident at Gatwick in December 2018. Avinor is active in the European branch of Airports Council International (ACI) and is represented at the ACI security committee, a strategic working group with seven other major airport operators. Drone threats are amongst the topics the committee discusses and exchanges best practices on, despite European airports currently heading in very different directions regarding C-UAS measures.

Additionally, the CAA leads – and Avinor is represented at – the Norwegian Security Council for Aviation (Sikkerhetsrådet for Luftfarten - SFL), which includes representatives from the Ministry of Defence, the Ministry of Justice, the Ministry of Transport and Communication, the Ministry of Foreign Affairs, the National Security Authority, the Norwegian Police, the Norwegian Police Security Services (PST), and representatives from larger air carrier companies. The Council has neither decision-making authority nor operational functions but may contribute to influencing regulations through proposals for amendments. Avinor also receives reports from the Police Secret Service and military intelligence on threat assessments, which include the potential threat posed by drones. Any interception of drones would have to be carried out by the police.

**Current situation and persisting challenges**

According to The Aviation Act (Lov om luftfart – luftfartsloven), Avinor has legal basis to conduct drone detection at its airports, but is not obliged to do so. Interception of drones lies solely in the hands of law enforcement. The CAA has established no-fly-zones for drones in a 5-kilometre radius of any airport in Norway. With the implementation of the EU framework on civil drones by July 2020, there will be a more cohesive framework of regulation of European airspace.

Avinor has installed a test installation at Sola airport in Stavanger. The Ctr+Sky 3D radars from the Polish operator Advanced Protection Systems are meant to detect both drones and birds.\footnote{‘Case study, Airport, Sola, Norway’, Advanced Protection Systems. Available at: apsystems.tech/en/case-studies/airport/} When drones enter a no-fly-zone, they appear on a screen, and personnel at the airport are supposedly able to track the person operating the drone. Amongst the lessons learned are that one radar system alone is insufficient for covering the whole airport, given the technology’s limited detection range, and that present systems are not always accurate enough to positively identify drone sightings.

During conversations with developers and end-users of C-UAS technology, several actors referred to the possibility of delegating C-UAS usage from law enforcement to airport operators. That is, for the airport to establish a direct line of communication with the police in which the police could give approval to ‘push the button’ activating jamming of drones, allowing airport staff to do so under the guidance of law enforcement. In order to be efficient, such a framework would have
to be capable of a very rapid turnaround, given the short window of time to respond to an incoming drone threat. This is not a viable possibility within the current Norwegian legal framework.

The use of C-UAS technology could be damaging to an airport’s communications and air navigation systems. For instance, jamming risks harming the airport Instrument Landing System (ILS). The C-UAS would therefore have to operate only on certain bandwidth frequencies. Another potential solution would be to rely on measures that would not interfere with lines of communication, such as catch-and-carry drones. However, as discussed in the previous chapter, such solutions might bring problems of their own – including complicating air traffic management – and would not be effective against large groups of drones.

4.4. Scenario 3: Armed drone attack on a Norwegian oil platform

Context and threat scenario

Critical infrastructure has proven vulnerable to armed drone attacks. The drone attacks on the Saudi Arabian oil processing facilities Abquaiq and Khurais on 14 September 2019 showed that these well-secured facilities, like most such facilities around the globe, are vulnerable to drone attacks.47 Given Norway’s role as a provider of energy, Norwegian oil and gas facilities make for potential targets for actors that want to harm not only Norway, but also Europe as a whole. Following the attack on the Saudi facilities, the extent to which Norwegian facilities are adequately protected has been debated in the media, and Equinor has admitted that their facilities both on land and offshore are vulnerable to targeted terror attacks.48 Further, such facilities are typically remotely located, making response time a potential challenge for law enforcement.

Actors

As opposed to what happens with drone flying management, the CAA does not have a role in approval and management of C-UAS. However, some actors operating critical infrastructure facilities still reach out for counsel and advice on how to protect against unwanted drone activity. The only remedy the CAA may offer is to establish restriction zones in airspace, which requires both sound knowledge of the legal framework on the part of drone operators and a willingness to follow the rules in order to be an efficient counter-measure.

On Norwegian soil, the general responsibility for counter-drone efforts and risk evaluation lies with the police, the Armed Forces and the Norwegian National Security Authority (NSM), but offshore installations are subject to a different legal framework, which further complicates the issue. For offshore installations and petroleum facilities, the responsibility for risk management is with the operators. As established by the Framework regulation for health, environment and security in petroleum activities (Forskrift om helse, miljø og sikkerhet i petroleumsvirksomheten og på enkelte landanlegg – rammeforskriften) §57–59, the operators have a duty to establish and implement security zones around their facilities. The security zones should be of 500 metres, both horizontally and vertically. Within their responsibilities lies surveillance of these zones, and action – which may include physical measures – if the infringement of the security zone leads to serious

47 It should be underlined, though, that this was a large-scale attack that cannot be replicated easily. The missiles allegedly used in this attack cannot be easily operated by a wide range of actors.
danger to the security of the operation. But these facilities would not, in theory, have the legal authority to intercept drones, since this authority is currently only held by the police. This example illustrates how legal frameworks lag behind technological developments, creating a paradox in which the facility operators are on the one hand responsible for managing security risks, while on the other they are forbidden from applying the necessary measures by a contradictory legal framework.

Current situation and persisting challenges

The attack on Saudi oil processing facilities triggered a public debate on how well protected Norwegian critical infrastructure is, and who is responsible for protecting different facilities. The case also highlights the role of industries and enterprises in countering security threats. While collaboration with business and industry was part of the report Support and Cooperation: A description of total defence in Norway published by the Ministry of Defence and the Ministry of Justice in 2018, the collaboration described is largely limited to industries and businesses as suppliers. Yet, the role of industries and businesses may be far more multifaceted, namely as providers of UAS and C-UAS technology, and as owners and managers of critical infrastructure. The NSM 2019 risk assessment report underlines how enhanced cooperation between military and the civil sector will shape the security response in the years to come, including facing hybrid threats. Close private-public cooperation, security assessments and risk-reduction strategies within this landscape will be critical for safety and security management.

4.5. Concluding note

The three hypothetical scenarios in this section illustrate the complexities civil authorities will have to grapple with when countering drones. There are high demands on efficient civil-military coordination and cooperation, in challenging and complex situations with severely limited response time. Legal restrictions and dependence on assistance from the Armed Forces gravely limit law enforcement’s capacity to respond to drone threats.
5. Military Scenarios

In recent years, the use of drones for military purposes has grown exponentially. Not only a great number of countries acquired some kind of armed drone capacity, but also a vast number of non-state actors have used drones with different levels of sophistication in conflict scenarios. In other words, it has become clear that drones are spreading rapidly and will figure in every conflict in the future. This could be in the form of large armed drones capable of employing a range of precision-guided missiles and bombs, or cheap commercial drones that carry communication systems and sensor suites that furnish even small state and non-state actors with airborne Intelligence, Surveillance and Reconnaissance (ISR) and Command and Control (C2) capabilities that would have been impossible to achieve by traditional means, not to mention the explosives-laden hobby drones deployed by groups like ISIS as rudimentary (but effective) miniature guided missiles. As such, the development of systems to counter the threat posed by these tools has emerged as one of the most pressing – and challenging – priorities for countries around the world, including Norway and its European and North American allies.

The following hypothetical scenarios illustrate two potential drone threats in a military context, describing the related challenges they present.

5.1. Scenario 1: Critical military infrastructure

One potential drone threat confronting Norway would be an attack on a military base in Norwegian territory. Military bases belonging to the Norwegian Armed Forces are spread all across the country. Moreover, a number of sensitive international military facilities are also located on Norwegian soil. These include the NATO Joint Warfare Centre (JWC) in Stavanger. The JWC is subordinate to Headquarters Supreme Allied Commander Transformation (HQ SACT) in Norfolk, Virginia, U.S., and is the premier training establishment of the NATO Alliance at the operational-level. The JWC achieved its Full Operational Capability in 2006 and conducts regular large-scale exercises. Facilities like the NATO JWC are considered critical military infrastructures and could be vulnerable to intrusions by small commercial unmanned aircraft that could collect detailed intelligence or, if weaponized, pose a kinetic threat to Norwegian and partner military assets. Meanwhile, in the conflict in Ukraine, Russia has demonstrated a sophisticated drone capability to support significant and effective kinetic actions, including fire correction, ISR, electronic warfare, and Psychological Operations. Given growing tensions between Russia and Norway and its allies, these Russian capabilities represent a significant tactical dimension to any hypothetical conflict.

5.2. Scenario 2: Protection of Norwegian and allied forces abroad

By the same token, Norway’s current peacekeeping forces will soon have to contend with the threat of small drones, as non-cooperative states and non-state actors alike discover that small drones can be an effective and inexpensive tool for disrupting the air and ground operations of even the most well-equipped military forces. There has already been use of armed drones by non-state groups in some of the regions where Norwegian troops are currently deployed, such as Mali and Iraq. As the technology proliferates, it is nearly certain that Norwegian forces deployed in areas such as South Sudan and Afghanistan will be confronted with drone threats in the coming years.
5.3. Strategic considerations

The legal restrictions that apply to the use of C-UAS technologies in civilian environments do not apply to overseas military operations. Therefore, there is generally far greater legal latitude for C-UAS usage in military contexts than in civilian settings. However, many of the operational problems carry over from the civilian environment. For example, radio frequency jamming systems have no effect against drones that operate without an active radio frequency link, and, as explained above, many signal jammers have a limited effective range of a few hundred metres – meaning that the system must be very close to the intruding drone to successfully mitigate it – and are generally not effective without a direct line-of-sight to the drone. In military settings, and in scenarios of active conflict, this is often not possible. Moreover, all kinetic systems may struggle against drones that are moving quickly or in unpredictable patterns. Additionally, spoofing systems may not be universally effective against all drones. For these reasons, countering nefarious drones remains a big challenge, even in military contexts.

Finally, the fact that Norwegian deployments abroad take place in multilateral and multinational frameworks means that additional challenges of system interoperability apply. C-UAS technology is not sufficiently developed nor harmonized, and therefore different countries use different systems that do not always work in compatible ways. As will be shown in the section ‘The NATO Dimension: Key Developments’, the Alliance has identified interoperability and standardization as a priority to ensure efficiency of C-UAS operations in military contexts.

5.4. Concluding note

The technology that enables drones to fly and to become weaponized has developed and proliferated faster than the technology to counter them. For this reason, countering the drone threat remains a formidable challenge in military contexts. Due to the kinetic potential of improvised weaponized drones and the difficulty of countering them, security experts and military operatives often refer to drones as the new Improvised Explosive Devices (IEDs). Despite significant progress in C-UAS technology, the continuing democratization of access to drone technology means that Norwegian soldiers deployed abroad will be increasingly exposed to this threat, and the Ministry of Defence may look to participation in international frameworks as a means to broaden its capability to counter it. The next sections point to avenues by which Norway may leverage its participation in, and financial contributions to, international programmes and frameworks in order to further address the C-UAS problem-set.
6. The European Union Context: Key Developments

Any discussion surrounding constraints and opportunities for Norwegian action in mitigating the drone threat needs to consider the European Union (EU) factor. Despite not being a member of the EU, Norway is impacted by EU regulations in a wide range of areas. Through its membership in the European Economic Area (EEA), it participates in several EU frameworks and initiatives. In these areas, developments taking place at the EU level have the potential of both influencing Norwegian policies and creating a number of new opportunities. For the purpose of this report, three areas deserve special attention and are specifically addressed in this section: the Single European Sky (SES), which Norway is a part of; the EU’s research programmes on security and defence; and the EU’s Common Security and Defence Policy, to which Norway contributes.

6.1. Regulating the European and the Norwegian airspaces

Norway is very much integrated in EU initiatives designed to reduce the fragmentation of the European airspace and to harmonize national legislations. First and foremost, Norway is part of the Single European Sky, an initiative that aims to increase the efficiency of air traffic management (ATM) and air navigation services by reducing the fragmentation of European airspace.\(^{51}\) Norway is also a member of the European Aviation Safety Agency (EASA), whose mission, under the authority of the European Commission (DG MOVE), is to ‘promote the highest common standards of safety and environmental protection in civil aviation’,\(^{52}\) developing ‘common safety and environmental rules at the European level’\(^{53}\) and monitoring the ‘implementation of standards through inspections in the member states’, providing ‘the necessary technical expertise, training and research’.\(^{54}\) The main tasks of the Agency include, among others, Rulemaking (drafting aviation safety legislation and providing technical advice to the European Commission and to the member states); Inspections, training and standardization programmes to ensure uniform implementation of European aviation safety legislation in all member states; and Safety and environmental type-certification of aircraft, engines and parts.

The membership of these different frameworks implies that the regulation of the Norwegian airspace happens in close harmonization with the different EU initiatives. For this reason, the Norwegian drone regulation, referred to in the previous section, is now in reform process in order to accommodate the July 2019 entry into force of the new EU policy framework for civilian drones. As explained by Chantal Lavallée in a PRIO Policy Brief published shortly after, the European policy for drones is based on the new Basic Regulation, which entered into force in September 2018, and two more specific regulations that entered into force in July 2019 and which provide the member states with detailed technical and operational rules. Lavallée contends that these changes constitute a paradigm shift for European airspace and represent the beginning of a longer implementation period across European countries – including Norway – which should lead to the creation of an ‘EU drone ecosystem’.\(^{55}\) The next step to consolidate this ecosystem is the U-Space

---

53 Ibidem.
54 Ibidem.
initiative, which should provide a platform for the Unmanned Traffic Management (UTM) for all drone operations in all types of airspace. The EASA is working on a draft regulation to be submitted to the Commission in the first quarter of 2020. Such a platform is crucial for C-UAS and for preventing incidents, especially in urban environments involving clueless drones.

It is in this context of increasing pan-European harmonization that the efforts to mitigate drone threats are taking place. As mentioned in the conclusions of the European Commission-organized October 2019 High-Level International Conference and subsequent EU-internal meeting on countering the threats posed by unmanned aircraft systems (UAS), the new EU drone policy framework has a security dimension. The different regulations require drone operators whose operations may present a ‘risk to safety, security, privacy, and protection of personal data or environment to register with national authorities’, which in turn ‘are given the authority to restrict drone use in specific geographical zones’. The European Commission understands that the task of effectively protecting European societies from nefarious use of drones requires a holistic approach involving a wide range of stakeholders in different sectors, and therefore several Directorate-Generals (DGs) such as Migration and Home Affairs (DG HOME), Mobility and Transport (DG MOVE), European Civil Protection And Humanitarian Aid Operations (DG ECHO), Defence Industry and Space (DG DEFIS), as well as the Joint Research Centre (JRC), are involved in raising awareness and moving the policy agenda forward.

6.2. The EU’s framework programmes for security and defence R&D

Since the 1980s, the EU has implemented multiannual framework programmes to foster research and innovation in the EU and associated countries, including Norway. Its current version, Horizon 2020, is the biggest EU Research and Innovation programme so far, with nearly €80 billion of funding available over 7 years (2014 to 2020). In the words of the European Commission, these programmes aim to drive economic growth and create jobs, putting emphasis on ‘excellent science, industrial leadership and tackling societal challenges’, ensuring that ‘Europe produces world-class science, removes barriers to innovation and makes it easier for the public and private sectors to work together in delivering innovation’. In the case of Horizon 2020 alone, Norwegian organizations have signed 1,448 grants with a net EU contribution of €1.08 billion.

Over the last 15 years, more than €500 million have been invested by the EU in projects that develop drone technology, and through this scheme the EU has been a key contributor to the advancement of drone technology in the continent. As explained in an article by Bruno Oliveira Martins and Christian Küsters, EU spending on drones grew sharply following Framework Programme 7 (FP7, 2007–2013), which inaugurated the EU’s Security Research Programme (SRP). FP7’s SRP had a total budget of €1,400 million and had the expectation of both generating new knowledge and promoting the application of new technologies while reinforcing the competitiveness of the European security industry. The EU understood improved security, advanced technology, and industrial development as being fully integrated. In the following
framework programme, Horizon 2020, the SRP thematic area is called Secure Societies and has the same objectives.

In a logic similar to the funding of the drone technology development, the EU has recently started to fund projects and initiatives that advance research on C-UAS technology. These initiatives include the above-mentioned ALADDIN project, which, in a series of complementary pilots, designs, develops, and evaluates ‘a counter UAV system as a complete solution to the growing UAV threat problem, building upon a state-of-the-art system and enhancing it by researching on various technologies and functionalities’. With a budget of nearly €5 million, the project develops solutions for detection, location and mitigation (jammers, physical and hacking). Another Horizon 2020 project worth mentioning is KNOX (Cost advantageous and scalable drone alarm and protection system for urban contexts). KNOX is an innovation project led by the Danish SME MyDefence that has developed an ‘innovative drone alarm able to detect, identify and locate civilian drones around secure areas, and to jam in a specific wireless frequency range without interfering with other mobile signals and forcing a controlled drone landing’. Besides these two projects, Horizon 2020 has also provided funded to other C-UAS-related projects, such as ALFA, SAFESHORE, DEFENDER, and SafeSky.

These projects illustrate that the EU’s engagement with C-UAS technology is happening not only at the regulatory and political level, but also through innovation and research and development (R&D) programmes. These projects are part of the above-mentioned SRP, and, as the EU moves towards a defence research programme, the investment on C-UAS R&D will likely increase.

From security R&D to defence R&D

Indeed, over the last two years, the EU has considerably expanded its commitment on defence R&D. In May 2017, the EU launched a Preparatory Action on Defence Research to fund defence-related research and technology development directly from EU funds, and not simply through member states’ joint initiatives. This scheme was framed as a concrete step aimed at assessing and demonstrating the added-value of EU-supported defence research, and it is a preparatory stage towards the establishment of a substantial European Defence Fund (EDF), which was approved in principle during the Spring of 2019. The EDF will award several billion euros in contracts between 2021 and 2027. Importantly, the ambiguous implications of Brexit notwithstanding, Norway will be the only non-EU member state to have access to the EDF. This means that the funding opportunities provided by the EDF will be accessible to Norway, and both Norwegian companies and governmental agencies could explore the different opportunities available to them. In a call for proposals issued in April 2019 in the framework of the European Defence Industrial Development Programme, for example, €80 million were made available to help develop chemical, biological, radiological and nuclear (CBRN) threat detection capabilities or

63 ALADDIN, grant agreement ID: 740859. Available at: cordis.europa.eu/project/id/740859.
64 KNOX, grant agreement ID: 768242. Available at: cordis.europa.eu/project/id/768242.
65 Ibidem.
66 Advanced Low Flying Aircrafts Detection and Tracking (ALFA), grant agreement ID: 700002. Available at: cordis.europa.eu/project/id/700002.
67 System for detection of Threat Agents in Maritime Border Environment (SAFESHORE), grant agreement ID: 700643. Available at: cordis.europa.eu/project/id/700643.
68 Defending the European Energy Infrastructures (DEFENDER), grant agreement ID: 740898. Available at: cordis.europa.eu/project/id/740898.
69 Integrated system for critical infrastructure and personal sphere monitoring and protection against aerial threats (SafeSky), grant agreement ID: 673627. Available at: cordis.europa.eu/project/id/673627.
counter drone systems,\textsuperscript{70} and through 2020 another call will be issued for C-UAS projects with an estimated budget of €13.5 million.\textsuperscript{71}

Finally, it should also be mentioned that besides Horizon 2020 and the EDF-related initiatives, the EU has used the Internal Security Fund – Police funding for C-UAS efforts, for example in the case of the project Skyfall\textsuperscript{72} involving Belgian and Romanian authorities.

\textbf{6.3. The EU’s Common Security and Defence Policy and the Permanent Structured Cooperation scheme}

Since the declaration of operationability of the EU’s Common Security and Defence Policy (CSDP) in 2003, Norway has been participating in several of its activities. Norway has contributed to three military and nine civilian missions under the EU flag and has expressed interest in participating in other initiatives, including the above mentioned EDF and the Permanent Structured Cooperation (PESCO) scheme.

The PESCO scheme allows a group of EU member states or associated countries to work closely on a defence-related project. Some of the more than forty projects approved so far relate to drone technology, and in November 2019 the PESCO project ‘Counter-Unmanned Aerial System (C-UAS)’ was approved. Led by Italy and with the participation of the Czech Republic, the project aims to ‘develop an advanced and efficient system of systems with C2 dedicated architecture, modular, integrated and interoperable with C2 info-structure, able to counter the threat posed by mini and micro Unmanned Aerial Systems’.\textsuperscript{73} According to the description of the project, the system will be ‘swift to deploy and reach operational status, to ensure protection to our troops in operational theatres, as well as employed for homeland defence, security and dual use tasks’,\textsuperscript{74} willing to ‘fulfil applicable certification and regulatory requirements, to allow homeland employment’.\textsuperscript{75} If defined as a priority for the Norwegian Ministry of Defence, Norway may participate in similar initiatives, benefit from co-funding opportunities, and influence the technology design.

Finally, it is worth pointing out that Norway has an agreement with the European Defence Agency (EDA). The EDA has drones as an important focus of attention, since the technology was designated one of four capability development priorities by the December 2013 European Council.\textsuperscript{76}

\textbf{6.4. Concluding note}

In the conclusions of the above-mentioned European Commission-organized October 2019 \textit{High-Level International Conference}, the European Commission identified six areas requiring further engagement and increased investment (see Table 4). While these priorities are appropriately

\begin{itemize}
\item \textsuperscript{72} Project Skyfall. Available at: www.projectskyfall.org/.
\item \textsuperscript{73} ‘Counter-Unmanned Aerial System (C-UAS)’, PESCO projects. Available at: pesco.europa.eu/project/counter-unmanned-aerial-system-c-uas/.
\item \textsuperscript{74} Ibidem.
\item \textsuperscript{75} Ibidem.
\item \textsuperscript{76} European Defence Agency, ‘What We Do’. Available at: www.eda.europa.eu/what-we-do/activities/activities-search/remotely-piloted-aircraft-systems---rpas.
ambitious, they are highly abstracted and do not cover the multiplicity of avenues through which the EU is investing both funds and political capital in countering the threat posed by drones.

Developing advanced knowledge on Norway's participation in the various different EU security and defence R&D initiatives explored in this chapter, such as the EDF, PESCO, the SRP, and other initiatives under the EDA, is highly relevant, given that some of these programmes may provide significant opportunities for Norway to enhance its C-UAS capabilities, if participation in these is held to the legal, ethical and societal considerations described in this report.

Table 4: Issue areas identified by the European Commission as requiring further EU engagement

<table>
<thead>
<tr>
<th>Issue areas identified as requiring further EU engagement</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Conduct regular risk assessments.</td>
</tr>
<tr>
<td>2 Empower competent authorities to exclude non-cooperative drones from restricted airspace.</td>
</tr>
<tr>
<td>3 Facilitate the development of effective tools to counter non-cooperative drones.</td>
</tr>
<tr>
<td>4 Ensure that drones operating in the European airspace are safe, secure, operationally reliable, and difficult to use for malicious purposes.</td>
</tr>
<tr>
<td>5 Cultivate a common drone culture in Europe.</td>
</tr>
<tr>
<td>6 Exchange best practices and experiences.</td>
</tr>
</tbody>
</table>
7. The NATO Context: Key Developments

Like many other security and defence organizations, NATO has identified counter-drone technology as a significant priority. However, NATO only formally began working on C-UAS in a comprehensive manner relatively recently.

In February 2019, at a meeting of member states’ ministers of defence, NATO adopted a Practical Framework programme for cooperation on C-UAS, thus formalizing and centralizing the organization’s efforts with respect to the counter-drone problem-set. This framework defines the organizational and divisional responsibilities for the various elements of the framework. Most significantly, the framework established the NATO C-UAS Working Group, which serves as the single point of contact on all things C-UAS.

7.1. The NATO C-UAS Working Group

The group, which comprises participants from all NATO member states, has had three meetings as of this writing, with a fourth meeting scheduled for January 2020. Its initial deliverables are scheduled for mid-2021, though this provisional timeline may be extended as the need arises. The Working Group’s activities are organized around four core focus areas:

1. **Building a Counter-UAS Community.** This activity seeks to provide a structure for a network of practitioners, subject matter experts, and relevant decision-makers that share a
common focus on C-UAS technology, acquisition, planning, policy, doctrine, or standards. This community, which consists of approximately 200 members from member states, has been structured so as to overlap with the membership of other similar communities of interest – such as counter-improved explosive devices and electronic warfare – and to facilitate engagement with those communities. This community of interest will work closely with other international organizations that are similarly seeking to address C-UAS, including INTERPOL (specifically the INTERPOL Drone Expert Group), the EU Commission, and the Global Counter-Terrorism Forum (which in the autumn of 2019 published the ‘Berlin Memorandum on Good Practices for Countering Terrorist Use of Unmanned Aerial Systems’. The goal of these interactions is to coordinate similar work on C-UAS and avoid replication. Finally, this community of interest seeks to build relationships with industry and academia related to C-UAS, with a particular emphasis on smaller companies (rather than the traditional defence prime contractors).

2. **Policy Review.** The NATO C-UAS WORKING GROUP is developing a set of policies, doctrine, and standard operating procedures for the acquisition and employment of C-UAS systems. These policies will include recommended requirements to guide the acquisition of C-UAS systems by member states. The policies and standards will not be compulsory for member states; however, they are compulsory for any state that employs a C-UAS system within a NATO operation.

3. **Development of Standards.** The group will develop a set of universal technical standards for C-UAS systems. As a precursor to the drafting of these standards, the working group will work to map existing standards for related weapons technologies such as intelligence, surveillance, and reconnaissance systems, command and control systems, and electronic warfare weapons. These standards are largely geared toward enabling a high level of interoperability between C-UAS systems and other weapons in NATO missions. As of this writing, the Working Group is seeking to establish a sub-group, the NATO C-UAS Standardization Sub-Group, that will focus on this area; the sub-group will be open for participation by industry members.

4. **Research & Development & Operation efforts.** Finally, the working group is organizing a series of exercises and demos to evaluate a range of counter-drone technologies. The first of these, held in December 2018 at the Marine Corps Base Quantico in Virginia, evaluated a range of ‘low collateral’ drone interdiction systems (such as, for example, non-kinetic systems like signal jammers). This exercise tested five C-UAS technologies across four different scenarios (including a drone swarming scenario), and accumulated almost 100 interdictions. In June 2019, NATO held Flaming Sword, an exercise on special forces that included a counter-drone vignette. In November 2019, the Working Group held a C-UAS Industry Day for companies that offer C-UAS products; in total, more than 90 individuals from industry participated in the event. In 2020, the organization will hold a series of demos built around NATO-funded counter-drone technology development projects. These projects include:

- **‘Comparative analysis of low-collateral damage techniques against Low Slow Small UAS’**: This is a follow-on to the Quantico exercise focusing on evaluating next-generation interdiction techniques, including directed energy. This programme, which is led by Belgium, will yield two demonstrations.

- **‘Drone Single Local Air Picture’**: This is a UK-led effort focusing on detection element technologies.
‘Cognitive radar system to detect Low Slow Small UAS’: This is led by the NATO Communications and Information Agency (NCIA).

In addition to these activities, NCIA, which is not directly affiliated with the Working Group, is currently in the process of procuring a counter-drone system for Operation Resolute Support, the NATO mission in Afghanistan. The agency issued an initial Invitation for Bids (also sometimes known as a request for proposals) in May 2019 and expected to award a contract by the end of the year. The programme has estimated that it will achieve initial operational capability by mid-2020. In general, NATO does not acquire its own weapon systems for such operations, relying instead on the systems acquired by participating member states, but opted to make an exception in this instance as a result of an urgent operational need among forces in Afghanistan. These acquired systems will additionally be used for C-UAS training and exercise, and as a testbed for the policies and doctrine established by the C-UAS Working Group. NATO is engaged in several additional R&D initiatives for counter-drone weapons at a classified level.77

7.2. Concluding note

Given Norway’s access to these initiatives through its NATO membership, these projects represent an opportunity for Norwegian stakeholders to directly engage with a broad and diverse group of entities that are similarly working to address C-UAS challenges in their own contexts. In the context of the newness of the drone threat, knowledge-sharing alone can be a fundamental component of the development of robust C-UAS policies and standards.

---

8. Conclusions

The drone threat remains a very relevant and complex challenge for both civilian and military operatives and decision-makers. Despite significant progress in recent years, C-UAS technology remains largely ineffective in real-world scenarios. Furthermore, it is very expensive, and many of the systems cannot operate in civilian contexts due to legal restrictions. These challenges mirror some natural difficulties at the operational level, and insufficient institutional coordination between different ministries and agencies may prevent efficiency in a crisis scenario.

The potential threat posed by drones is multifaceted and multilayered; consequently, the response to this threat will also necessarily be multifaceted, and different actors operating in different environments will mobilize different resources and operate under different legal and regulatory frameworks. This means that no single C-UAS system, efficient as it may be, can counter the drone threat in all its different facets.

In line with many other countries, Norway is adapting to this new threat environment by mobilizing human and financial resources and by adapting some regulatory and legislative frameworks. These efforts often entail cooperation between these two environments, and from this perspective some of the strategies being explored to address the drone threat are an example of the erosion of a strict separation of civil and military organizations and practices. Yet this erosion also brings important ethical and societal risks that need to be taken into account.

Recent NATO and – in particular – EU frameworks provide important opportunities for bringing Norway closer to the technological edge and to international best practices. Through different schemes such as the security research programme, the defence research programme, or PESCO, the EU is investing financial and political capital in developing C-UAS technology. These opportunities are open to Norwegian participation and may serve to increase public safety and contribute to the Norwegian R&D environment.

This all being said, it is crucial that stakeholders work to ensure that the response to the drone threat always meets high standards of legal and ethical compliance. C-UAS technology has societal impacts, spanning privacy concerns, psychological stress, and elevation of threat perception. For this reason, societal impact assessments need to be a part of the decision-making process behind C-UAS technology acquisition. This applies to both private actors and public authorities.

In the years ahead, automation and Artificial Intelligence will permeate both the daily lives of smart cities and the dynamics of armed conflict, rendering all of the challenges described in this report all the more urgent and complex. Continuous monitoring of both technological developments and the social contexts from which they emerge is crucial for ensuring public safety.
9. Further Reading


U.S. Federal Aviation Administration (2019) Unmanned Aircraft System Detection - Technical Considerations, U.S. Federal Aviation Administration. Available at:

Countering the Drone Threat
Implications of C-UAS technology for Norway in an EU and NATO context

This report provides a critical analysis of the typology, procedures, and challenges of counter-drone technology, as well as an assessment of its application in both civilian and military scenarios. Counter-drone technology – or, as it is also designated, C-UAS – refers to systems designed to detect, track, identify and/or intercept unmanned aircraft (commonly referred to as drones), particularly small drones that cannot be countered with traditional anti-aircraft systems designed for use against manned aircraft.

The report argues that C-UAS technology is often not fully effective, and that those wishing to use the technology face a range of hurdles with respect to legality, coordination, planning, and safety. Current legal frameworks are lagging behind technological developments, and therefore many of the available technological solutions cannot be used in civilian settings due to legal restrictions.

Malicious drone use represents a significant security challenge. However, policymakers and practitioners should be careful not to allow this challenge to trigger an over-zealous securitization of civilian airspace.

Drones offer a range of important benefits when used properly. While a balanced approach towards C-UAS is certainly difficult to achieve, it is important that policy-makers, regulators, and law enforcement agencies take both the risks and the opportunities of C-UAS into account in their strategic decision-making.