HM Government

UK Counter-Unmanned Aircraft Strategy

CP 187

UK Counter-Unmanned Aircraft Strategy

Presented to Parliament
by the Secretary of State for the Home Department
by Command of Her Majesty

October 2019

CP 187

This publication is available at www.gov.uk/official-documents

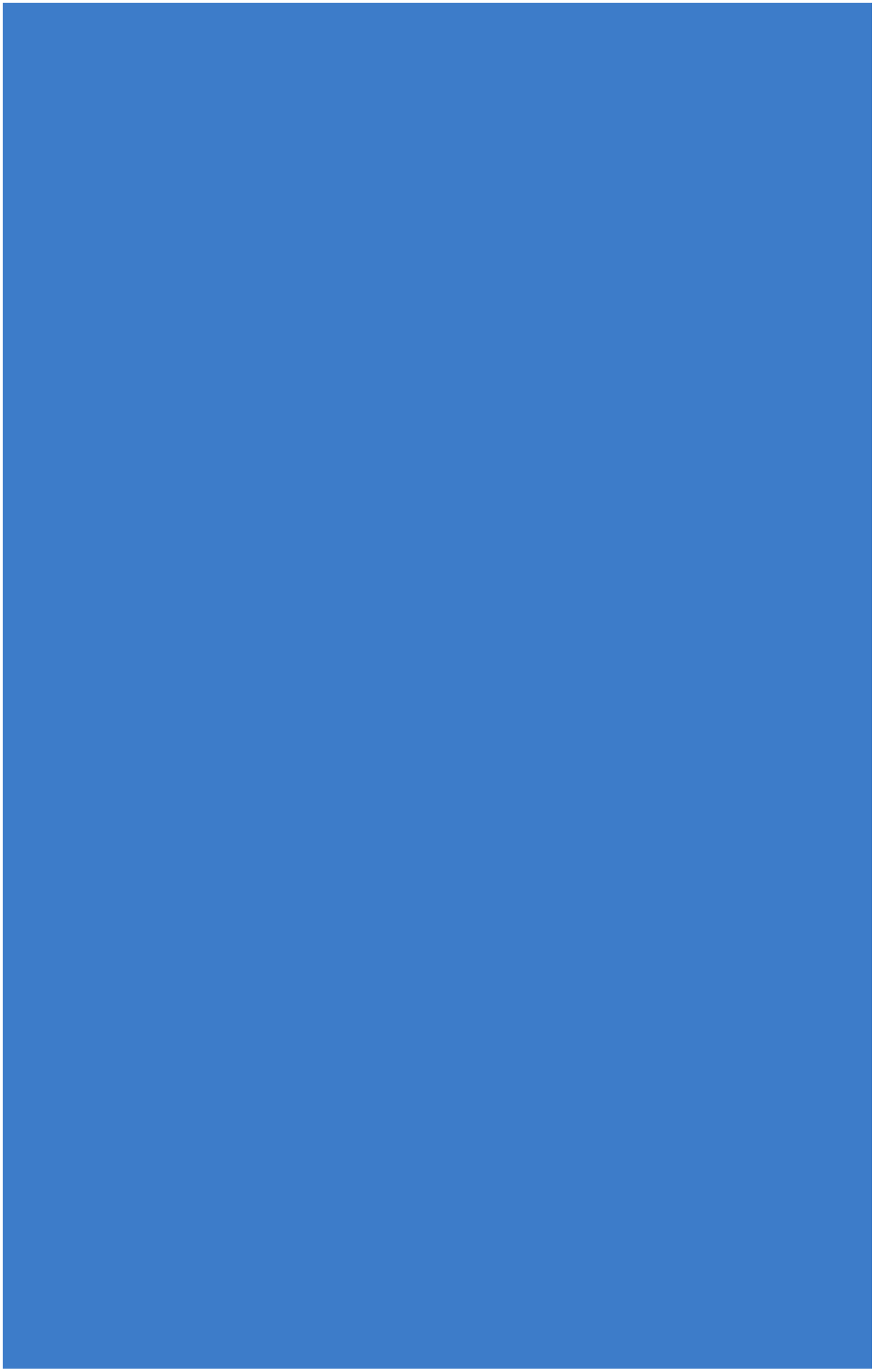
Any enquiries regarding this publication should be sent to us at public.enquiries@homeoffice.gsi.gov.uk

ISBN 978-1-5286-1554-9
CCS0719668012 10/19

Printed on paper containing 75% recycled fibre content minimum

Printed in the UK by the APS Group on behalf of the Controller of Her Majesty's Stationery Office

Contents



Foreword

Rt Hon Brandon Lewis MP

Baroness Vere of Norbiton

By the Security Minister and the Transport Security Minister

Unmanned aircraft – often colloquially called 'drones' – have been available for decades. Until lately the unique challenges of operating aircraft remotely have meant that there have been relatively few users of such systems outside of specialist military operators and skilled model aircraft pilots.

Advances in key technologies mean that in recent years remotely piloted aircraft have become increasingly available, increasingly capable, and increasingly easy to use. Twenty years ago a petrol engine radio-controlled model helicopter would have cost hundreds of pounds and required significant skill by the operator to simply take off. Today a quadcopter drone capable of reliable outdoor flight can be bought for less than £100, and learning to operate it takes a few minutes.

As the barriers to unmanned flight fall, we are beginning to understand the exciting potential benefits to society of embracing drone technology. They have already transformed aerial filming, are increasingly being used for search and rescue and for dangerous, labour-intensive industrial survey work; we could also soon see this technology revolutionise urban logistics and personal transport. Flying drones is a source of enjoyment too, as increasing numbers of recreational users are finding.

Inevitably, this technology comes with risks. Careless and inconsiderate drone users can cause a nuisance and pose a safety risk to others. Ignorance is not an excuse, but we have already produced clear guidance that sets out the responsibilities of drone users[1], and planned legislation will make it easier for the police to act against reckless drone use.

There are also those who would more deliberately use drones for criminal acts, whether that is to facilitate organised crime, to disrupt our national infrastructure, or to commit acts of terrorism. The drone disruption to UK airports over the 2018 Christmas period was a wake-up call for the UK and the rest of the world over how significant the impact of malicious drone use can be. Hundreds of thousands of people had their travel disrupted, with tens of millions of pounds of economic damage.

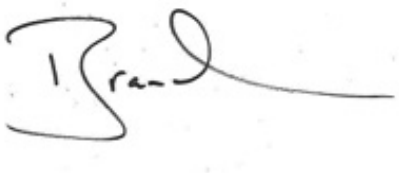
1 https://dronesafe.uk/drone-code/

These events also highlighted that tackling malicious drone use is not easy. Work to reduce the likelihood of such an incident, and our ability to respond to one, had begun before these events and our response was watched closely by our international partners. There is clear international consensus that there is no technological silver bullet suitable for use against all drones under all circumstances and as drone technology advances, the nature of the threat will change. Government needs to strike a balance: we need a security posture that keeps us safe, but it must also recognise the benefits of the legal uses of drones and allow us to reap the fullest rewards of incorporating drone technology into society.

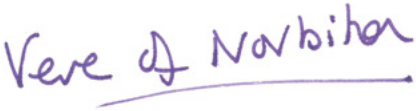
It is clear that the scale of this challenge is wider than any one government department. Tackling malicious drone use needs a comprehensive and layered approach to be put in place by government. This approach will need to blend technological innovation with legislation, regulation and education.

We are also clear that the solutions to this will not reside solely in the UK government. At-risk sectors within private industry will increasingly have to consider their vulnerability to malicious drone use, and how they should best mitigate it safely and legally. Technological countermeasures will need to co-evolve with drones, and within the legal and regulatory frameworks that govern their use.

This strategy sets out how government plans to tackle the malicious use of drones. It will not settle the matter but it is a stepping stone to the future. It sets out the broad principles and priorities for ensuring that the drone-using public knows what is expected of them and the consequences of failing to meet their obligations. It explains how we will make it easier to act against malicious drone use. And it highlights how we will invite industry to work with us to ensure that our evolving security requirements are met.



The Rt Hon Brandon Lewis MP
Minister of State for Security



Baroness Vere of Norbiton
Transport Security Minister

Executive Summary

In recent years unmanned aircraft or 'drones' have evolved rapidly in capability, availability, and their uptake for commercial and leisure use.

The development of drone technology presents significant opportunities. In the coming years, drones have the potential to revolutionise logistics and even personal transport.

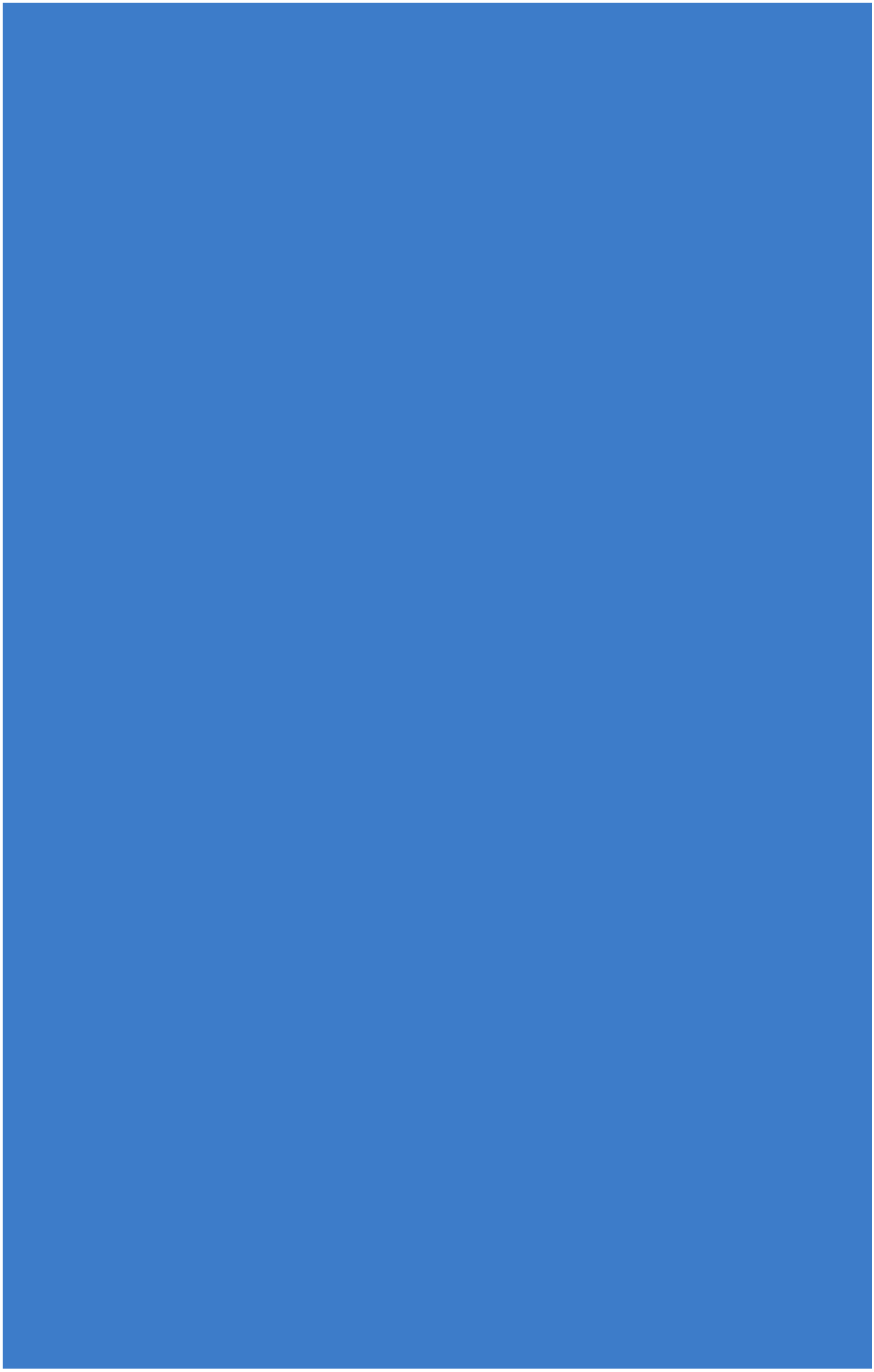
But drones can be misused. If flown recklessly or negligently they can pose a nuisance and a risk to public safety, such as at Gatwick airport over the 2018 Christmas period. Drones can also be used to facilitate or commit crimes.

This document sets out the government's strategy to mitigate the malicious, criminal use of drones, including threats to the UK's national security and critical national infrastructure.

The strategy is forward-looking and will evolve along with the underlying technology to keep ahead of the threat. It provides a single vision for government and industry that will ensure coherence, efficiency and value for money. It will also show the government's intent to ensure a proportionate response to the security challenges posed by drones that will keep the UK an attractive prospect for companies seeking to invest in drone technology and drone security.

The objective of the strategy is to reduce the risk posed by the highest-harm illegal use of drones. We will achieve this by:

1. developing a **comprehensive understanding** of the evolving risks posed by the malicious and illegal use of drones
2. taking a **'full spectrum'** approach to deter, detect and disrupt the misuse of drones
3. building **strong relationships with industry** to ensure their products meet the highest security standards
4. empowering **the police and other operational responders** through access to counter-drone capabilities and effective legislation, training and guidance.



Part 1: Introduction

1.1 Getting ahead of the threat: a counter-drone strategy

This document sets out the government's strategy for reducing the risk posed by the highest-harm illegal use of drones in the UK. It describes four strategic outcomes, and it sets out the actions we will take to achieve those outcomes.

Drone and counter-drone technologies are evolving rapidly. This strategy is flexible and will evolve along with the underlying technology to keep ahead of the threat.

This strategy encompasses the roles of both government and industry, and sits alongside CONTEST, the UK's Counter-Terrorism Strategy[2], and the UK's Serious and Organised Crime Strategy[3].

This document is concerned only with countering the malicious and illegal use of aerial drones. The government's strategy for promoting legitimate drone use in the UK will be set out in the forthcoming Aviation Strategy.

This strategy focuses on the highest-harm risks resulting from malicious use of drones. These include:

- facilitating terrorist attacks
- facilitating crime, especially in our prisons
- disrupting critical national infrastructure (CNI)
- potential use by hostile state actors

These risks are described in more detail in Part 2.

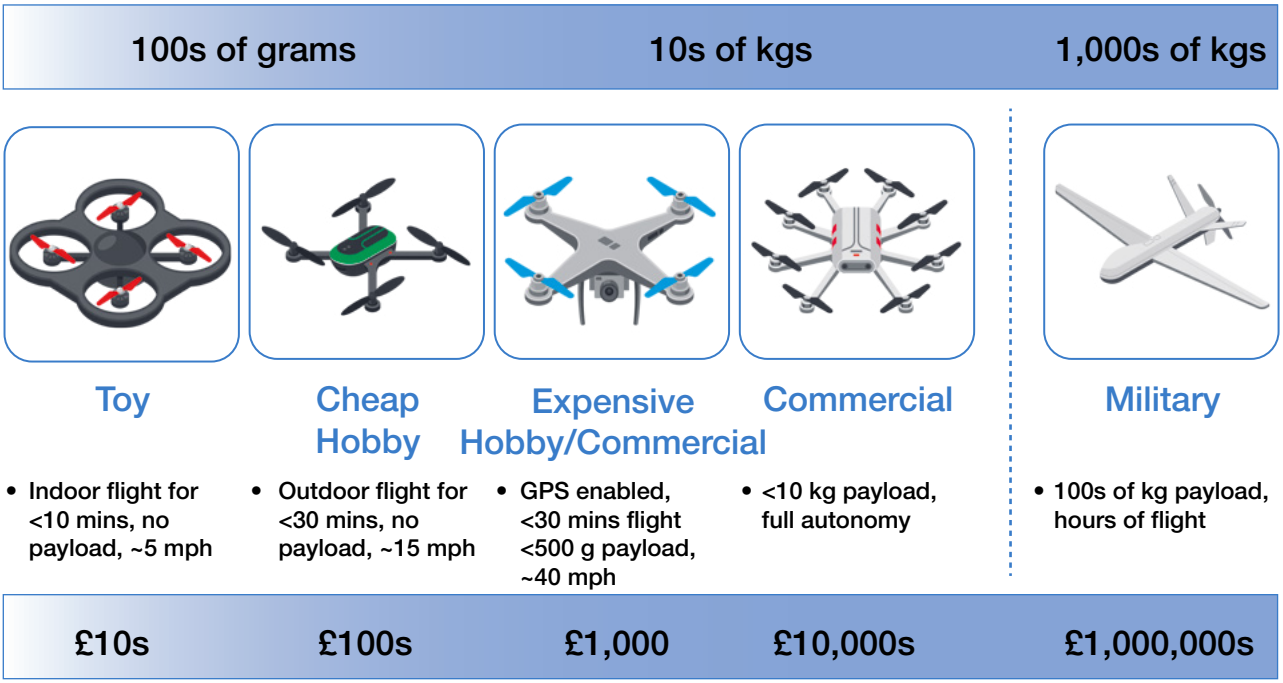
1.2 Background

This document uses the term 'drone' throughout to refer to small unmanned aircraft, whether they are remotely piloted or autonomous.[4] A drone can be fixed-wing, rotary-winged, or a combination of both. It may be controlled remotely, or use satellite navigation systems or other methods to fly autonomously or semi-autonomously. Traditional radio-controlled model aircraft are also classed as drones.

2 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97995/strategy-contest.pdf
3 https://www.gov.uk/government/collections/serious-and-organised-crime-strategy
4 Drones are also referred to as 'unmanned aircraft', 'unmanned aerial vehicles' (UAV), 'remotely-piloted aerial systems' (RPAS), and 'unmanned aerial system' (UAS).

The UK regulates drone use based on weight. The Civil Aviation Authority (CAA) defines those that weigh less than 20 kg as 'small drones'. Those heavier than this tend to be more specialised, complex, and expensive, which means that the barriers to obtain and operate one are much higher. This strategy focuses on countering the risks posed by small drones.

Fig 1. In general, the larger/heavier a drone is, the greater its capability.



Drones can now be easily purchased and are often inexpensive. Many commercial off-the-shelf drones can be modified or upgraded to improve their performance or capabilities.

Drone use in the UK is growing rapidly. This is largely due to increased retail availability, better technology, and lower prices. PwC predicts that by 2030 there could be more than 76,000 commercial and government drones in use in the UK.[5]

The police and other emergency services are embracing drones to protect the public. Drones have the potential to transform activities such as searches for missing people. They have also been adopted into a variety of industries, including: commercial photography, surveying and mapping, search and rescue; safety inspection, and agriculture. In 2014 there were around 400 commercial drone operators in the UK approved by the CAA. There are now over 5000[6], with the number having doubled within the last two years. These primary commercial enterprises have also spawned a secondary level of drone-related support industries, such as drone pilot training and accreditation.

5 https://www.pwc.co.uk/intelligent-digital/drones/Drones-impact-on-the-UK-economy-FINAL.pdf
6 https://publicapps.caa.co.uk/docs/33/20191011RptUAVcurrent.pdf – as of 16 October 2019

Drones already have many agricultural and industrial applications such as crop spraying and survey.

In many cases, drones offer a more cost-effective solution than older technologies. For example, a drone can operate at a fraction of the cost of a helicopter or light aircraft. It also removes the need for physical human access in situations which might otherwise be difficult or dangerous.

Drones have the potential to bring great benefits to the UK. PwC predicts that the industry will contribute an extra £42 billion to the UK by 2030[7]. Increasing levels of drone autonomy will present further uses, such as involvement in supply chains and logistics.

The government supports the responsible use of unmanned aviation to unlock the economic benefits new innovate forms of aviation technology can offer. As announced by the Prime Minister in August the government is providing £125m to the Future Flight Challenge to support the development of innovative aviation systems, and the infrastructure and regulations needed to support them. The government is also supporting work by the Connected Places Catapult[8] to consider how unmanned and manned aircraft may operate alongside each other in the future safely and securely.

But there are risks associated with the rapid increase in drone usage. As with any technology, they are open to abuse. Their misuse through negligence and recklessness also poses a risk to public safety. This is covered in more detail in Part 2.

1.3 What we have been doing

The government is already acting to reduce the risks associated with the illegal use of drones. The **strategy and policy** for this is primarily the responsibility of two departments:

7 https://www.pwc.co.uk/intelligent-digital/drones/Drones-impact-on-the-UK-economy-FINAL.pdf
8 https://cp.catapult.org.uk/2019/09/30/new-report-points-way-to-shared-airspace-between-drones-and-traditional-aircraft/

- The **Department for Transport** is responsible for the safe and lawful use of drones within UK airspace and the associated prosperity benefits
- The **Home Office** has overall responsibility for domestic counter-drone activity as part of its wider security remit

These departments work alongside a range of partner organisations. Further details are set out in Annex A.

Reducing vulnerability

Some of our most important work to date has involved reducing the vulnerability of sensitive sites to drone incursions. Much of this has been undertaken by the Centre for the Protection of National Infrastructure (CPNI). It has included:

- guidance for critical national infrastructure operators, including airports, on how to assess drone risks and vulnerabilities, and on counter-drone technology
- standardised signage to clearly designate areas where drone flights are prohibited, as well as providing information to the public on how to report drone sightings
- setting security requirements for manufacturers and end-users of counter-drone equipment, and providing opportunities for vendors of counter-drone equipment to safely test and refine their equipment

Following multiple drone sightings at Gatwick in December 2018, we have also taken significant additional steps to ensure that our airports are prepared to detect, deter and disrupt drone incursions.

Regulation and guidance

Other aspects of this work are more visible. This includes educating drone users on the obligations the law places on them so that they are less likely to unintentionally misuse drones, increased public awareness of what is legal and what is not, and of the penalties for breaking the law to deter those who may seek to deliberately misuse drones.

In 2016 the Air Navigation Order[9] (ANO 2016) established a number of offences regarding the irresponsible use of drones[10]. Further drone offences were brought in when the ANO 2016 was amended in 2018. These included the requirement, from 30 November 2019, for operators of drones weighing between 250 g and 20 kg to register them and for drone remote pilots to undertake an online competency test. Both registration and competency testing will promote sensible drone use by educating users on regulations and making it easier to identify a drone that is being misused.

We have updated the ANO 2016 as our understanding of the risks posed by drones has evolved.

9 http://www.legislation.gov.uk/uksi/2016/765/contents/made
10 https://www.legislation.gov.uk/uksi/2016/765/contents/made

In the Department for Transport's 2018 consultation, *Taking Flight: The Future of Drones in the UK*, the government announced its intention to give the police new powers to enforce drone offences under the ANO 2016, by:

DRONE **SAFE**
dronesafe.uk

The CAA's 'drone code' clearly sets out what is expected from drone pilots, reducing the likelihood of incidents resulting from ignorance of the rules over unmanned flight.

- giving police the power to require a drone to be grounded
- giving police the power to require operators to produce evidence of registration and competency, and provide the identity of the operator
- improving police powers to investigate where an offence has been committed

The response to the consultation also announced a substantial expansion to the 'no-fly zones' around airports from 1 km to 5 km, which came into effect in March 2019.

In 2018 the Home Office ran the public consultation, *Stop and search: extending police powers to cover offences relating to unmanned aircraft (drones), laser pointers and corrosive substances*. The Home Office response to the consultation, published in February 2019, included a commitment to develop a stop and search power for offences relating to flying a drone in the restricted zone of an aerodrome[11].

The government is committed to introducing legislation to give the police new powers to effectively investigate and act against illegal drone use.

Drones have caused high-profile disruption at airports in the UK and overseas.

11 ANO 2016 article 94A; http://www.legislation.gov.uk/uksi/2016/765/contents/made

International partnerships

We continue to work internationally with partners who are facing similar challenges, to ensure that best practice, intelligence sharing and technological innovation in the counter-drone sector is shared and fully reflected in our decision-making.

We have also worked with UK and EU regulators to develop product standards for counter-drone technologies. We have conducted technical evaluation and testing on a range of counter-drone technologies, as well as developing a programme to direct research efforts into improving counter-drone technology. In addition, we are standardising other measures such as deterrence communications and signage. This messaging is underpinned by the CAA's work to educate drone users about responsible and safe flying. Some drone manufacturers have proactively introduced geofencing to protect key sites, ahead of new European drone regulations which will come into force over the next three years.

1.4 Our vision for the future

Success over the next three years will involve a reduction in the risks posed by the highest-harm use of drones while also maximising the benefits of drone technology to our society and economy.

We will achieve this by:

1. developing a comprehensive understanding of the evolving risks posed by the malicious and illegal use of drones
2. taking a 'full spectrum' approach to deter, detect and disrupt the misuse of drones
3. building strong relationships with industry to ensure their products meet the highest security standards
4. empowering the police and other operational responders through access to counter-drone capabilities and effective legislation, training and guidance

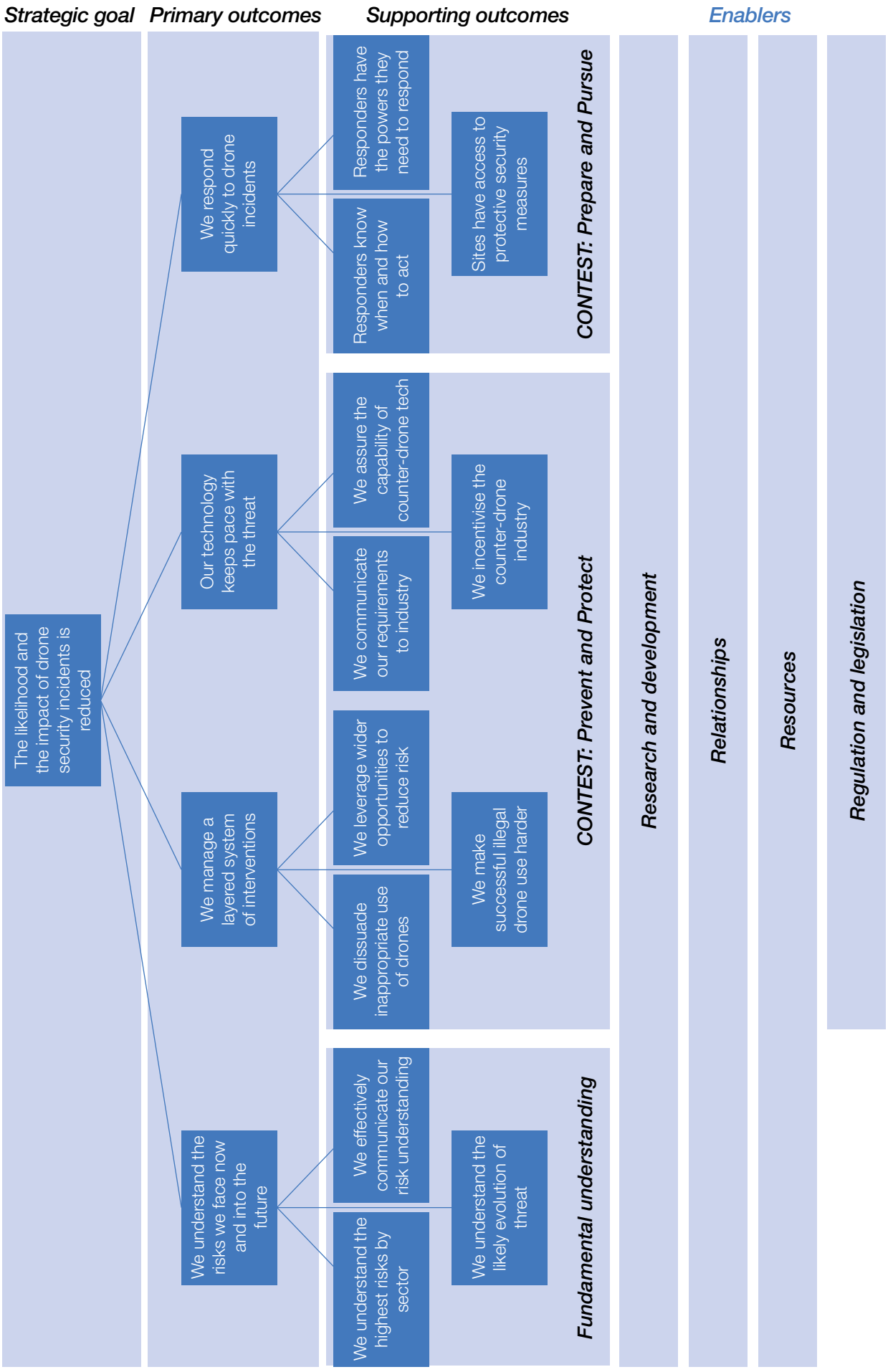
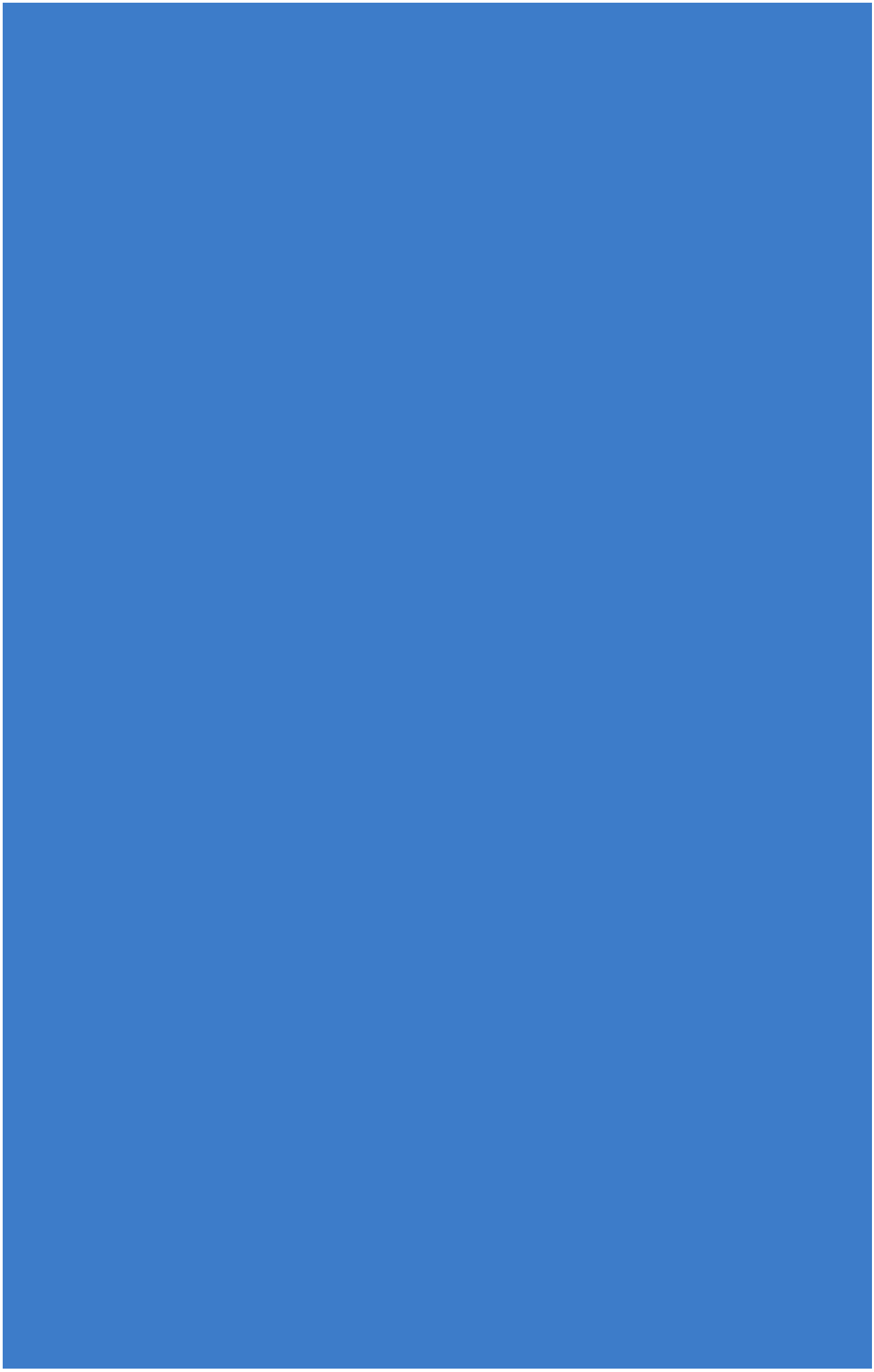


Fig 2. The four outcomes we seek to achieve are aided by a number of supporting outcomes, and key enablers.



Part 2: A Comprehensive Understanding of Risk

Objective: We will develop a comprehensive understanding of the evolving risks posed by the malicious and illegal use of drones.

The misuse of drones presents a range of risks. We are most concerned about their potential for misuse in support of terrorism, serious and organised crime, or disruption of critical national infrastructure. Some of these risks are set out in more detail below.

Terrorist use of drones

Commercially-available drones have already been used and modified in Syria and Iraq by terrorists to conduct reconnaissance, attacks, and filming for propaganda purposes. Terrorists in the UK could attempt to use such methodologies for similar attacks.

Serious and organised crime

Criminals, such as serious and organised crime groups, currently use commercially-available drones to deliver contraband into prisons. In prisons across England and Wales there were 284 drone incidents in 2016, 319 in 2017 and 168 in 2018, with 165 drones actually recovered at prisons during 2016 and 2017. The profits on offer can make it worthwhile for criminal gangs to prepare and run relatively sophisticated operations following a modest investment in a drone. On 26 October 2018, following the largest investigation of its kind, 15 members of an organised criminal gang were collectively sentenced to nearly 40 years in prison for using drones to drop drugs into Merseyside prisons. The ringleader received a custodial sentence of 10 years, the highest single sentence for drone-related activity to date. The contraband delivered, such as drugs, contributes to violence, crime and vulnerability within prisons, which threatens safety, destabilises prisons and undermines the efforts of hardworking staff and prison officers in delivering effective rehabilitative regimes.

Disruption to aviation and critical national infrastructure

Aviation facilities, particularly large airports, are attractive targets for terrorists and those involved in serious and organised crime because of their high-profile and iconic nature. An attack, or malicious and disruptive incursion using a drone, such as that seen at Gatwick Airport in December 2018, can have serious safety, security and economic consequences.

Our response needs to be proportionate to the threat. In order to ensure our approach is effective, we need a detailed understanding of how drones can be misused. We must also keep pace with changing technology. Understanding the evolution of drone technology and the increasing incorporation of drones into business and society will be crucial to staying ahead of the threat.

What we will do

Build a comprehensive, up-to-date risk picture, with greater understanding of threats, impacts and vulnerabilities

We will draw together and focus our cross-government expertise on threats, vulnerabilities, and scientific and technological developments. This will ensure that we have a clear, consistent understanding of the different risks that we face today and will in the future.

To enable this we will use the full range of the information available to our law enforcement and intelligence agencies – and our international partners – on the intent of our adversaries and how they will look to use drones against us.

We will improve our understanding of the scale of malicious drone use by introducing new national standards to improve the consistency of how hostile drone incidents are logged and reported by the police across the UK, as well as by those responsible for security in specific at-risk sectors.

As not all drone threats will arise from commercial off-the-shelf drones, our policymakers and regulators will engage with the manufacturers of drone components and aftermarket products to give us greater insight into how these capabilities might be exploited for malicious purposes.

The government already gives security advice through a number of organisations including CPNI and the police. We will expand government engagement over security with at-risk sites and sectors to encourage them to consider drones as a distinct threat and will work with them to identify and address vulnerabilities.

Horizon scanning to predict the evolving threat

Drone technology is rapidly evolving and our response needs to keep pace. We will therefore work to understand how drone-based threats might evolve in the future, both at the tactical and strategic levels.

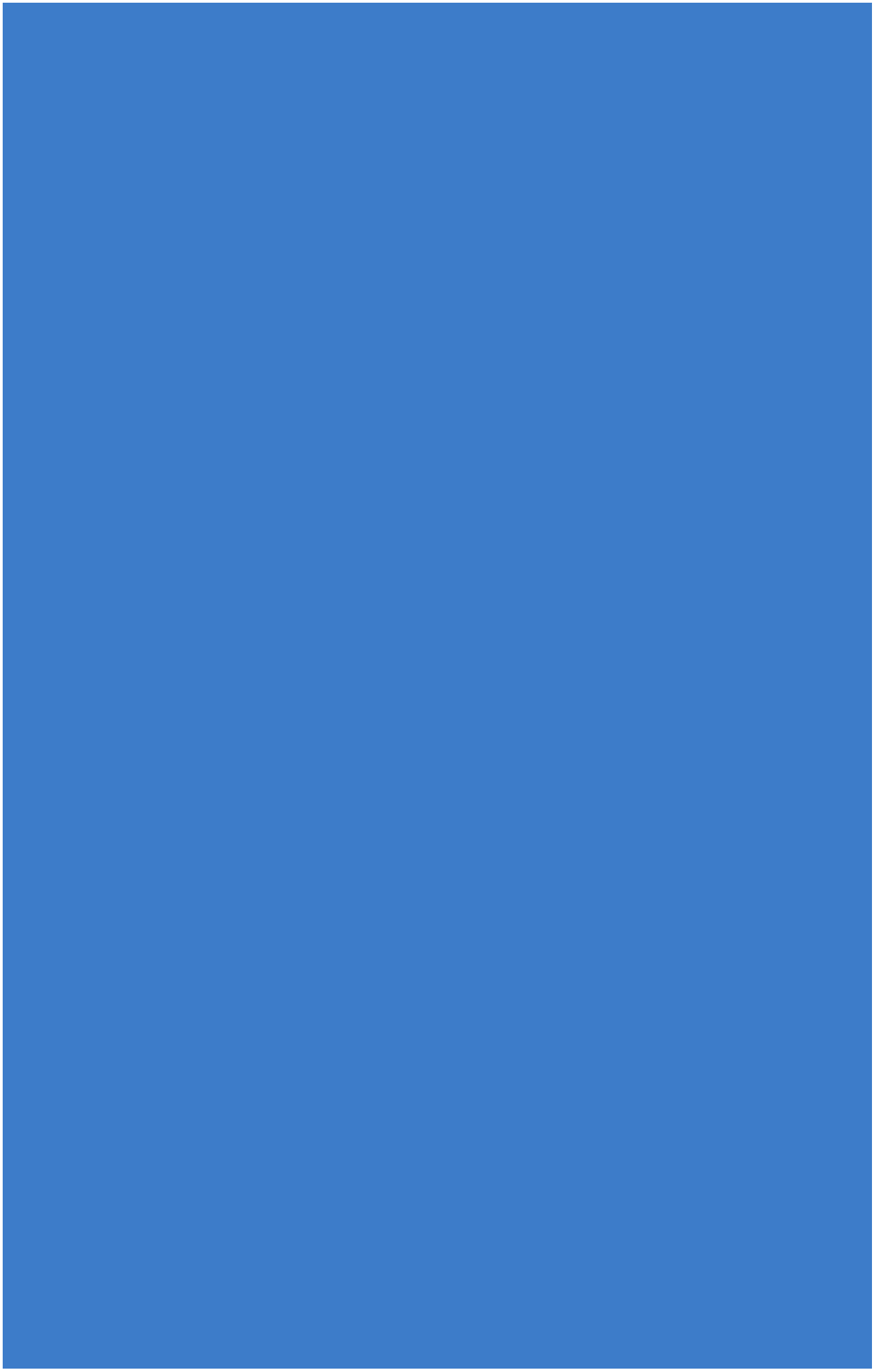
As part of this we will draw upon the resources of the UK intelligence community as well as science and technology partners such as the Government Chief Scientific Adviser community, industry and academia.

We will use our continuing engagement with drone manufacturers to understand their technology pipelines and how drones are likely to evolve over the medium- and longer-term in ways that might be exploited by rogue operators.

We will also work with wider industry to understand their plans for incorporating drones into their business models. This will allow us to understand and address potential future vulnerabilities.

Communicate the risk picture to those that need it

We will provide clear and consistent advice on the threat to the police, as well as to those responsible for providing security at at-risk sites. We already have well-established networks for sharing security information and advice with private operators that own or operate CNI, crowded places, and other at-risk sites. We will use these to share more on drone-related risks to allow a common understanding of threats and ensure that risk can be determined consistently. We will also use these networks to encourage at-risk industry sectors to share counter-drone information and best practice amongst themselves to improve knowledge and awareness.



Part 3: An End-to-End Approach to Reducing Risk

Objective: We will take a 'full spectrum' approach that maximises the opportunities to deter, detect and disrupt the criminal misuse of drones.

The UK has well-established and successful 'full spectrum' approaches to countering terrorism and serious and organised crime[12]. These approach risk reduction as a system of layered and overlapping activities, using a wide range of tools and opportunities across law enforcement, wider government, and the private sector. We will approach tackling the highest-harm criminal use of drones in a way that is consistent with these approaches.

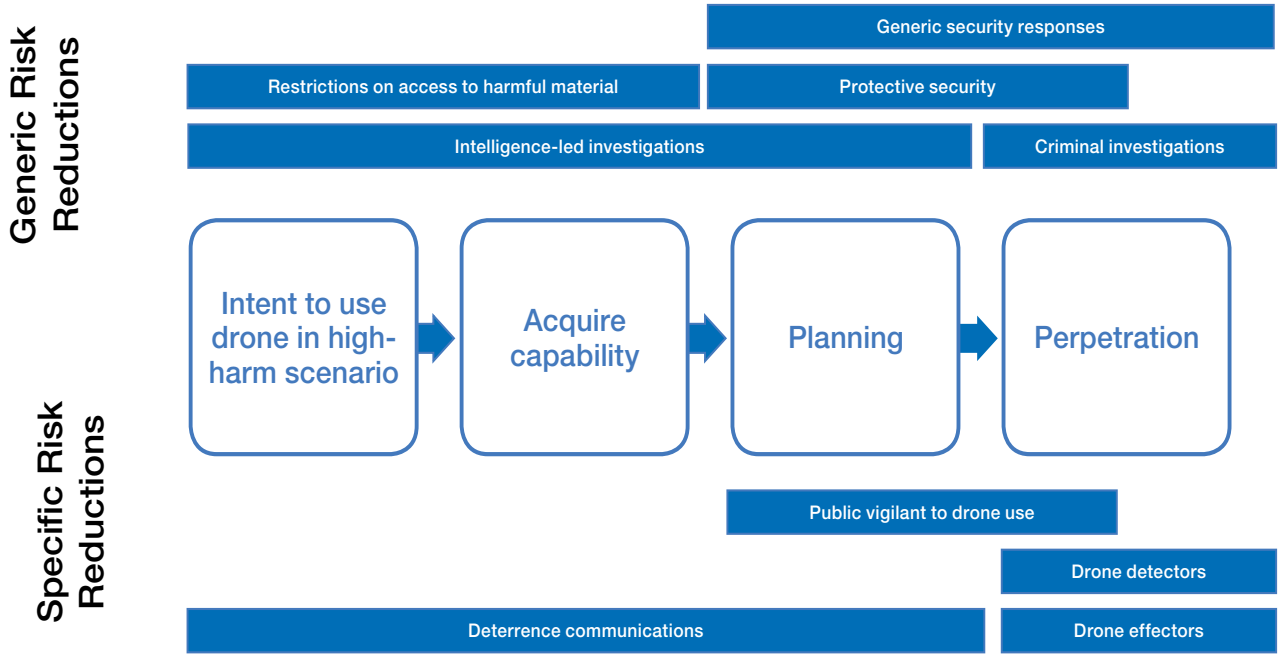
What we will do

We will apply our understanding of the evolving drone risk to build an end-to-end approach to tackling the highest-harm criminal use of drones. We will reduce risk by ensuring that we maximise existing opportunities and reinforce points of relative weakness across the system, whether early in the development of a threat, or later in specific at-risk sectors.

Our aim will be to stop malicious and illegal drone use as early as possible, ideally before a drone is used in a crime. We will ensure that existing approaches to drone safety and wider security challenges are exploited for maximum benefit to drone security. We will also work to make it easier to identify malicious drone use against a backdrop of increased legitimate use.

12 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97995/strategy-contest.pdf; https://www.gov.uk/government/collections/serious-and-organised-crime-strategy

Fig 3. Examples of layered risk-reduction across a timeline of high-harm criminal drone use. Risk reduction activity become more specific and layered later in the timeline



Use the full range of tools at our disposal

This strategy sets out a number of approaches that are specific to the drone element of high-harm criminal use of drones. But many of these scenarios involve drones being used as new ways to facilitate old crimes, for which there are already end-to-end security approaches such as community policing, proactive intelligence-led investigations, and initiatives that restrict access to the most hazardous materials. We will ensure that the benefits of these approaches are factored into our planning, and that those that deliver these wider interventions do the same.

Make it easier to identify illegal drone use earlier

Capitalising on safe-use initiatives

Measures designed to promote the safe and responsible use of drones bring security benefits of their own. The greater the proportion of remote pilots who fly their drones by the rules, the harder it becomes for hostile use to go unnoticed.

The CAA's DroneSafe website, and the associated Drone Code, use simple, clear messaging to promote the basic rules governing safe drone operation. The CAA also operates a scheme that allows retailers who follow a specific set of safety guidelines when selling drones to be designated 'DroneSafe'.

From 30 November 2019, we will place a legal requirement on all drone operators[13] to register with the CAA and receive a validated drone operator registration number which they must affix to their drone before it is flown. We will also require all remote pilots of drones to pass an online competency test and receive an acknowledgement of competency from the CAA before flying a drone. As we update the online systems that enable this we will ensure the needs of the police, drone operators and remote pilots are reflected to facilitate effective, real-time enforcement.

13 These regulations will affect operators of drones with a take-off weight greater than 250 g.

The government is developing its concepts for the future implementation of an unmanned traffic management (UTM) system. UTM will provide a means of preventing collisions between unmanned aircraft and other aircraft, manned or unmanned. While UTM will not be delivered in the lifetime of this strategy, we will ensure that security concerns are appropriately incorporated in early planning.

The drone industry

We will continue to build on our successful relationship with the drone industry. This will help to improve existing counter-drone measures and identify new opportunities. We are establishing a new Industry Action Group that will provide a starting point for us to ensure a continued, stronger dialogue between manufacturers and government.

Many commercially-available drones already include geo-fencing capabilities – software that can restrict a drone from flying in certain areas, such as airports. The government is engaging directly with drone manufacturers and industry on how these capabilities can be improved. We are working with airspace managers and regulators to understand how best robust data on permanent and temporary airspace restrictions, such as those around airports and other critical national infrastructure sites, can be made available in a format that manufacturers and technology developers can easily use, in order to improve safety and help drone users fly in accordance with the rules.

The government will consider what further product standards or restrictions within the drone sector could reduce risks associated with the misuse of drones without disproportionately affecting legitimate users, setting new international standards with likeminded partners such as Five-Eyes nations and the European Union Aviation Safety Agency.

We will also work with the wider drone industry of retailers and distributors, flight or maintenance training providers, and drone-focused publications and media to achieve our security objectives. This also includes working with companies operating in the UK that might aspire to use drones as a fundamental part of their business model, such as agricultural suppliers, online retail companies and companies offering taxi-style services.

Signage is designed to make it clear to drone operators that they are in restricted airspace, and make it easier for the public to report illegal drone use.

Deter people from using drones illegally

We will work with behavioural scientists, law enforcement, and at-risk sites to identify the most effective ways to deter people from using drones maliciously.

We will act to improve the public's awareness of the illegal use of drones, whether that is irresponsible use or deliberate malicious use. We will encourage the public to report instances of drone misuse and equate wider vigilance campaigns with suspicious drone use, as much as other terrorist or criminal activity. By better publicising prosecutions for drone offences we will reinforce this narrative and make it harder for people to claim ignorance when prosecuted.

We will encourage local-level messaging to support community engagement in the vicinity of critical national infrastructure and other at-risk sites, such as urban areas adjacent to prisons.

We will complement this with more targeted messaging and engagement to encourage vigilance amongst the recreational drone and model aircraft flying communities, and with commercial drone operators. These communities are more likely to have a greater ability to identify suspicious drone behaviour – either on the part of the pilot or the craft itself – than the public at large. This will be similar to existing campaigns with the general aviation and maritime communities.

Part 4: Counter-Drone Technology, Testing and Industry

Objective: We will build strong relationships with industry to ensure their products meet the highest security standards.

There is a clear need for effective technical solutions to counter the malicious use of drones. Our police need access to a range of equipment that can allow them meet the wide range of drone security challenges that they may have to respond to. At-risk sectors will also need access to technologies that are appropriate to them.

The counter-drone industry that will provide this equipment is small but evolving rapidly, with many small-to-medium enterprises having emerged recently. Many of the systems entering the market are prohibitively expensive, and no single system is suitable for all situations. We need to ensure that the counter-drone industry meets our security requirements. This means producing equipment that is safe, effective, and offers good value for money. It also means keeping pace with the continued rapid development of drone technology.

The government already engages with the counter-drone industry to a significant degree, across multiple sectors and agencies. We will take a stronger, cross-government approach to working with the counter-drone industry, including sharing information on threats and vulnerabilities so that industry can offer solutions.

We will work with industry to ensure that the equipment available to operational responders to deal with a hostile drone situation is both effective and safe. We are already conducting work to research and test counter-drone equipment. This benefits both industry and government, and helps to ensure new technical solutions move quickly from next-generation to in-service. We will ensure that any solutions remain proportionate to the threats we face.

What we will do

Communicate the UK's security requirements to the counter-drone industry

We will work with the counter-drone industry to encourage a thriving sector that is aware of, and responsive to, the needs of government. As set out in Part 2, we will help industry to plan for the future by sharing more information about current threats and vulnerabilities, and by helping them better understand how drone technology development might challenge their security in the future. We will also provide greater clarity around our operational response (Part 5) and the legislation and regulation underpinning the use of counter-drone technology as it evolves. We will also ensure that both drone and counter-drone industries are aware of our long-term intent over our plans to increasingly incorporate drone technology into society and our economy.

Incentivise and facilitate the counter-drone industry to meet our requirements

We will do more to ensure that the counter-drone industry brings to market the most effective technologies, including by incentivising investment in new technology.

Testing and accreditation will facilitate this. We will also explore and encourage innovative technologies that could be incorporated into counter-drone approaches. We will ensure that we take a co-ordinated approach to funding science research and technology development that accelerates the early development of potential solutions, as we have already done in sectors such as airport security. We will also explore how we can make it easier for small companies with novel approaches and technologies to collaborate in the development of new systems.

The UK has the potential to be a world leader in counter-drone technology. We will work with overseas partners to promote our approaches and technology solutions internationally.

Evaluate and assure the counter-drone solutions that industry develops

Informed by our understanding of current and future risks, we will work with industry to ensure our research, development and testing takes into account innovation in drones and in counter-drone approaches. This activity will support the development of the full range of counter-drone technology, including systems to detect, track and identify drones, as well as counter-drone effector systems that can disrupt drones being used illegally.

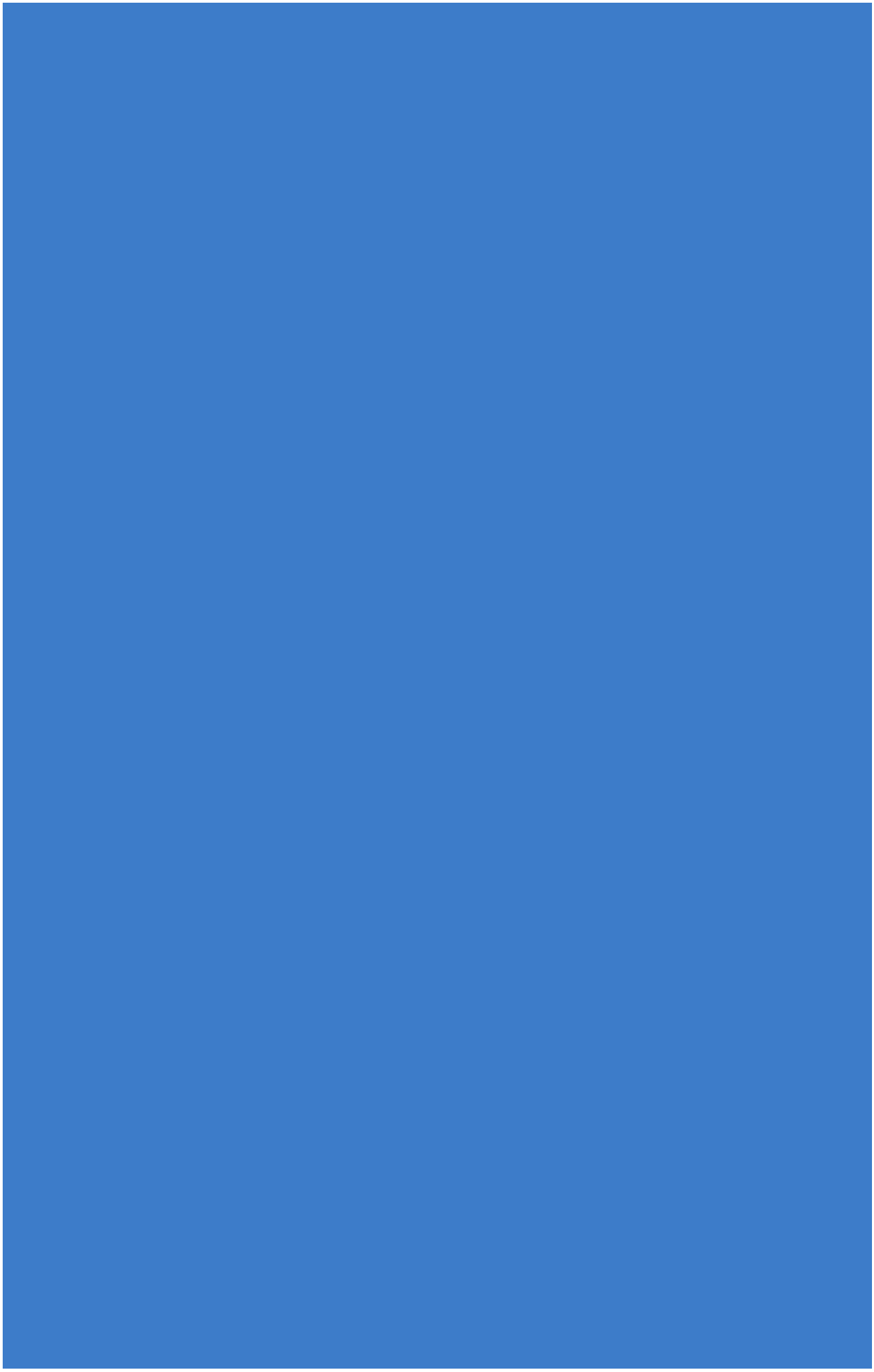
We will incorporate the results of this testing into a single government catalogue of approved domestic counter-drone capabilities. This will be available to partners to help them make effective procurement decisions.

We will investigate how both government and industry can safely and legally test and evaluate counter-drone systems throughout their development in settings that are as close as possible to the real-world environments in which they will ultimately be used. Our approach will evolve over time to ensure our operational responders continue to have access to effective capabilities.

We will continue to develop and refine our frameworks for evaluating counter-drone equipment that can be shared with industry, so that our accreditation methods are transparent. To reduce the burden on industry of successfully bringing counter-drone technology to market, we will also work alongside international partners to promote the importance of common international standards for counter-drone systems.

We will increase our collaboration with international partners on counter-drone research and testing. Where those links are already strong we will look for opportunities to align our respective counter-drone research programmes and adopt a complementary approach, sharing resources and knowledge.

We will accelerate our investigations into the potential benefits of new and emerging technologies in other fields, drawing upon expertise from across government science and technology programmes.



Part 5: Enabling Effective Operational Responses

Objective: We will empower the police and other operational responders through access to counter-drone capabilities and effective legislation, training and guidance.

Capable operational responders are vital to our counter-drone approach. These responders will in many cases be police officers, who, depending on the incident, could be required to exercise a counter-drone response across any at-risk sector. Specific at-risk sites will have their own operational responders. This could include other public sector employees such as prison officers, or private sector employees responsible for safety and security in a variety of locations, such as privately-operated prisons, critical national infrastructure, and crowded open-air public spaces.

We need the police to have a full range of powers and technologies to act against malicious drone use, but these other responders also need to be empowered through training and, where appropriate, through access to counter-drone systems and the powers to use them.

We will work to ensure that all responders have access to training, technology and legal powers appropriate to their roles and the drone risks they face, so that they can act confidently and decisively to address drone-based threats.

Different sectors and the sites within them face different risks, and have different response requirements. While response plans might be site-specific, they will need to be guided by nationally-consistent principles to prevent any gaps in capability.

What we will do

Ensure operational responders know when and how to act

A wide range of government organisations play a role in responding to malicious and illegal drone activity (see Annex A). A co-ordinated approach is critical to maximising the effectiveness of our response.

We will clarify which parts of government are responsible for each aspect of the response. We will ensure that operational processes and requirements, and the legislation that enables them, are reviewed regularly so that we are able to keep them up-to-date with evolving drone risks.

The police and other operational responders must have counter-drone knowledge and capabilities appropriate to their remit in order to mount effective, proportionate counter-drone responses. We will use the principles within this strategy to develop nationally consistent guidance and response plans. We will continue our ongoing programme of counter-drone response exercises to inform our approach.

This guidance will act as a toolkit that can be applied to different scenarios and sectors. Guidance for responding to nuisance drone use will be developed separately.

As first responders, the police need training, powers and equipment to tackle illegal drone use.

We will continue to share advice and guidance with privately-operated CNI and other at-risk sites through our existing security engagement networks, to inform and improve their counter-drone approaches. This will ensure consistency and interoperability with the wider government response in the event of an incident.

We will encourage all public and private sector organisations involved in counter-drone activity to resource their efforts appropriately and focus them in the right places.

We will work to understand how police investigations and prosecutions can be strengthened through improved capabilities to obtain forensic information from recovered hostile drones.

Facilitate access to layered, complementary counter-drone defences

Layered, complementary drone defence is about ensuring that at-risk sites have the right combination of complementary measures to enable an effective response. It takes the principle of the whole-system approach, and applies it at the local or site level. These measures can be employed from the point an adversary has deployed to a launch site in preparation for their hostile activity. Earlier opportunities to disrupt hostile drone use are covered in more detail in Part 3.

Often these measures will consist of counter-drone technology, such as geo-fences, equipment to detect, track and identify (DTI) and effector equipment that can disrupt illegally-operated drones. The most effective response may often include non-technical measures such as physical security, (e.g. fencing, screens, window bars or anti-helicopter nets), general surveillance (e.g. CCTV or clearing lines of sight), or personnel (e.g. patrolling likely launch sites). However, these measures can prove prohibitively expensive in some settings.

Every at-risk location will have different requirements. Through our existing security engagement arrangements, we will support sites and sectors, and the operational responders at them, to understand what comprehensive, layered counter-drone defences are appropriate to them so that they can provide an effective response to hostile drone incidents.

In general, non-technical measures are already proven and readily available, although they can be disproportionately expensive for widespread use. We will therefore encourage at-risk sites to prioritise implementing these measures to mitigate the threat from malicious drone use. As our testing and evaluation activity matures, sites will be able to access advice over counter-drone technical capabilities suitable for their needs.

The police are able to legally deploy a range of DTI and counter-drone effector systems. We will develop options for the creation of a UK national counter-drone capability that will reduce our domestic reliance on defence capability to respond to the most challenging drone security incidents, and will allow the police to protect national iconic events, or support crisis response. We will identify the most appropriate equipment and resource to procure and deliver this capability.

The use of many counter-drone technologies outside of the police is restricted. We will explore how best we can ensure that other operational responders are able to legally use a range of counter-drone effector technologies.

Where those technologies are deployed, we will mandate that a record is kept of the circumstances surrounding every occasion on which the equipment is used. We will also require processes for recording and resolving any complaints received in relation to the use of this equipment.

We will develop standardised, appropriate signage for use at CNI and other at-risk sites to deter hostile drone use. Consistent, clear signage will also help the public better understand where drones can and cannot be flown, and this knowledge in turn will mean that operational responders are better able to determine the intent of any drone that is flying in contravention to that signage. With the use of DTI and effector equipment becoming more widespread, we will also ensure that signage conveys sufficient legal information to warn drone users of the consequences of breaching a site perimeter.

In the longer term, we will use our understanding of future threats and risk to develop our thinking and guidance on interoperability between counter-drone equipment and drones operated legitimately by, for example, the police, or logistics companies.

Provide appropriate powers to enable an effective response

Drones provide a new way to commit acts that are already criminal. However, some of the unique and evolving capabilities of drones mean that current police powers need to be built upon to meet the evolving threat, and some of the processes that underpin these powers were not designed with counter-drone capability in mind, and will benefit from being refined.

The government will introduce an Air Traffic Management and Unmanned Aircraft Bill to tackle the misuse of drones. The measures contained in the Bill will provide greater enforcement capability to the police and act as a deterrent to those who would commit offences related to drones.

To enable this, the Bill will make provision for new powers for police officers to allow them to better enforce drone regulations in the Air Navigation Order, and prohibitions related to prisons in the UK. This will include powers to stop and search in specific circumstances, and powers to issue fixed penalty notices for minor offences.

The Bill will also make provision for the police and those acting on their behalf to use counter-drone technologies against drones being used to commit certain ANO 2016 offences, certain prison related offences and an offence in the Aviation and Maritime Security Act 1990.

Further work will be needed to ensure that our legislation keeps pace with the evolving threat, is responsive to operational experience, and directly informs training and guidance. We will continue to develop proposals for inclusion in future legislation so that the legal framework within which operational responders must operate does not become obsolete or hamper their ability to respond to and investigate hostile drone activity. In particular, government will:

- streamline the ability of police and third parties to secure authorisation to use counter-drone technologies (both effectors, and some DTI equipment) to ensure that they remain accessible as the need to use them increases
- explore how we can provide operational responders with the ability to seize or retain any drones that land or crash within at-risk sites, to allow them to be passed on to the police for further investigation

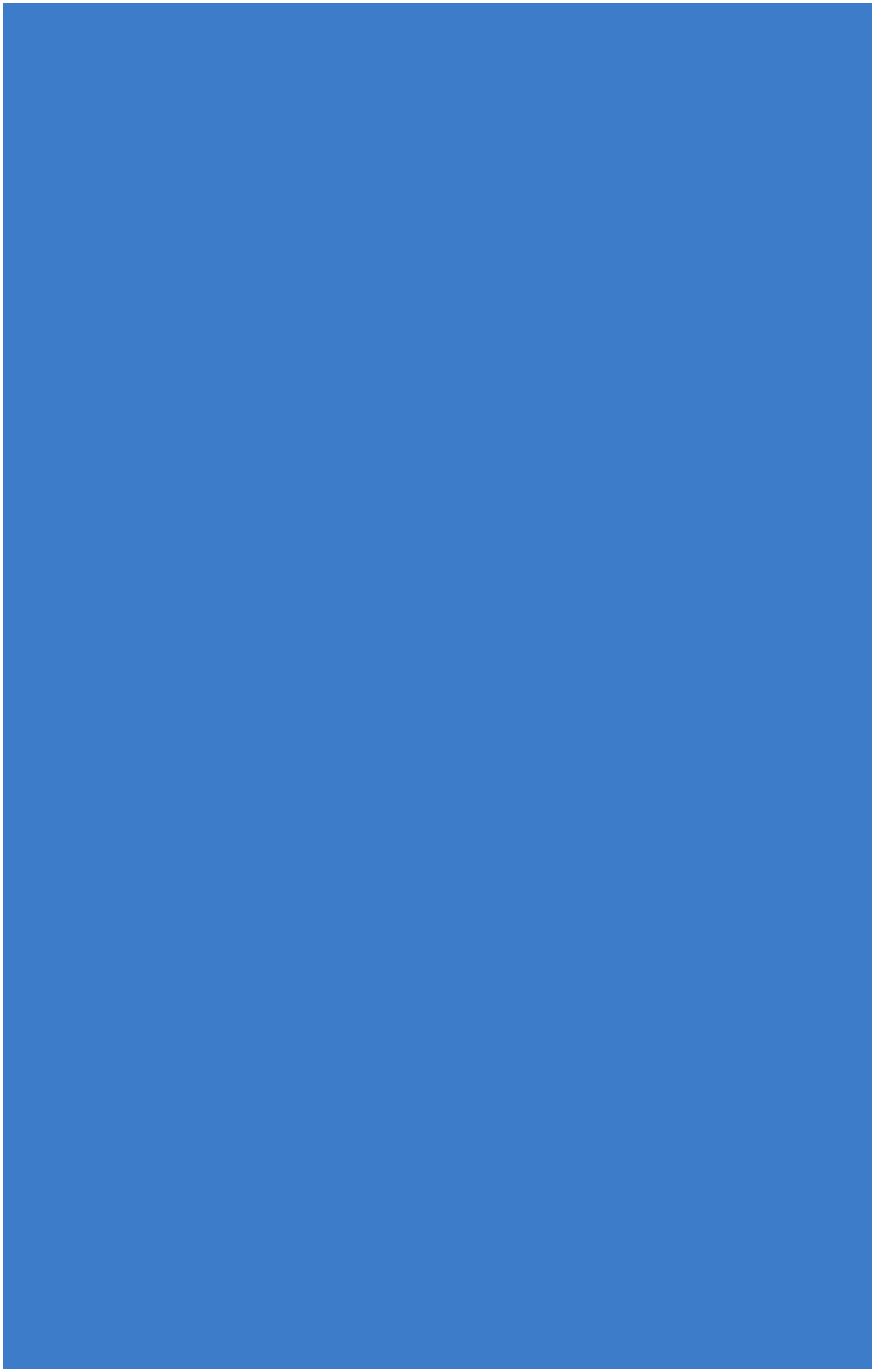
As referred to in Part 3, new legislative approaches to restrict the sale of certain drone types or drone components that could make it harder to respond to a drone incident will also be investigated.

Part 6: Tracking Success

Reducing the risks posed by malicious illegal drone use will require investment of time, money and personnel. We must ensure that this investment offers positive benefits. To do so, we will measure performance and delivery throughout the life of the strategy.

We will develop new performance measures to track delivery against the strategy. We will regularly review these measures to determine where and how to rebalance our investment in drone security in order to keep it effective whilst providing value for money, and ensuring that the UK remains able to reap the positive benefits of incorporating drone technology into business and society.

Due to the fast-evolving nature of drone and counter-drone technology, it is our intent to review and if necessary refresh this strategy in three years. Success in that period will look like the embedding of counter-drone technology and approaches into business as usual practice across our police forces and increasingly in the private sector, all against the continued increasing incorporation of drone use into business models. It will also see the UK at the forefront of the incorporation of drone technology into society and into our business models.



Annexes

Annex A: Key Counter-Unmanned Aircraft Stakeholders

Delivering the strategy will be a collective effort across a range of departments and stakeholders, each of which has a distinct counter-drone interest:

Cabinet Office and Ministers – National Security Council co-ordination, providing oversight and direction.

Centre for the Protection of National Infrastructure – Provision of advice to CNI on the national security risks they face, and support to the implementation of protective security measures for CNI sites and assets.

Civil Aviation Authority – Regulates UK aviation and airspace.

Crown Prosecution Service – Responsible for prosecuting criminal offences involving drones.

Department for Business, Energy and Industrial Strategy – Lead government department for supporting business, including the protection of civil nuclear and energy sites.

Department for Transport – Promotion of safe and responsible drone use with CAA and general transport security.

Defence Science and Technology Laboratory – Technical expertise and testing to support protection of defence infrastructure.

Her Majesty's Prison and Probation Service – Responsible for custodial facilities and for policy over their protection.

Home Office – Oversight and coordination of CONTEST, the UK's counter-terrorism strategy, wider policing, and overall responsibility for domestic counter-drone activity.

Military Aviation Authority – Regulates all UK military aviation.

Ministry of Defence – Protection of UK defence sites and overseas force protection. Defence also holds specialist counter-drone capabilities that can be made available to the civil authorities under extraordinary circumstances.

Ministry of Justice – Prevention of conveyance of prohibited articles into prisons.

Ofcom – Protects and manages the radio spectrum.

Police – Operational activity, enforcement & response.

Industry – Drone and counter-drone development, innovation and delivery.

International Partners – We work with many agencies across our international partners to share knowledge and best practice over drone safety and security.

Annex B: Key Enablers

Research and Development. Scientific and technical understanding is vital to all elements of understanding current and future drone risks, and of how to develop effective countermeasures for malicious illegal drone use. In government this research is typically sponsored by departments and undertaken in government research organisations (e.g. Defence Science and Technology Laboratory) or contracted out to academia and private industry.

Resource. Developing new counter-drone approaches requires appropriate resourcing. Technological solutions will form a significant element of counter-drone capability and will require appropriate investment in testing and evaluation, as well as procurement, operation and maintenance. Ensuring that this is appropriately resourced will be a key part of any government Spending Review.

Relationships. The counter-drone strategy presents a central government vision for a collective response to the risks posed by the malicious and illegal use of drones. The risks posed and the response needed is bigger than any single UK government department. It will require action from across government organisations, the private sector, our international allies, and multilateral organisations.

Regulation and legislation. The Air Traffic Management and Unmanned Aircraft Bill will contain a number of proposals that will make it easier for the police to enforce legislation over the safe and responsible use of drones, but further regulation and legislation will be needed. This will have to co-evolve with drone technology.

HM Government

ISBN 978-1-5286-1554-9

CCS0719668012